Révisions : correction

Exercice 1. Dans cet exercice et dans la suite, on notera $[a]_\mathrm{I} \in \mathrm{A/I}$ la classe modulo I d'un élément $a \in \mathrm{A}$.

1. Soit $\mathrm{I} \subseteq \mathrm{A}$ un idéal maximal et $a, b \in \mathrm{A}$ tels que $ab \in \mathrm{I}$. L'idéal (I, a) engendré par I et a contient évidemment I. On a donc $(\mathrm{I}, a) = \mathrm{I}$ ou $(\mathrm{I}, a) = \mathrm{A}$. Dans le premier cas, $a \in \mathrm{I}$. Dans le second, a est inversible modulo I : il existe $c \in \mathrm{A}$ et $i \in \mathrm{I}$ tel que $ac + i = 1$. Cela entraîne $b = b(ac+i) = (ab)c + bi \in \mathrm{I}$.
2. On a la suite d'équivalences

$$\begin{aligned}\mathrm{I\ premier} &\Leftrightarrow \forall a, b \in \mathrm{A}, ab \in \mathrm{I} \Rightarrow a \in \mathrm{A} \text{ ou } b \in \mathrm{A} \\ &\Leftrightarrow \forall a, b \in \mathrm{A}, [a]_\mathrm{I} \cdot [b]_\mathrm{I} = 0_{\mathrm{A/I}} \Rightarrow [a]_\mathrm{I} = 0_{\mathrm{A/I}} \text{ ou } [b]_\mathrm{I} = 0_{\mathrm{A/I}} \\ &\Leftrightarrow \forall \alpha, \beta \in \mathrm{A/I}, \alpha\beta = 0 \Rightarrow \alpha = 0 \text{ ou } \beta = 0 \\ &\Leftrightarrow \mathrm{A/I\ intègre.}\end{aligned}$$

   (La troisième équivalence vient du fait que tout élément de A/I s'écrit par définition $[a]_\mathrm{I}$ pour un certain élément $a \in \mathrm{A}$.)
3. Notons $p : \mathrm{A} \to \mathrm{A/I}$ la surjection canonique. On sait qu'il existe une correspondance bijective

$$\begin{array}{ccc}\{\text{idéaux de A/I}\} & \to & \left\{\text{idéaux K} \subseteq \mathrm{A} \,\middle|\, \mathrm{K} \supseteq \mathrm{I}\right\} \\ \mathrm{J} & \mapsto & p^{-1}[\mathrm{J}]\end{array}.$$

   Puisque l'hypothèse « I maximal » signifie exactement que l'ensemble de droite possède exactement deux éléments, I et A, on obtient l'équivalence

$$\mathrm{I\ maximal} \Leftrightarrow \mathrm{A/I\ a\ 2\ idéaux,\ A/I\ et\ \{0\}}.$$

   Or, cette dernière propriété est équivalente au fait que A/I soit un corps : si K est un corps, il n'est pas réduit à l'anneau nul et tout idéal non trivial J contient un élément non nul, donc inversible, donc $\mathrm{J} = \mathrm{K}$. Réciproquement, si un anneau B a deux idéaux, {0} et B, il n'est pas réduit à l'anneau nul et tout élément non nul $b \in \mathrm{B}$ est inversible, puisque $(b) = \mathrm{B}$.

Puisqu'un corps est en particulier un anneau intègre, il s'ensuit une nouvelle démonstration de la première question.

Exercice 2. Soit K un corps.

1. Comme on l'a vu à l'exercice précédent, tout corps a 2 idéaux, {0} et K lui-même.
2. Soit $f : \mathrm{K} \to \mathrm{A}$ un morphisme d'anneaux. Son noyau $\ker f$ est un idéal de K. Puisqu'on a supposé que les anneaux n'étaient pas nuls et que les morphismes préservaient les unités des anneaux, le morphisme f ne peut pas être nul. En particulier, $\ker f \neq \mathrm{K}$. Il s'ensuit $\ker f = \{0\}$: f est injectif.

