Exercice 1 (idéaux et quotients).

1. $\boxed{\Longrightarrow}$ *Micro analyse* : si I est un tel idéal, on a à $a\in A$ fixé les équivalences $a\in I\iff a-0\in I\iff a\equiv 0\iff a\in\overline{0}$, d'où l'égalité $I=\overline{0}$. *Fin de l'analyse.* Définissons $I:=\overline{0}$ et montrons que ce dernier est un idéal de A. On aura alors (pour tout $a,b\in A$) d'une part les implications

$$a\equiv b\iff\overline{a}=\overline{b}\Longrightarrow\overline{a}+\overline{-b}=\overline{b}+\overline{-b}\iff\overline{a+(-b)}=\overline{b+(-b)}\iff\overline{a-b}=\overline{0}\iff a-b\in\overline{0}\iff a-b\in I$$

d'autre part les implications

$$a-b\in I\iff\overline{a-b}=\overline{0}\Longrightarrow\overline{a-b}+\overline{b}=\overline{0}+\overline{b}\iff\overline{(a-b)+b}=\overline{0+b}\iff\overline{a}=\overline{b}\iff a\equiv b\text{, ce qui conclura.}$$

Montrons que I est un sous-groupe additif. On a déjà l'appartenance $0\in\overline{0}=I$. Soient $i,j\in I$: alors d'une part $\overline{i+j}=\overline{i}+\overline{j}=\overline{0}+\overline{0}=\overline{0+0}=\overline{0}$, d'où $i+j\in I$, d'autre part $\overline{-i}=\overline{0+(-i)}=\overline{0}+\overline{-i}=\overline{i}+\overline{-i}=\overline{i+(-i)}=\overline{0}$, d'où $-i\in I$.

Montrons $AI\subset I$. Soit $(a,i)\in A\times I$. Multiplier les égalités $\begin{cases}\overline{a+i}=\overline{a}\\ \overline{0}=\overline{i}\end{cases}$ donne $\overline{(a+i)\times 0}=\overline{a\times i}$, *i. e.* $\overline{ai}=\overline{0}$, ou encore $ai\in I$.

$\boxed{\Longleftarrow}$ Soit I un idéal comme dans l'énoncé. Soient $a,a',b,b'\in A$ tels que $\begin{cases}a\equiv a'\\ b\equiv b'\end{cases}$. Soient $i_a,i_b\in I$ tels que $\begin{cases}a'-a=i_a\\ b'-b=i_b\end{cases}$. On a alors d'une part les égalités

$$\overline{a'+b'}=(a'+b')+I=(a+i_a)+(b+i_b)+I=(a+b)+\overbrace{\underbrace{i_a+i_b}_{\in I}+I}^{=I}=a+b+I=\overline{a+b},$$

d'autre part les égalités

$$\overline{a'b'}=a'b'+I=(a+i_a)(b+i_b)+I=ab+\underbrace{ai_b}_{\in I}+\underbrace{i_ab}_{\in I}+\underbrace{i_ai_b}_{\in I}+I=ab+I=\overline{ab}\text{, ce qui conclut.}$$

On se place dans le cas décrit. On raisonne par transfert de structure : tous les axiomes de l'anneau A passent "sous la barre", par exemple la distributivité en écrivant (à $a,b,c\in A$ fixés)

$$\overline{a}\times\left(\overline{b}+\overline{c}\right)=\overline{a}\times\left(\overline{b+c}\right)=\overline{a\times(b+c)}=\overline{a\times b+a\times c}=\overline{a}\times\overline{b}+\overline{a}\times\overline{c}.$$

Les autres axiomes se traitent de même : $+$ est associatif, $\overline{0}$ est neutre additif, l'opposé d'un $\overline{a}$ est $\overline{-a}$, $\times$ est associatif, $\overline{1}$ est neutre multiplicatif.

2. Toutes les classes sont des translatées de I ; or les translations d'un groupe (ici $(A,+)$) sont bijectives, ce qui conclut. Puisque A est la réunion de $\left|{}^{A}\!/_{I}\right|$ classes $a+I$ chacune de cardinal I, on a les égalités suivantes lorsque A est fini :

$$|A|=\sum_{C\in{}^{A}\!/_{I}}|C|=\sum_{C\in{}^{A}\!/_{I}}|I|=|I|\sum_{C\in{}^{A}\!/_{I}}1=|I|\left|{}^{A}\!/_{I}\right|,\ c.\ q.\ f.\ d..$$

3. Il est clair que de tels produits sont des idéaux. Réciproquement, notons I_A et I_B les projections d'un idéal I de $A\times B$ sur A et B respectivement. Ce sont des idéaux en vertu de la surjectivité de ces projections. Alors l'injection canonique $I\hookrightarrow I_A\times I_B$ (produit de ces projections) est surjective : pour $(a,b)\in I_A\times I_B$, il y a un $(\alpha,\beta)\in A\times B$ tel que (a,β) et (α,b) sont dans I, donc leur produit par $(0,1)$ et $(1,0)$ sont aussi dans I, à savoir $(a,0)$ et $(0,b)$, donc leur somme (a,b) également, *c. q. f. d.*[1]

4. (pour se donner confiance en le résultat à montrer, se souvenir de l'égalité $\frac{a\times b}{i\times j}=\frac{a}{i}\times\frac{b}{j}$ dans les rationnels)
Soit $I\times J$ un idéal de $A\times B$. L'application considérée sera bien définie si deux éléments de $A\times B$ différant d'un élément de $I\times J$ ont même image par la surjection $s:\begin{cases}A\times B&\twoheadrightarrow&{}^{A}\!/_{I}\times{}^{B}\!/_{J}\\ (a,b)&\longmapsto&\left(\overline{a},\widehat{b}\right)\end{cases}$. On vérifie donc pour tout $(a,a',b,b',i,j)\in A^2\times B^2\times I\times J$ tel que $\binom{a'}{b'}=\binom{a}{b}+\binom{i}{j}$ les égalités

$$s\begin{pmatrix}a'\\b'\end{pmatrix}-s\begin{pmatrix}a\\b\end{pmatrix}=s\left(\begin{pmatrix}a'\\b'\end{pmatrix}-\begin{pmatrix}a\\b\end{pmatrix}\right)=s\begin{pmatrix}i\\j\end{pmatrix}=\begin{pmatrix}\overline{i}\\\widehat{j}\end{pmatrix}=\begin{pmatrix}\overline{0}\\\widehat{0}\end{pmatrix}=0,\ c.\ q.\ f.\ d..$$

[1] On prendra garde que le résultat n'est pas vrai pour un produit infini. Ce qui précède montre qu'un tel idéal est compris entre la somme directe de ses projections et leur produit, mais les deux inclusions peuvent être strictes. Considérer par exemple, dans un anneau $\prod_{i\in I}A_i$, des idéaux I_i de chaque A_i et, pour toute partie $J\subset I$ infinie, l'idéal $\bigoplus_{j\in J}I_j\times\prod_{i\notin J}I_i$.