Exercice 3. Pour tout $b \in \mathrm{A}$, on a les équivalences

$$\begin{aligned}&(a) \subseteq (b) \Leftrightarrow b \text{ divise } a\ ; \\ &(a) = (b) \Leftrightarrow a \text{ et } b \text{ sont associés, i.e. } \exists u \in \mathrm{A}^\times : b = au\ ; \\ &(b) = \mathrm{A} \Leftrightarrow b \in \mathrm{A}^\times.\end{aligned}$$

Cela démontre que a est irréductible si et seulement si

$$\forall b \in \mathrm{A}, (a) \subseteq (b) \Rightarrow (a) = (b) \text{ ou } (b) = \mathrm{A},$$

c'est-à-dire que b est inversible parmi les idéaux principaux.
Traitons la question à l'envers : l'anneau $\mathbf{C}[\mathrm{X}]$ est principal. La question précédente entraîne donc que les idéaux maximaux de $\mathbf{C}[\mathrm{X}]$ sont les (P), où P est un élément irréductible. Autrement dit, l'ensemble des idéaux maximaux de $\mathbf{C}[\mathrm{X}]$ est

$$\operatorname{Spm} \mathbf{C}[\mathrm{X}] = \left\{ \mathfrak{m}_z = (\mathrm{X} - z) \subseteq \mathrm{A} \,\middle|\, z \in \mathbf{C} \right\}.$$

L'anneau $\mathbf{C}[\mathrm{X}]$ étant intègre, l'idéal nul est premier.
On a en fait trouvé ainsi tous les idéaux premiers : d'après ce qui précède, si un idéal de $\mathbf{C}[\mathrm{X}]$ n'est ni nul, ni maximal, il s'écrit $\mathrm{I} = (\mathrm{P})$, où P est un polynôme réductible. Si $\mathrm{P} = \mathrm{P}_1\mathrm{P}_2$ est une factorisation non triviale de P (c'est-à-dire que ni P_1 ni P_2 n'est inversible), on a $\mathrm{P}_1 \notin (\mathrm{P})$, $\mathrm{P}_2 \notin (\mathrm{P})$ et pourtant $\mathrm{P}_1\mathrm{P}_2 = \mathrm{P} \in \mathrm{P}$, ce qui entraîne la non-primalité de (P). L'ensemble des idéaux maximaux de $\mathbf{C}[\mathrm{X}]$ est donc

$$\operatorname{Spec} \mathbf{C}[\mathrm{X}] = \left\{ \mathfrak{m}_z = (\mathrm{X} - z) \subseteq \mathrm{A} \,\middle|\, z \in \mathbf{C} \right\} \cup \{(0)\}.$$

Exercice 4. Soit $\mathrm{A}[\mathrm{X}]$ l'anneau des polynômes à une variable.

1. On effectue la preuve par récurrence sur $\deg \mathrm{P}$, le cas $\deg \mathrm{P} = 0$ étant évident. On peut en outre supposer $\deg \mathrm{P} \geq \deg \mathrm{D}$ (dans le cas contraire, $\mathrm{Q} = 0$ et $\mathrm{R} = \mathrm{P}$ conviennent).
   Écrivons
   $$\mathrm{P} = \sum_{k=0}^{n} p_k \mathrm{X}^k \qquad \text{et} \qquad \mathrm{D} = \sum_{k=0}^{m} d_k \mathrm{X}^k$$
   (on suppose $n = \deg \mathrm{P}$ et $m = \deg \mathrm{D}$, de telle sorte que l'hypothèse de l'énoncé est $d_m \in \mathrm{A}^\times$.)
   On peut alors écrire
   $$\mathrm{P} = a_n d_m^{-1} \mathrm{X}^{n-m} \mathrm{D} + \mathrm{P}_1,$$
   avec $\deg \mathrm{P}_1 < \deg \mathrm{P}$. D'après l'hypothèse de récurrence, il existe $\mathrm{Q}_1, \mathrm{R}_1 \in \mathrm{A}[\mathrm{X}]$ tels que
   $$\mathrm{P}_1 = \mathrm{Q}_1 \mathrm{D} + \mathrm{R}_1 \qquad \text{et} \qquad \deg \mathrm{R}_1 < \deg \mathrm{D}.$$
   On obtient donc
   $$\mathrm{P} = \left(a_n d_m^{-1} \mathrm{X}^{n-m} + \mathrm{Q}_1 \right) \mathrm{D} + \mathrm{R}_1.$$
2. Soit
   $$\mathrm{P} = \sum_{k=0}^{n} p_k \mathrm{X}^k \qquad \text{et} \qquad \mathrm{Q} = \sum_{k=0}^{m} q_k \mathrm{X}^k$$
   deux polynômes non nuls (on suppose $p_n \neq 0$ et $q_m \neq 0$, de telle sorte que $n = \deg \mathrm{P}$ et $m = \deg \mathrm{Q}$). On a alors
   $$\mathrm{PQ} = \sum_{k=0}^{n+m} \left(\sum_{i+j=k} p_i q_j \right) \mathrm{X}^k.$$
   Comme A est intègre, $\displaystyle\sum_{i+j=n+m} p_i q_j = p_n q_m \neq 0$, ce qui montre
   $$\deg \mathrm{PQ} = n + m = \deg \mathrm{P} + \deg \mathrm{Q}.$$