L'application considérée (notons-la $\widetilde{s}$) est clairement surjective (tout élément de ${}^{A}\!/_{I} \times {}^{B}\!/_{J}$ est de la forme $\left(\overline{a}, \widehat{b}\right) = s\left(a,b\right) = \widetilde{s}\left(\widetilde{(a,b)}\right)$) et son injectivité vient des implications (à $(a,b) \in A \times B$ fixé)

$$\begin{aligned}\widetilde{(a,b)} \in \operatorname{Ker} \widetilde{s} \quad &\Longrightarrow \quad \widetilde{s}\left(\widetilde{(a,b)}\right) = 0 \Longrightarrow \left(\overline{a}, \widehat{b}\right) = \left(\overline{0}, \widehat{0}\right) \Longrightarrow \left\{\begin{array}{l} a = 0 \mod I \\ b = 0 \mod J \end{array}\right. \\ &\Longrightarrow \quad \left\{\begin{array}{l} a \in I \\ b \in J \end{array}\right. \Longrightarrow (a,b) \in I \times J \Longrightarrow \widetilde{(a,b)} = 0.\end{aligned}$$

Remarque. Plus généralement, étant donnés un morphisme d'anneaux $f : A \longrightarrow B$ et deux idéaux I de A et J de B tels que $f(I) \subset J$, on montrerait que l'application $\left\{\begin{array}{ccc} {}^{A}\!/_{I} & \longrightarrow & {}^{B}\!/_{J} \\ \overline{a} & \longmapsto & \widetilde{f(a)} \end{array}\right.$ est bien définie et est un morphisme d'anneaux. En imposant $I := \operatorname{Ker} f$ et $J := \{0\}$, on en déduirait que l'application $\left\{\begin{array}{ccc} {}^{A}\!/_{\operatorname{Ker} f} & \stackrel{\sim}{\longrightarrow} & \operatorname{Im} f \\ \overline{a} & \longmapsto & f(a) \end{array}\right.$ est bien définie et est un isomorphisme d'anneaux. Ainsi aurait-il suffit de dire que le morphisme s est surjectif de noyau $I \times J$.

5. Soit J un idéal de A contenant I. D'une part, la partie ${}^{J}\!/_{I} = \{j + I \; ; \; j \in J\} \subset {}^{A}\!/_{I}$ contient le neutre additif $0 + I$ de ${}^{A}\!/_{I}$, d'autre part, pour tous $j, j' \in J$ et $a \in A$, on a

$$\overline{j} + \overline{a}\overline{j'} = \overline{j + aj'} \in {}^{J}\!/_{I} \text{ car } J \text{ est un idéal, d'où l'idéalité de } {}^{J}\!/_{I}.$$

Réciproquement, observons que toute partie $\mathcal{P} \subset {}^{A}\!/_{I}$ s'écrit $\mathcal{P} = {}^{\cup\mathcal{P}}\!/_{I}$. Ainsi, pour $\mathcal{J}$ idéal de ${}^{A}\!/_{I}$, il suffit de montrer que $J := \cup\mathcal{J}$ est un idéal de A. D'une part, $\mathcal{J}$ contient $\overline{0} \ni 0$, donc J contient 0. D'autre part, pour $j, j' \in J$ et $a \in A$, il y a des $\overline{u}, \overline{v} \in \mathcal{J}$ tels que $\left\{\begin{array}{l} j \in \overline{u} \\ j' \in \overline{v} \end{array}\right.$, d'où $j + ak \in \overline{u} + a\overline{v} \in \mathcal{J}$ par idéalité de ce dernier, d'où $j + ak \in J$, ce qui conclut.

6. (pour se donner confiance en le résultat à montrer, se souvenir de l'égalité $\frac{\frac{a}{i}}{\frac{j}{i}} = \frac{a}{i}$ dans les rationnels)

Apprécions la remarque du point 4. Puisque $I \subset J$, la projection modulo J passe au quotient par I, d'où une surjection $\left\{\begin{array}{ccc} {}^{A}\!/_{I} & \twoheadrightarrow & {}^{A}\!/_{J} \\ \overline{a} & \longmapsto & \widehat{a} \end{array}\right.$ de noyau ${}^{J}\!/_{I}$ vu les équivalences

$$\widehat{a} = 0 \Longleftrightarrow a \in J \Longleftrightarrow \overline{a} \in \overline{J} \Longleftrightarrow \overline{a} \in {}^{J}\!/_{I}.$$

7. Remarquer que le lemme chinois devient tautologique pour *un seul* idéal.

Montrons tout de suite l'énoncé concernant les noyaux : un élément est annulé par toutes les projections canoniques ssi il est nul modulo tous les idéaux, *i. e.* ssi il appartient à tous ces idéaux, *i. e.* ssi il appartient à leur intersection.

Regardons le cas de deux idéaux I et J étrangers. Soit $(i,j) \in I \times J$ tel que $1 = i + j$. On observe que, par la flèche $A \longrightarrow {}^{A}\!/_{I} \times {}^{A}\!/_{J}$, l'élément i est envoyé sur $\left(\overline{i}, \widehat{1-j}\right) = \left(\overline{0}, \widehat{1}\right)$ et que j est envoyé sur $\left(\overline{1-i}, \widehat{j}\right) = \left(\overline{1}, \widehat{0}\right)$, ce qui montre qu'un élément $\left(\overline{a}, \widehat{b}\right)$ est l'image de $aj + bi$, d'où la surjectivité.

Concluons par récurrence. Soit $n \geq 2$ un entier vérifiant le résultat pour n idéaux quelconques. Soient $I_0, I_1, ..., I_n$ des idéaux deux à deux étrangers. L'hypothèse de récurrence appliquée à $I_1, ..., I_n$ (et la remarque du point 4) nous donne un isomorphisme ${}^{A}\!/_{I_1 \cap \cdots \cap I_n} \cong {}^{A}\!/_{I_1} \times \cdots \times {}^{A}\!/_{I_n}$. Par ailleurs, si l'on montrait l'extranéité des idéaux I_0 et $I_1 \cap \cdots \cap I_n$, on aurait un isomorphisme

$${}^{A}\!/_{I_0 \cap (I_1 \cap \cdots \cap I_n)} \cong {}^{A}\!/_{I_0} \times {}^{A}\!/_{I_1 \cap \cdots \cap I_n} \underset{\text{précédent}}{\overset{\text{isomorphisme}}{\cong}} {}^{A}\!/_{I_0} \times \left({}^{A}\!/_{I_1} \times \cdots \times {}^{A}\!/_{I_n}\right), \text{ ce qui conclurait}$$

(bien vérifier que la composée ci-dessus agit comme le produit des $A \twoheadrightarrow {}^{A}\!/_{I_k}$). Soit $(a_k, i_k) \in I \times I_k$ tel que $a_k + i_k = 1$ pour tout $k \in \{1, ..., n\}$. Développer le produit $\prod (a_k + i_k)$ donne un terme $i_1 \cdots i_n \in I_1 \cap \cdots \cap I_n$ plus une somme de termes restant chacun dans I (puisque contenant un facteur $a_k \in I$), ce qui montre l'appartenance $1 = \prod (a_k + i_k) \in I + I_1 \cap \cdots \cap I_n$ et conclut la récurrence.

Montrons la réciproque par récurrence. (Le cas d'un seul idéal est tautologique.) Soient $I_1, ..., I_n$ des idéaux tels que la flèche $A \twoheadrightarrow \prod_{k=1}^{n} {}^{A}\!/_{I_k}$ soit surjective. On en déduit (en oubliant $n-2$ coordonnées) la surjectivité de n'importe quel flèche $A \twoheadrightarrow {}^{A}\!/_{I_k} \times {}^{A}\!/_{I_\ell}$, ce qui nous ramène au cas de deux idéaux. Soient donc I et J deux idéaux tels que la flèche $A \twoheadrightarrow {}^{A}\!/_{I} \times {}^{A}\!/_{J}$ soit surjective. Soit i un antécédent de $\left(\overline{0}, \widehat{1}\right)$ et posons $j := 1 - i$. L'abscisse montre que i est nul modulo I et l'ordonnée que j est nul modulo J, d'où l'appartenance $1 = i + j \in I + J$ et l'égalité $A = I + J$.

Exercice 2 (racines).

1. Un élément a est nilpotent ssi $\exists n \in \mathbf{N}^*,\ a^n = 0$, ce qui revient à dire $a \in \sqrt{0}$, d'où la première égalité.

   Soit $\overline{a}$ un nilpotent du quotient ${}^{A}\!/_{\sqrt{0}}$. Il y a donc un entier $n \geq 1$ tel que $\overline{a}^n = 0$ modulo $\sqrt{0}$, ce qui s'écrit $a^n \in \sqrt{0}$, d'où un entier m tel que $(a^n)^m = 0$, de sorte que a est nilpotent et sa classe $\overline{a}$ nulle (modulo $\sqrt{0}$).

2. Le sens $\Longrightarrow$ est trivial. Supposons réciproquement I stable par racine carrée. Soient $a \in A$ et $n \in \mathbf{N}^*$ tels que $a^n \in I$. Alors $a^{2^n} = a^n a^{2^n - n} \in I$, d'où par récurrence descendante (sur la puissance de 2) l'appartenance $a \in I$.

3. L'idéal nul est clairement radical puisque $\mathbf{Z}$ est intègre (réduit suffirait).

   Soit à présent $\mathfrak{r}$ un idéal radical non nul de $\mathbf{Z}$. Soit $r \in \mathbf{N}^*$ tel que $\mathfrak{r} = (r)$. Décomposons $r = \prod p_i^{v_i}$ en facteurs premiers. Si l'une des valuations v_{i_0} est ≥ 2, alors l'entier $p_{i_0} \prod_{i \neq i_0} p_i$ élevé à la puissance $\max v_i$ est multiple de r, donc a une puissance dans $\mathfrak{r}$, donc doit rester dans $\mathfrak{r} = (r)$, ce qui est impossible en regardant la valuation p_{i_0}-adique. Ainsi r est-il *quadratfrei* (sans facteur carré).

   Supposons réciproquement r quadratfrei et montre que (r) est radical. Soit $n \in \mathbf{Z}$ dont une puissance k-ième tombe dans (r). En termes de valuations, cette divisibilité $r \mid n^k$ s'écrit (pour tout premier $p \mid r$) $v_p(r) \leq k v_p(n)$, d'où $v_p(n) \geq \frac{v_p(r)}{k} = \frac{1}{k} > 0$ et $v_p(n) \geq 1$, ce qui montre que n est divisible par tous les premiers divisant r, donc par leur produit r, *c. q. f. d.*.

4. $\sqrt{I}$ contient les racines 1-èmes des éléments de I, donc contient I.

   Montrons que $\sqrt{I}$ est un idéal. Déjà $\sqrt{I}$ contient $0 \in I$. Soient ensuite $x, y \in \sqrt{I}$. Soient $p, q \in \mathbf{N}^*$ tels que $x^p, y^q \in I$. On a alors

$$\begin{aligned}
(x+y)^{p+q-1} &= \sum_{i+j=p+q-1} \binom{p+q-1}{i} x^i y^j \\
&= \sum_{i=0}^{p-1} \binom{p+q-1}{i} x^i y^{p+q-1-i} + \sum_{j=0}^{q-1} \binom{p+q-1}{j} x^{p+q-1-j} y^j \\
&= \left[\sum_{i=0}^{p-1} \binom{p+q-1}{i} x^i y^{p-1-i} \right] \underbrace{y^q}_{\in I} + \left[\sum_{j=0}^{q-1} \binom{p+q-1}{j} x^{q-1-j} y^j \right] \underbrace{x^p}_{\in I} \\
&\in I, \text{ d'où } x+y \in \sqrt{I}.
\end{aligned}$$

   De plus, pour tout $a \in A$ on a $(ax)^p = (a^p) x^p \in I$, d'où $ax \in \sqrt{I}$.