(a) D'après ce qui précède, si P et Q sont deux polynômes dont le produit est une constante (c'est-à-dire un élément de degré nul), les deux polynômes sont eux-même de degré nul. Il s'ensuit que les décompositions de $a \in \mathrm{A}$ dans A[X] sont les mêmes que celles dans A. En particulier, si $a \in \mathrm{A}$ est irréductible, il le reste dans A[X].

(b) On copie la preuve d'Euclide : si $p_1, \dots, p_n \in \mathrm{A}[\mathrm{X}]$ sont un nombre fini d'irréductibles, le polynôme $p_1 \cdots p_n + 1$ est congru à 1 modulo chacun des p_i et, de degré $\deg p_1 + \cdots + \deg p_n$, il ne peut pas être inversible. En particulier, chacun de ses facteurs irréductibles est différent des (p_i), ce qui montre qu'aucune collection finie n'épuise l'ensemble des irréductibles de A[X].

Si A est un anneau factoriel, A[X] reste factoriel et la même preuve fonctionne à peu près : le seul problème est qu'*a priori*, $p_1 \cdots p_n + 1$ pourraît être inversible (il faudrait en particulier que tous les p_i soient des constantes). Pour éviter ce problème, il suffit de choisir $p_1 = \mathrm{X}$.

Remarques.

– La preuve d'Euclide donne une infinité d'éléments irréductibles **deux à deux non associés** dans **Z** et dans K[X]. Tous les anneaux ne vérifient pas cette propriété. Par exemple, soit p un nombre premier et

$$\mathbf{Z}_{(p)} = \left\{ \frac{a}{b} \,\middle|\, a \in \mathbf{Z} \text{ et } b \in \mathbf{N}^* \text{ premier avec } p \right\} \subseteq \mathbf{Q}.$$

On peut montrer que dans cet anneau, les éléments non inversibles forment l'idéal $(p) = p\mathbf{Z}_{(p)}$. (On dit que l'anneau est *local*.) Cela entraîne que les éléments irréductibles sont exactement les pu, avec $u \in \mathbf{Z}_{(p)}^{\times}$: ils sont tous associés (mais ils sont quand même en nombre infini).
On voit d'ailleurs sur cet exemple pourquoi la preuve d'Euclide échoue : si on part de l'élément irréductible $p_1 = p$, l'élément $p+1$ est inversible et la preuve s'arrête là.
Les mêmes remarques restent vraie, *mutatis mutandis*, dans l'anneau

$$\mathrm{K}[[\mathrm{X}]] = \left\{ \sum_{i=0}^{+\infty} a_i \mathrm{X}^i \,\middle|\, a_i \in \mathrm{K} \right\}$$

muni des addition et multiplication standard (dans ce cas, les éléments irréductibles sont tous associés à X).

– En revanche, une variante de la preuve d'Euclide montre que dans tout anneau factoriel qui ne soit pas un corps, il y a une infinité d'éléments irréductibles (éventuellement associés entre eux) : soit A un anneau factoriel qui ne soit pas un corps (en particulier, il possède un élément irréductible $p_1 \in \mathrm{A}$).
Si A a une infinité d'unités, le résultat est démontré : les $(u p_1)_{u \in \mathrm{A}^\times}$ forment une infinité d'éléments irréductibles tous distincts (mais tous associés). On peut donc supposer que $\mathrm{A}^\times$ est fini. Sous cette hypothèse, on va faire marcher une preuve à la Euclide, qui construit, étant donné une collection finie d'irréductibles, un irréductible absent de la liste (et qui construit donc par récurrence une infinité d'irréductibles).
Soit donc $p_1, \dots, p_n$ une liste d'irréducibles distincts et soit $a = p_1 \cdots p_n$. Considérons les éléments