   Montrons que $\sqrt{I}$ est radical. On a déjà l'inclusion $\sqrt{I} \subset \sqrt{\sqrt{I}}$ d'après ce qui précède. Soit réciproquement $x \in \sqrt{\sqrt{I}}$. Soit $p \in \mathbf{N}^*$ tel que $x^p \in \sqrt{I}$. Soit $q \in \mathbf{N}^*$ tel que $(x^p)^q \in I$. Alors $x^{pq} \in I$, donc $x \in \sqrt{I}$, d'où l'inclusion réciproque.

   Soit enfin $\mathfrak{r}$ un idéal radical contenant I. Montrons $\sqrt{I} \subset \mathfrak{r}$. Soit $x \in \sqrt{I}$. Soit $n \in \mathbf{N}^*$ tel que $x^n \in I$. Puisque $I \subset \mathfrak{r}$, on obtient $x^n \in \mathfrak{r}$, d'où $x \in \sqrt{\mathfrak{r}} = \mathfrak{r}$.

5. Supposons tout idéal radical. Soit $a \in A$. Alors l'idéal $\left(a^2\right)$ est radical et contient a^2, donc a reste dans $\left(a^2\right)$, donc est multiple de son carré

   Supposons tout élément multiple de son carré. Montrons que I est radical. Soit $a \in A$ tel que $a^2 \in I$. Soit $\lambda \in A$ tel que $a = \lambda a^2$. On a tout de suite $a \in I$.

   Sont de tels anneaux (par exemple) les corps et les produits de corps.

6. La radicalité de I s'écrit $\forall n \in \mathbf{N}^*,\ \forall a \in A,\ a^n \in I \Longrightarrow a \in I$; or l'implication se réécrit $\overline{a^n} = \overline{0} \Longrightarrow \overline{a} = \overline{0}$, ou encore $\overline{a}^n = \overline{0} \Longrightarrow \overline{a} = \overline{0}$, *i. e.* ${}^{A}\!/_{I}$ est réduit.

7. Appliquer le point précédent lorsque $I = \{0\}$ et se souvenir que ${}^{A}\!/_{0}$ est isomorphe à A.

8. Soit ${}^{J}\!/_{I}$ un idéal de ${}^{A}\!/_{I}$ (une proposition précédente nous dit qu'il est de cette forme). On a alors les équivalences

$${}^{J}\!/_{I} \text{ est radical} \Longleftrightarrow \text{l'anneau } {}^{\left({}^{A}\!/_{I}\right)}\!/_{\left({}^{J}\!/_{I}\right)} \text{ est réduit} \Longleftrightarrow {}^{A}\!/_{J} \text{ est réduit} \Longleftrightarrow J \text{ est radical.}$$

9. Soit $a \in \sqrt{I}$. Soit $n \in \mathbf{N}^*$ tel que $a^n \in I$. Alors $a^n \in J$, d'où $a \in \sqrt{J}$.

10. Par une récurrence immédiate, on se ramène à montrer les inclusions désirées[2] pour $k = 2$. Soient donc I et J deux idéaux de A. On montre les trois inclusions

$$\sqrt{I}\sqrt{J} \subset \sqrt{I \cap J} \subset \sqrt{I} \cap \sqrt{J} \subset \sqrt{IJ} \subset \sqrt{I \cap J}.$$

[2] pour la première, il convient de préciser que la multiplication idéale est compatible avec $\subset$

La deuxième inclusion découle de la croissance de $\sqrt{\cdot}$ et de ce que l'inersection $I\cap J$ est incluse d'une part dans I (d'où $\sqrt{I\cap J}\subset\sqrt{I}$) d'autre part dans J (d'où $\sqrt{I\cap J}\subset\sqrt{J}$).

De même, le produit IJ reste d'une part inclus dans I (car ce dernier est un idéal) et d'autre part inclus dans J, d'où l'inclusion $IJ\subset I\cap J$. La croissance de $\sqrt{\cdot}$ fournit alors la quatrième inclusion.

Prenons un $a\in\sqrt{I}\cap\sqrt{J}$. On a deux entiers $n,m\geq 1$ tels que $\left\{\begin{array}{l} a^n\in I \\ a^m\in J\end{array}\right.$, d'où $a^{n+m}=a^na^m\in IJ$ et la conclusion $a\in\sqrt{IJ}$.

Soit enfin un produit ab tel que $a\in\sqrt{I}$ et $b\in\sqrt{J}$, disons $a^p\in I$ et $b^q\in J$. Alors $(ab)^{p+q}=a^p\left(a^qb^{p+q}\right)=b^q\left(b^pa^{p+q}\right)\in I\cap J$, donc $ab\in\sqrt{I\cap J}$: sommer de tels produits montre que $\sqrt{I}\sqrt{J}\subset\sqrt{I\cap J}$, d'où la première inclusion.

Contre exemple : $A=\mathbf{Z}$ et $I=(2)$. Alors $I^2=(4)$, $\sqrt{I^2}=(2)$ et $\sqrt{I}=(2)=I$, d'où $\sqrt{I}\sqrt{I}=(2)(2)=(4)\neq(2)=\sqrt{II}$.

11. Immédiat par le point précédent.

12. Vu les implications $i\neq j\implies E_{i,j}^2=0$ pour tous entiers $i,j\in\{1,2,...,n\}$, une sous-algèbre radicale de $M_n(\mathbf{K})$ doit contenir tous les $E_{i,j}$ pour $i\neq j$, donc leur produit $E_{i,j}E_{j,i}=E_{i,i}$, donc contient une base des matrices, donc vaut tout $M_n(\mathbf{K})$.

Exercice 3 (idéaux premiers).

1. D'une part l'inclusion stricte $\mathfrak{p}\subsetneq A$ équivaut à la non-nullité du quotient, d'autre part la seconde condition se traduit en termes d'égalité modulo $\mathfrak{p}$ en $\left(\overline{ab}=0\iff\overline{a}=0\text{ ou }\overline{b}=0\right)$.

2. Appliquer le point précédent à l'idéal nul et se souvenir que ${}^{A}\!/_{0}$ est isomorphe à A.

3. Soit ${}^{J}\!/_{I}$ un idéal de ${}^{A}\!/_{I}$. On a alors les équivalences

$$ {}^{J}\!/_{I}\text{ premier}\iff {}^{\left({}^{A}\!/_{I}\right)}\!/_{\left({}^{J}\!/_{I}\right)}\text{ intègre}\iff {}^{A}\!/_{J}\text{ intègre}\iff J\text{ premier.}$$

4. Supposons $\mathfrak{p}$ premier contenant un produit fini d'idéaux. Quitte à récurrer sur le nombre d'idéaux, on peut prendre ce nombre égal à 2, mettons $IJ\subset\mathfrak{p}$. Supposons alors $I\not\subset\mathfrak{p}$ et montrons $J\subset\mathfrak{p}$. Il y a un élement $i\in I\backslash\mathfrak{p}$: alors, pour tout $j\in J$, le produit ij est dans $IJ\subset\mathfrak{p}$, d'où par primalité $i\in\mathfrak{p}$ (exclu) ou $j\in\mathfrak{p}$; ceci tenant pour tout $j\in J$, on a terminé.

   Soit $\mathfrak{p}$ comme dans l'énoncé. Considérons un produit $ab\in\mathfrak{p}$. Alors le produit d'idéaux principaux $(a)(b)=(ab)$ est inclus dans $\mathfrak{p}$ (car $\mathfrak{p}$ idéal), donc par hypothèse $\mathfrak{p}$ contient (a) (donc a) ou (b) (donc b), ce qui montre sa primalité.

5. Soit I idéal non premier : il y a donc deux éléments a et b hors de I dont le produit est dans I. Pour créer un idéal strictement plus grand que I, on peut ajouter à ce dernier un autre idéal $\not\subset I$, par exemple un idéal principal engendré par un élément $\notin I$. Dans notre cas, on doit essayer $I+(a)$ et $I+(b)$. Leur produit a tous ses éléments de la forme

$$(i+\lambda a)(i'+\mu b)=\underbrace{i(i'+\lambda a)}_{\in I\text{ car }i\in I}+\underbrace{\lambda ai'}_{\in I\text{ car }i'\in I}+\underbrace{\lambda\mu ab}_{\in I\text{ car }ab\in I}\in I+I+I=I\text{, ce qui conclut.}$$

6. Soit $\mathfrak{p}$ un idéal premier. Puisque le quotient ${}^{A}\!/_{\mathfrak{p}}$ est intègre, il est réduit, donc $\mathfrak{p}$ est radical. Soient à présent I et J deux idéaux tels que $\mathfrak{p}=I\cap J$. Puisque $I\cap J\supset IJ$, un point précédent entraine l'une des inclusions $\mathfrak{p}\supset I$ ou $\mathfrak{p}\supset J$ mais alors les inclusions $\mathfrak{p}=I\cap J\subset I$ (idem pour J) entraînent l'une des égalités.

   Soit $\mathfrak{r}$ un idéal radical non premier. Montrons qu'il est décomposable. D'après le point précédent, il y a deux idéaux I et J contenant strictement $\mathfrak{r}$ tels que $IJ\subset\mathfrak{r}\subset I\cap J$. Prendre la racine donne $\sqrt{IJ}\subset\sqrt{\mathfrak{r}}\subset\sqrt{I\cap J}$, d'où (à l'aide d'un point précédent) l'égalité $\mathfrak{r}=\sqrt{I}\cap\sqrt{J}$, ce qui conclut vu la stricte inclusion $\mathfrak{r}\subsetneq I\subset\sqrt{I}$ (*idem* pour J).

7. Supposons par l'absurde que l'ensemble R des idéaux radicaux échappant à la conclusion soit non vide. Prenons-en un maximal et appelons-le $\mathfrak{r}$. S'il est irréductible, alors il est premier par le point précédent, ce qui contredit l'appartenance $\mathfrak{r}\in R$. On peut donc écrire $\mathfrak{r}=I\cap J$ pour deux idéaux I et J contenant strictement $\mathfrak{r}$, d'où l'on déduit $\mathfrak{r}=\sqrt{\mathfrak{r}}=\sqrt{I\cap J}=\sqrt{I}\cap\sqrt{J}$; puisque $\sqrt{I}$ et $\sqrt{J}$ contiennent strictement $\mathfrak{r}$, la maximalité de ce dernier les empêche d'appartenir à R, donc ces idéaux radicaux se décomposent en intersection de premiers, décomposition se propogeant à $\mathfrak{r}=\sqrt{I}\cap\sqrt{J}$ et contredisant l'appartenance $\mathfrak{r}\in R$.

8. Si le produit est intègre, vu la nullité du produit $(1,0)(0,1)$, l'un des deux facteurs A ou B doit être nul. Alors le facteur restant, disons A, est isomorphe au produit $A\times 0\cong A\times B$ qui est intègre. La réciproque est claire : l'intégrité de A équivaut à (donc implique) celle de $A\times 0$.

9. Un corps a un seul idéal strict, (0), qui est premier car tout corps est intègre. Soit réciproquement A un anneau comme dans l'énoncé. Déjà, A étant non nul, l'idéal (0) est strict, donc premier, donc A est intègre. Ensuite, pour a non nul, le produit $a\times a$ est dans l'idéal $\left(a^2\right)$, d'où (par primalité) $a\in\left(a^2\right)$, d'où (par intégrité) $1\in(a)$, ce qui traduit l'inversibilité de a.

10. L'idéal nul est bien premier puisque $\mathbf{Z}$ est intègre.

Soit p un nombre premier. Le cours nous dit que l'anneau ${}^{\mathbf{Z}}\!/_{p\mathbf{Z}}$ est un corps, donc est intègre, donc l'idéal (p) est premier.