$$1 + a^i, \qquad i \in \mathbf{N}^*.$$

Aucun des $1+a^i$ n'est nul (cela entraînerait que a, et donc p_i, soit une unité, ce qui est exclu). Pour la même raison, aucun des a^i ne vaut 1. Les $1 + a^i$ sont par ailleurs tous distincts : si $i < j$,

$$(1 + a^j) - (1 + a^i) = a^j - a^i = a^i(a^{j-i} - 1) \neq 0.$$

D'après le principe des tiroirs, il existe $n \in \mathbf{N}^*$ tel que $1+a^n$ ne soit pas une unité. Il a donc un diviseur irréductible p_{n+1} qui ne peut pas être dans la liste $p_1, \dots, p_n$, car tous ces éléments divisent a. Cela conclut la preuve.

(c) Soit $P = Q_1 D + R_1 = Q_2 D + R_2$ deux divisions euclidiennes. On a alors

$$(Q_1 - Q_2)D = R_2 - R_1.$$

Le deuxième terme de cette égalité est de degré strictement inférieur à $\deg D$ alors que le premier est un multiple de D. Si $Q_1 \neq Q_2$, on obtient alors une contradiction en comparant les degrés. On a donc $Q_1 = Q_2$ et $R_1 = R_2$.

3. Dans K[X], l'hypothèse d'inversibilité du coefficient dominant est évidemment vide. On peut donc toujours effectuer la division euclidienne, ce qui montre que K[X] est euclidien (de stathme deg) et donc principal.

4. Dans K[X], le pgcd peut se calculer via l'algorithme d'Euclide. Celui-ci ne fait intervenir que des polynômes de K[X]. En particulier, le pgcd de deux polynômes est le même dans tous les L[X], où L est un corps contenant les coefficients des deux polynômes.

   Si $K \subseteq L$ sont deux corps, un polynôme de K[X] irréductible dans L[X] reste irréductible dans K[X] : si $P = P_1 P_2$ est une factorisation non triviale dans K[X], cela donne une factorisation non triviale dans L[X]. La réciproque est évidemment fausse : le polynôme $X^2 - 2$ est irréductible dans $\mathbf{Q}$[X] mais pas dans $\mathbf{R}$[X], le polynôme $X^2 + 1$ est irréductible dans $\mathbf{R}$[X] mais pas dans $\mathbf{C}$[X]...

Exercice 5. Si un polyôme P (de degré ≥ 2) a une racine $a \in K$, il est divisible (dans K[X] ou dans tout L[X], pour $L \supseteq K$) par le polynôme $(X-a)$. Ainsi, sur tout corps, avoir une racine est équivalent à être divisible par un polynôme de degré 1 (en particulier, cela empêche tout polynôme de degré ≥ 2 d'être irréductible).
Mais les seules factorisations non triviales d'un polynôme de degré 2 sont de la forme $P = \ell_1 \ell_2$ avec $\deg \ell_1 = \deg \ell_2 = 2$ et les seules factorisations possibles d'un polynôme de degré 3 sont de la forme $P = \ell_1 \ell_2 \ell_3$ (avec $\deg \ell_i = 1$) ou $P = Q\ell$ (avec $\deg Q = 2$ et $\deg \ell = 1$). Dans tous les cas, un polynôme réductible a une racine, ce qui démontre le résultat.
Le polynôme $P = (X^2+1)(X^2-2)$ est réductible sur $\mathbf{Q}$ mais il n'y a pas de racines (ses racines complexes sont $\pm i$ et $\pm\sqrt{2}$, qui n'appartiennent pas à $\mathbf{Q}$).

Exercice 6.

1. Si $(X-a)^2$ divise P, on peut écrire $P = (X-a)^2 Q$, avec $Q \in K[X]$. On a alors

$$\begin{aligned} P' &= 2(X-a)Q + (X-a)^2 Q' \\ &= (X-a)\left(2Q + (X-a)Q'\right) \end{aligned}$$

   donc $(X-a)$ divise bien P'.