Soit réciproquement $\mathfrak{p}$ un idéal premier non nul. Puisque $\mathbf{Z}$ est principal, on peut écrire $\mathfrak{p}=(a)$ pour un certain entier $a>0$. Puisque $\mathfrak{p}$ est un idéal strict, l'entier a n'est pas 1. Si a n'était pas premier, il pourrait s'écrire $a=bc$ pour certains entiers $1<b,c<a$; mais alors le produit bc appartiendrait à l'idéal $\mathfrak{p}$, donc b ou c y serait par primalité de $\mathfrak{p}$, disons $b\in\mathfrak{p}=(a)$, d'où un entier n tel que $b=na$, divisibilité qui contredirait l'encadrement $1<b<a$.

11. Un point précédent montre égalité$\sqrt{I}=\bigcap_{\mathfrak{r}\supset I}^{\mathfrak{r}\text{ radical}}\mathfrak{r}$; puisque tout premier est radical, cette intersection est incluse dans $\bigcap_{\mathfrak{p}\supset I}^{\mathfrak{p}\text{ premier}}\mathfrak{p}$. Montrons l'autre inclusion par contraposée. Soit $x\notin\sqrt{I}$. On va exhiber un idéal premier $\mathfrak{p}$ contenant I et pas x.

Soit $\mathcal{I}$ l'ensemble des idéaux contenant I et ne contenant aucune puissance $\in\mathbf{N}^*$ de x ordonné par l'inclusion. $\mathcal{I}$ est non vide car il contient I. Soit par ailleurs $(I_\omega)_{\omega\in\Omega}$ une famille totalement ordonnée d'éléments de $\mathcal{I}$. Montrons que $\bigcup_\Omega I_\omega$ (qui majore clairement cette chaîne) est un élément de $\mathcal{I}$. Chaque I_ω contenant I, leur réunion le contient ; si une puissance x^n appartient à $\bigcup_\Omega I_\omega$, elle doit appartenir à l'un des I_ω, ce qui contredit $I_\omega\in\mathcal{I}$. On peut donc appliquer le lemme de Zorn et invoquer un élément $\mathfrak{p}$ maximal dans $\mathcal{I}$. Montrons que $\mathfrak{p}$ est premier.

Si ce n'est pas le cas, on peut trouver $a,b\notin\mathfrak{p}$ tels que $ab\in\mathfrak{p}$. Alors l'idéal $\mathfrak{p}+(a)$ contenant I est strictement plus grand que $\mathfrak{p}$, donc n'est pas dans $\mathcal{I}$, *i. e.* contient une puissance $x^{n\geq 1}$, d'où un $j\in\mathfrak{p}$ et un $\lambda\in A$ tels que $x^n=j+\lambda a$. De même, on aurait une puissance $x^m=i+\mu b$ pour un $i\in\mathfrak{p}$ et $\mu\in A$. On en déduirait

$$x^{n+m}=(i+\mu b)(j+\lambda a)=\underbrace{ij+i\lambda a+j\mu b}_{\in\mathfrak{p}}+\underbrace{ab}_{\in\mathfrak{p}}\lambda\mu\in\mathfrak{p}\text{, ce qui est absurde.}$$

12. Appliquer le point précédent lorsque $I=\{0\}$.

13. Lorsque A est intègre, on retrouve le classique $A[X]^\times=A^\times$ en regardant le coefficient dominant d'une égalité $PQ=1$. Pour se ramener à ce cas, on va quotienter par un idéal premier $\mathfrak{p}$ fixé.

Soit donc (dans le cas général) une égalité $PQ=1$ dans $A[X]$. On la réduit modulo $\mathfrak{p}$, d'où $\overline{P}$ inversible dans ${}^{A}\!/_{\mathfrak{p}}[X]$, d'où (par intégrité de ${}^{A}\!/_{\mathfrak{p}}$) $\overline{P}$ constant, *i. e.* P constant modulo $\mathfrak{p}$, donc tous les coefficients non constants de P sont dans $\mathfrak{p}$; ceci tenant pour tout $\mathfrak{p}$, ces coefficients sont dans l'intersection $\bigcap\mathfrak{p}$, donc sont nilpotents. Par ailleurs, prendre les termes constants dans $PQ=1$ montre que celui de P est inversible.

Réciproquement, considérant un $P=i+\sum_{k\geq 1}n_kX^k$ avec i inversible et n_k nilpotents, on peut l'écrire $i\left(1+\sum_{k\geq 1}\frac{n_k}{i}X^k\right)$ où la somme à l'intérieur est nilpotente car les n_k (en nombre fini) le sont (élever à une puissance plus grande que la somme des indices de nilpotence des n_k). On se rappelle alors qu'un élément de la forme $1-N$ où N est nilpotent est inversible d'inverse $\sum_{k\geq 0}N^k$.

Exercice 4 (idéaux maximaux).

1. Soit $\mathfrak{m}$ un idéal maximal. Soit $\overline{a}\in{}^{A}\!/_{\mathfrak{m}}$ non nul : puisque $a\notin\mathfrak{m}$, l'idéal $\mathfrak{m}+(a)$ contient strictement $\mathfrak{m}$, donc vaut tout A, *i. e.* contient 1, mettons $1=m+\lambda a$, d'où (en réduisant modulo $\mathfrak{m}$) l'égalité $\overline{1}=\overline{0}+\overline{\lambda}\overline{a}$, ce qui montre que $\overline{a}$ est inversible (d'inverse $\overline{\lambda}$).

Soit $\mathfrak{m}$ un idéal tel que ${}^{A}\!/_{\mathfrak{m}}$ soit un corps. Soit I un idéal contenant strictement $\mathfrak{m}$. Soit $i\in I\backslash\mathfrak{m}$. Alors i est non nul modulo $\mathfrak{m}$, donc est inversible, mettons $\overline{ij}=\overline{1}$, ou encore $ij+m=1$, d'où l'on tire l'appartenance $1=\underbrace{ij}_{\in I}-\underbrace{m}_{\in\mathfrak{m}\subset I}\in I$ et l'égalité $I=A$.

2. Appliquer le point précédent à l'idéal nul et se souvenir que ${}^{A}\!/_{0}$ est isomorphe à A.

3. Un maximal étant premier, seuls (0) et les (p) premiers sont candidats. Le quotient $\mathbf{Z}/_0 \cong \mathbf{Z}$ n'étant pas un corps, 0 n'est pas maximal. Par ailleurs, le cours nous que l'anneau $\mathbf{Z}/_{p\mathbf{Z}}$ est un corps pour tout premier p.

4. Soit $J/_I$ un idéal de $A/_I$. On a alors les équivalences

$$J/_I \text{ maximal} \iff {}^{\left(A/_I\right)}/_{\left(J/_I\right)} \text{ corps} \iff A/_J \text{ corps} \iff J \text{ maximal.}$$

5. Immédiat en terme de quotients vu qu'un corps est intègre

La réciproque est fausse : dans l'anneau $\mathbf{Z}$, l'idéal nul est premier mais pas maximal (exemple valide dans tout anneau intègre qui n'est pas un corps). Autre contre-exemple : l'anneau $k[X,Y]$. L'idéal (X) est premier mais pas maximal car le quotient est isomorphe à $k[Y]$ (on a "tué" X) qui est intègre mais qui n'est pas un corps.

6. Soient $\mathfrak{m}$ et $\mathfrak{M}$ deux idéaux maximaux distincts. Par symétrie, on peut par exemple supposer $\mathfrak{m} \not\subset \mathfrak{M}$. Soit $m \in \mathfrak{m} \backslash \mathfrak{M}$. Alors l'idéal $\mathfrak{m} + \mathfrak{M}$ contient strictement $\mathfrak{M}$, donc par maximalité vaut tout A.

7. Utilisons la remarque de l'exercice 1. Soit $i \in I$. Le morphisme de groupes additifs $h_i : \left\{ \begin{array}{ccc} A & \longrightarrow & I \\ a & \longmapsto & ai \end{array} \right.$ vérifiant $h_i(\mathfrak{m}) \subset I\mathfrak{m}$, il induit un morphisme de groupes additifs $\left\{ \begin{array}{ccc} A/_\mathfrak{m} & \longrightarrow & I/_{I\mathfrak{m}} \\ \overline{a} & \longmapsto & \widetilde{ai} \end{array} \right.$, ce qui définit l'action du corps $A/_\mathfrak{m}$ sur $\widetilde{i}$, donc sur tout le groupe additif $I/_{I\mathfrak{m}}$. Les axiomes d'un espace vectoriels sont alors immédiat à vérifier (par exemple, l'associativité découle des égalités $\overline{a}\left(\widetilde{bi}\right) = \overline{a}\widetilde{bi} = \widetilde{a(bi)} = \widetilde{(ab)i} = \widetilde{\overline{ab}i} = \left(\overline{a}\overline{b}\right)\widetilde{i}$).

8. Soit I un idéal strict. L'ensemble $\mathcal{I}$ des idéaux stricts contenant I est non vide (I est dedans). Montrons que $\mathcal{I}$ est stable par union de chaîne. Soit $(I_\omega)_{\omega\in\Omega}$ une famille totalement ordonnée d'éléments de $\mathcal{I}$. Montrons que $\bigcup_\Omega I_\omega$ (qui majore clairement cette chaîne) est un élément de $\mathcal{I}$. Chaque I_ω contenant I, leur réunion le contient ; si elle valait tout A, elle contiendrait 1, donc l'un des I_ω contiendrait 1 et vaudrait tout A, ce qui contredirait $I_\omega \in \mathcal{I}$. On peut donc appliquer le lemme de Zorn et invoquer un élément $\mathfrak{m}$ maximal dans $\mathcal{I}$. Montrons que l'idéal $\mathfrak{m}$ est maximal. Soit M un idéal strict contenant $\mathfrak{m}$. Il contient alors I, donc appartient à $\mathcal{I}$; puisque $\mathfrak{m}$ est un élément maximal de $\mathcal{I}$, l'inclusion $\mathfrak{m} \subset M$ devient une égalité, *c. q. f. d.*.

9. Appliquer le point précédent à l'idéal nul.

10. Soit $a \in A$. Un point précédent permet d'écrire les équivalences

$$a \notin A^\times \iff (a) \subsetneq A \overset{\text{Krull}}{\iff} \exists \mathfrak{m} \text{ maximal, } (a) \subset \mathfrak{m} \iff \exists \mathfrak{m} \text{ maximal, } a \in \mathfrak{m} \iff a \in \bigcup_{\mathfrak{m} \text{ maximal}} \mathfrak{m}.$$

11. Si A admet un unique idéal maximal, alors la réunion des idéaux maximaux est un idéal strict. Montrons la réciproque. Supposons que la réunion $M := \bigcup_{\mathfrak{m} \text{ maximal}} \mathfrak{m}$ soit un idéal strict. Soit $\mathfrak{m}$ un idéal maximal. Puisque $\mathfrak{m} \subset M \subsetneq A$, on a l'égalité $\mathfrak{m} = M$, ce qui montre que M est l'unique idéal maximal de A.

Par conséquent, A admet un unique idéal maximal ssi les éléments non inversibles forment un idéal strict, *i. e.* ssi $A \backslash A^\times$ (qui est stable par multiplication par n'importe élément de A) contient 0 et est stable par addition, ce qui conclut.

Une autre démonstration serait possible en traitant le cas $A = 0$ à part puis en joignant les deux idées suivantes : une réunion $\bigcup A_i$ de parties $A_i \subset A$ est stable par $+$ ssi $\bigcup A_i = \sum A_i$, une somme d'au moins deux idéaux étrangers deux à deux (comme le sont des maximaux) vaut A.

12. Soit M et N les matrices d'un isomorphisme $A^p \widetilde{\longrightarrow} A^q$ et de sa réciproque. Réduisant modulo un idéal maximal $\mathfrak{m}$ de A (qui existe d'après Krull), la relation $MN = 1$ devient $\overline{M}\ \overline{N} = \overline{1}$ (on ne fait que des sommes et produits qui passent modulo $\mathfrak{m}$) où les matrices sont à coefficients dans un corps (à savoir $A/_\mathfrak{m}$), donc leur inversibilité impose qu'elle soient carrées (sinon le rang est trop petit), *c. q. f. d.*.