2. Commençons par remarquer que la propriété précédente possède une espèce de réciproque : si α est à la fois une racine de P et de P', alors $(X-\alpha)^2$ divise P (c'est-à-dire que α est une racine multiple de P). En effet, la division euclidienne de P par $(X-\alpha)^2$ donne :

$$P = (X-\alpha)^2 Q + (\lambda(X-\alpha) + \mu).$$

   En évaluant en α, il vient $\mu = 0$. En dérivant, on obtient

$$P' = \left(2Q + (X-\alpha)Q'\right)(X-\alpha) + \lambda$$

   donc l'hypothèse $P'(\alpha) = 0$ entraîne $\lambda = 0$, ce qui montre que P est divisible par $(X-\alpha)^2$.

Ainsi, une racine multiple α de X^4+X+6 dans $\mathbf{F}_p$ est un élément $\alpha \in \mathbf{F}_p$ qui est à la fois racine de X^4+X+6 et de $4X^3+1$. Or, dans $\mathbf{Z}$, on a l'égalité

$$4\left(X^4+X+6\right) = \left(4X^3+1\right)X + (3X+24).$$

En réduisant modulo $p \neq 2$, on obtient que $\alpha \in \mathbf{F}_p$ est une racine double de X^4+X+6 si et seulement si $\alpha^4+\alpha+6=0$ et $3\alpha+24=0$ dans $\mathbf{F}_p$.
Pour $p \neq 2,3$, cela résout le problème : $3\alpha+24=0 \Leftrightarrow \alpha+8=0$ donc la seule racine double possible est $-8 \in \mathbf{F}_p$: Or, $(-8)^4-8+6=4094=2\cdot 23\cdot 89$. Les $p \neq 2,3$ répondant à la question sont donc 23 et 89.
Il suffit maintenant de traiter les cas $p=2$ et $p=3$ à la main. Or, la factorisation de X^4+X+6 en facteurs irréductibles est

$$\begin{aligned}
&\text{dans } \mathbf{F}_2 : X^4+X+6 = X^4+X = X(X^3+1) = X(X+1)(X^2+X+1)\,;\\
&\text{dans } \mathbf{F}_3 : X^4+X+6 = X^4+X = X(X^3+1) = X(X+1)^3.
\end{aligned}$$

Au final, X^4+X+6 a une racine double dans trois $\mathbf{F}_p$: $\mathbf{F}_3$, $\mathbf{F}_{23}$ et $\mathbf{F}_{89}$.

Exercice 7. On a

$$0 = P\left(\frac{a}{b}\right) = \sum_{i=0}^{n} a_i \frac{a^i}{b^i}$$

donc

$$0 = \sum_{i=0}^{n} a_i a^i b^{n-i}.$$

En particulier,

$$a_0 b^n = -a\left(\sum_{i=1}^{n} a_i a^{i-1} b^{n-i}\right) \qquad \text{et} \qquad a_n a^n = -b\left(\sum_{i=0}^{n-1} a_i a^i b^{n-i-1}\right).$$

Cela entraîne que a divise $a_0 b^n$ et que b divise $a_n a^n$. Puisque a et b sont premiers entre eux, cela entraîne que a divise a_0 et que b divise a_n. Si P est unitaire, cette dernière propriété entraîne que les racines de P dans K ont un dénominateur inversible, c'est-à-dire qu'elles sont en fait dans A. (On dit qu'un anneau factoriel est *intégralement clos*.)

Exercice 8. Comme d'habitude, on va utiliser la formule

$$(a^2+b^2)(c^2+d^2) = (ac-bd)^2+(ad+bc)^2$$

(qui vient par exemple de la multiplicativité du module d'un nombre complexe) pour garantir que l'ensemble des sommes de carrés est stable par produit.
Tout polynôme de $\mathbf{R}[X]$ se factorise sous la forme

$$P(X) = a\prod_{i=1}^{n}(X-x_i)^{r_i}\prod_{j=1}^{m}(X^2+2b_jX+c_j)^{s_j}$$

(où $a \in \mathbf{R}^\times$, $(x_i)_{i=1}^n \in \mathbf{R}^n$, $(r_i)_{i=1}^n \in (\mathbf{N}^*)^n$, $(s_j)_{j=1}^m \in (\mathbf{N}^*)^m$ et $(b_j)_{j=1}^m, (c_j)_{j=1}^m \in \mathbf{R}^m$ vérifient $b_j^2 - c_j > 0$).

Si P ne prend que des valeurs positives, l'analyse du signe de P au voisinage de $\pm\infty$ et des racines réelles x_i montre que $a > 0$ et que les (r_i) sont pairs. En particulier, le facteur réel

$$a\prod_{i=1}^{n}(\mathrm{X}-x_i)^{r_i}$$

est un carré. Il suffit donc de démontrer que chacun des facteurs imaginaires $\mathrm{X}^2+2b\mathrm{X}+c$ $(b^2<c)$ est une somme de carrés. Or,

$$\mathrm{X}^2+2b\mathrm{X}+c=(\mathrm{X}+b)^2+(c-b^2)=(\mathrm{X}+b)^2+\left(\sqrt{c-b^2}\right)^2.$$

Variante : puisque a est positif et les (r_i) sont pairs, on peut obtenir la décomposition en somme de deux carrés d'une autre façon : choisissons, pour $j\in[\![1,m]\!]$, une racine complexe z_j de $\mathrm{X}^2+2b_j\mathrm{X}+c_j$ et posons

$$\mathrm{U}=\sqrt{a}\prod_{i=1}^{n}(\mathrm{X}-x_i)^{r_i/2}\prod_{j=1}^{m}(\mathrm{X}-z_i)^{s_j}\in\mathbf{C}[\mathrm{X}].$$

On a alors $\mathrm{P}=\mathrm{U}\overline{\mathrm{U}}$. En écrivant $\mathrm{U}=\mathrm{R}+i\mathrm{S}$, avec $\mathrm{R},\mathrm{S}\in\mathbf{R}[\mathrm{X}]$, on obtient

$$\mathrm{P}=\mathrm{U}\overline{\mathrm{U}}=(\mathrm{R}+i\mathrm{S})(\mathrm{R}-i\mathrm{S})=\mathrm{R}^2+\mathrm{S}^2.$$

Exercice 9.

1. Si $a\in\mathrm{K}^\times$ et $b\in\mathrm{K}$, l'application

$$\begin{array}{ccc}\mathrm{K}[\mathrm{X}] & \to & \mathrm{K}[\mathrm{X}]\\ \mathrm{P} & \mapsto & \mathrm{P}(a\mathrm{X}+b)\end{array}$$

est un morphisme d'anneaux. C'est même un automorphisme : son inverse est donné par $\mathrm{Q}\mapsto\mathrm{Q}(a^{-1}\mathrm{X}-a^{-1}b)$. En particulier, il envoie irréductible sur irréductible.

Remarque : on peut même dire mieux : le groupe affine $\mathrm{GA}_1(\mathrm{K})=\left\{x\mapsto ax+b\,\middle|\,a\in\mathrm{K}^\times,b\in\mathrm{K}\right\}$, que l'on peut aussi voir comme le groupe de matrices

$$\left\{\begin{pmatrix}a & b\\ 0 & 1\end{pmatrix}\,\middle|\,a\in\mathrm{K}^\times,b\in\mathrm{K}\right\}\subseteq\mathrm{GL}_2(\mathrm{K})$$

opère sur $\mathrm{K}[\mathrm{X}]$ par automorphismes. On peut par exemple voir que si $\mathrm{K}=\mathbf{R}$, on obtient ainsi tous les automorphismes.

2. Supposons par l'absurde que P ait deux racines complexes $\alpha,\alpha'\in\mathbf{C}$ telles que $r=\alpha'-\alpha\in\mathbf{Q}^\times$. Le polynôme $\mathrm{Q}=\mathrm{P}(\mathrm{X}+r)-\mathrm{P}(\mathrm{X})$ est encore dans $\mathbf{Q}[\mathrm{X}]$ et, le coefficient dominant de $\mathrm{P}(\mathrm{X}+r)$ étant le même que celui de P, on a $\deg\mathrm{Q}<\deg\mathrm{P}$. En outre, Q et P ont une racine commune : $\mathrm{Q}(\alpha)=\mathrm{P}(\alpha+r)-\mathrm{P}(\alpha)=\mathrm{P}(\alpha')-\mathrm{P}(\alpha)=0$. Si Q est non nul, cela entraîne que leur pgcd (dans $\mathbf{C}[\mathrm{X}]$, mais on sait que c'est le même que dans $\mathbf{Q}[\mathrm{X}]$) est non trivial, ce qui contredit l'irréductibilité de P. On a donc $\mathrm{Q}=0$, c'est-à-dire que $\mathrm{P}(\mathrm{X}+r)=\mathrm{P}(\mathrm{X})$. Cela fournit une infinité de racines $\alpha+kr, k\in\mathbf{Z}$ et donc une contradiction.