13. Montrons que $\operatorname{Jac} A$ est stable par racine carrée. Soit $a \in A$ tel que $a^2 \in \operatorname{Jac} A$. Soit $\lambda \in A$. Alors est inversible $1 + \left(\lambda^3 a\right) a^2 = (1 + \lambda a)\left(1 - \lambda a + (\lambda a)^2\right)$, donc $1 + \lambda a$ l'est aussi. On en déduit $a \in \operatorname{Jac} A$, *c. q. f. d.*.

Montrons $\operatorname{Nilrad} A \subset \operatorname{Jac} A$. Démo 1 : vérifier pour tout n nilpotent que la somme $\sum_{k\geq 0} n^k$ fait sens et est un inverse de $1 - n$; ensuite, étant donnés un nipotent n et un $a \in A$, l'élément $-na$ est nilpotent, donc $1 + na$ est inversible, d'où $n \in \operatorname{Jac} A$. Démo 2 : un idéal maximal étant premier, l'intersection $\operatorname{Jac} A$ des maximaux contient l'intersection $\operatorname{Nilrad} A$ des premiers.

14. Montrons que $\operatorname{Jac} A$ est un idéal de A (il vérifie clairement $1 + \operatorname{Jac} A \subset A^\times$). On a déjà $0 \in \operatorname{Jac} A$. Soient $x, y \in \operatorname{Jac} A$ et $a \in A$. Alors $1 + a(x+y)$ est inversible car

$$\begin{aligned}(1 + a(x+y)) \frac{1}{1+ax} \frac{1}{1 + \frac{a}{1+ax} y} &= ((1+ax) + ay) \frac{1}{1+ax} \frac{1}{1 + ay\frac{1}{1+ax}} \\ &= \left(1 + ay \frac{1}{1+ax}\right) \frac{1}{1 + ay \frac{1}{1+ax}} \\ &= 1.\end{aligned}$$

Enfin, pour tout $\lambda \in A$, l'élément $1 + \lambda(ax) = 1 + (a\lambda)x$ est inversible, donc $ax \in \operatorname{Jac} A$.

Soit maintenant I un idéal de A qui vérifie $1 + I \subset A^\times$. Soit $x \in I$ et $a \in A$. On a $ax \in I$, donc $1 + ax \in A^\times$, d'où $x \in \operatorname{Jac} A$ et l'inclusion $I \subset \operatorname{Jac} A$.

15. Soit $x \in \bigcap \mathfrak{m}$. Supposons par l'absurde $x \notin \operatorname{Jac} A$. Soit $a \in A$ tel que $y := 1 + ax$ ne soit pas inversible. L'idéal (y) est donc contenu dans un idéal maximal, mettons $\mathfrak{m}' \ni y$. Alors $x \in \bigcap \mathfrak{m} \subset \mathfrak{m}'$, donc $ax \in \mathfrak{m}'$, d'où $y - ax \in \mathfrak{m}'$, *i. e.* $1 \in \mathfrak{m}'$, ce qui est absurde.

Réciproquement, soient $x \in \operatorname{Jac} A$ et $\mathfrak{m}$ un idéal maximal de A. L'idéal $\mathfrak{m} + (x)$ est un idéal qui contient $\mathfrak{m}$, donc vaut $\mathfrak{m}$ ou A. Si $\mathfrak{m} + (x) = A$, on aurait $1 = m + ax$ pour un certain $m \in \mathfrak{m}$ et un certain $a \in A$; comme $x \in \operatorname{Jac} A$, l'élément $1 - ax = m$ est inversible, ce qui est absurde. L'idéal $\mathfrak{m} + (x)$ vaut donc $\mathfrak{m}$, d'où l'appartenance $x = 0 + 1x \in \mathfrak{m} + (x) = \mathfrak{m}$, *c. q. f. d.*.

16. Les idéaux maximaux de ${}^{A}\!/_{\operatorname{Jac} A}$ sont les quotients ${}^{\mathfrak{m}}\!/_{\operatorname{Jac} A}$ où $\mathfrak{m}$ idéal maximal contenant $\operatorname{Jac} A$. D'après le point précédent, cette dernière condition est tautologique. Ainsi, pour $\overline{a}$ dans $\operatorname{Jac}\left({}^{A}\!/_{\operatorname{Jac} A}\right)$, on a $\overline{a} \in {}^{\mathfrak{m}}\!/_{\operatorname{Jac} A}$ pour tout $\mathfrak{m}$, d'où $a \in \mathfrak{m}$ pour tout $\mathfrak{m}$, *i. e.* $a \in \operatorname{Jac} A$, d'où $\overline{a}$ nul dans ${}^{A}\!/_{\operatorname{Jac} A}$, *c. q. f. d.*.

17. Si A est nul, alors il n'admet aucun idéal maximal. On suppose désormais A non nul.

Soit $a \in A$. Comparons a et $a+1$ (intuition : dans les entiers, ils ne sont presque jamais comparables, donc forcer leur comparaison devrait faire des étincelles).

Supposons $a \mid a+1$. Soit $\lambda \in A$ tel que $a + 1 = \lambda a$. On a alors $a(\lambda - 1) = 1$ donc a est inversible. Supposons cette fois $a+1 \mid a$, mettons $a = \lambda(a+1)$ pour un certain $\lambda \in A$. On a alors $(a+1)(1-\lambda) = 1$, donc $a+1$ est inversible.

Nous venons de montrer l'implication $\forall a \in A,\ a \notin A^\times \Longrightarrow a + 1 \in A^\times$. On en déduit les implications (à $a \in A$ fixé)

$$\begin{aligned} a \in \bigcup_{\mathfrak{m} \text{ maximal}} \mathfrak{m} &\implies a \in A \backslash A^\times \Longrightarrow \forall x \in A,\ ax \in A \backslash A^\times \Longrightarrow \forall x \in A,\ 1 + ax \in A^\times \Longrightarrow a \in \operatorname{Jac} A \\ &\implies a \in \bigcap_{\mathfrak{m} \text{ maximal}} \mathfrak{m}, \text{ d'où l'inclusion } \bigcup_{\mathfrak{m} \text{ maximal}} \mathfrak{m} = \bigcap_{\mathfrak{m} \text{ maximal}} \mathfrak{m}, \text{ ce qui conclut.}\end{aligned}$$