Exercice 10.

1. C'est une petite manipulation sur les coefficients. Le plus simple est peut-être d'introduire la fonction *valuation (en 0)* $v:\mathrm{A}[\mathrm{X}]\to\mathbf{N}\cup\{+\infty\}$:

$$v\left(\sum_{i=0}^{n}a_i\mathrm{X}^i\right)=\min\left\{i\in\mathbf{N}\,\middle|\,a_i\neq0\right\}.$$

Cette fonction vérifie évidemment $\forall P \in A[X] \setminus \{0\}, \nu(P) \leq \deg(P)$, et l'égalité a lieu exactement pour les monômes. Si A est intègre, on a la propriété $\nu(PQ) = \nu(P) + \nu(Q)$ exactement de la même façon que la propriété duale $\deg(PQ) = \deg P + \deg Q$.

Revenons au critère d'Eisenstein : supposons que

$$P_1 = \sum_{i=0}^{r} b_i X^i \text{ et } P_2 = \sum_{i=0}^{s} c_i X^i$$

soient des éléments de A[X] de degré r et s tels que $P = P_1 P_2$. Par hypothèse, la réduction $\overline{P}$ de P dans (A/I)[X] est un monôme $\overline{a}_n X^n$ et vérifie donc $\deg \overline{P} = \nu(\overline{P}) = n$. D'après les propriétés d'additivité du degré et de la valuation évoquées plus haut, on a donc nécessairement que $\overline{P}_1$ et $\overline{P}_2$ sont également des monômes. Puisque $0 \neq \overline{a}_n = \overline{b}_r \cdot \overline{c}_s$, on a même que $\overline{P}_1$ et $\overline{P}_2$ sont des monômes de degré $r = \deg P_1$ et $s = \deg P_2$, respectivement. Or, puisque $a_0 = b_0 c_0 \notin I^2$, on a nécessairement $\overline{b_0} \neq 0$ ou $\overline{c}_0 \neq 0$, ce qui entraîne $r = 0$ ou $s = 0$, et donc que P_1 ou P_2 est une constante.

2. Le polynôme $2X^2 - 6 = 2\left(X^2 - 3\right)$ est manifestement réductible dans $\mathbf{Z}[X]$. Il vérifie pourtant les conditions pour l'idéal premier $(3) \subseteq \mathbf{Z}$.

   Remarque. C'est évidemment le seul genre de problèmes qui peut survenir : si $P \in A[X]$ vérifie le critère d'Eisenstein, il n'est réductible dans A[X] que s'il existe un non-inversible de A divisant tous ses coefficients (c'est ce que dit la proposition précédente).

3. C'est une des versions du lemme de Gauß.

   Écrivons une décomposition de P dans K[X] : $P = \widetilde{P}_1 \cdot \widetilde{P}_2$. On peut trouver des éléments Δ_i de A tels que les produits $\Delta_i \widetilde{P}_i$ soient des polynômes de A[X]. On a donc une décomposition dans A[X] : $\Delta_1 \Delta_2 P = (\Delta_1 \widetilde{P}_1)(\Delta_2 \widetilde{P}_2)$. Le lemme de Gauß implique donc que $\operatorname{cont}(\Delta_1 \Delta_2 P) = \Delta_1 \Delta_2 \operatorname{cont}(P)$ est associé au produit $\operatorname{cont}(\Delta_1 P_1)\operatorname{cont}(\Delta_2 P_2)$. On a donc

   $$P = \operatorname{cont}(P)\frac{\Delta_1 \Delta_2 P}{\operatorname{cont}(\Delta_1 \Delta_2 P)} = \operatorname{cont}(P)\frac{\Delta_1 \widetilde{P}_1}{\operatorname{cont}(\Delta_1 \widetilde{P}_1)}\frac{\Delta_2 \widetilde{P}_2}{\operatorname{cont}(\Delta_2 \widetilde{P}_2)},$$

   ce qui est une décomposition dans A[X].

   D'après ce qui précède, cette décomposition fait intervenir un polynôme de degré 0, disons $P_1 = \Delta_1 \widetilde{P}_1 / \operatorname{cont}(\Delta_1 \widetilde{P}_1)$. Le polynôme $\widetilde{P}_1 \in K[X]$ est donc lui aussi de degré 0 et c'est donc un inversible de K[X]. La factorisation de départ était triviale, et P est bien irréductible dans K[X].

   Remarque. Le fait que si un polynôme de A[X] se factorise dans K[X], il se factorise également dans A[X] est un apport crucial du lemme de Gauß. C'est faux dans un anneau intègre général : par exemple, le polynôme

   $$X^2 - X - 1 = \left(X - \frac{1+\sqrt{5}}{2}\right) \cdot \left(X - \frac{1-\sqrt{5}}{2}\right)$$

   est irréductible sur $A = \mathbf{Z}[\sqrt{5}]$ mais réductible sur $K = \mathbf{Q}(\sqrt{5}) = \operatorname{Frac} A$.

4. Notons $\Phi_p(X) = X^{p-1} + X^{p-2} + \cdots + X + 1$. Évidemment, Φ_p est irréductible si et seulement si $\Phi_p(X+1)$ l'est. Or,

   $$\Phi_p(X) = \frac{X^p - 1}{X - 1}$$

   donc

   $$\Phi_p(X+1) = \frac{(X+1)^p - 1}{(X+1) - 1} = X^{p-1} + pX^{p-2} + \binom{p}{2} X^{p-2} + \cdots + pX.$$

   Et le critère d'Eisenstein pour $I = (p)$ s'applique directement.

5. Le polynôme X^2+1 est irréductible dans $\mathbf{Q}[X]$ (il l'est même dans $\mathbf{R}[X]$). L'idéal $I=(X^2+1)\subseteq \mathbf{Q}[X]$ est donc premier. On peut ainsi appliquer le critère d'Eisenstein à $A=\mathbf{Q}[X]$, ce qui montre que le polynôme

$$P(X,Y)=Y^2+(X^2+1)^2Y+(X^2+1)\in \mathbf{Q}[X,Y]=(\mathbf{Q}[X])[Y]$$

est irréductible dans $\mathbf{Q}(X)[Y]$. Or, vu comme polynôme en Y, ce polynôme est unitaire. D'après le lemme de Gauß, il est donc irréductible dans $A[Y]=\mathbf{Q}[X,Y]$.

6. Remarquons déjà que le critère d'Eisenstein (couplé au lemme de Gauß pour passer de l'irréductibilité sur $\mathbf{Q}$ à l'irréductibilité sur $\mathbf{Z}$) montre directement que X^n-p est irréductible sur $\mathbf{Z}$.

   La difficulté est que l'élément p ne reste pas toujours irréductible sur $\mathbf{Z}[i]$. En effet, on rappelle que

$$p\in\mathbf{Z}[i] \text{ réductible} \Leftrightarrow \exists (n,m)\in\mathbf{Z}^2 : p=n^2+m^2 \Leftrightarrow p=2 \text{ ou } p\equiv 1 \pmod 4$$

   et que dans ce cas, on peut écrire $(p)=(n+im)(n-im)$. Ainsi, on a deux cas :
   - $p\equiv -1 \pmod 4$; dans ce cas, p reste irréductible, l'idéal (p) reste premier et le critère d'Eisenstein s'applique directement.
   - $p\equiv -1 \pmod 4$; dans ce cas, p s'écrit comme le produit de $n+im$ et $n-im$, deux nombres *non associés* (les inversibles de $\mathbf{Z}[i]$ sont ± 1 et $\pm i$: si les deux nombres étaient associés, on aurait $n=\pm m$, ce qui impliquerait $p=2n^2$, ce qui est impossible). Les entiers de Gauß $n\pm im$ sont bien irréductibles sur $\mathbf{Z}[i]$ (leur norme est égale à p). On peut alors appliquer le critère d'Eisenstein à l'idéal premier $(n+im)$.