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

Anneaux de polynômes II, anneaux quotients

Exercice 1

Dans le cours nous avons déjà montré que le produit de polynômes primitifs est aussi primitif et que

$$c(f \cdot g) = c(f) \cdot c(g) \qquad \forall\, f,g \in \mathbb{Z}[x].$$

1. Etant donné $f \in \mathbb{Q}[x]$, alors $f = \alpha \cdot f_0$ où $f_0 \in \mathbb{Z}[x]$ est un polynôme primitif et $\alpha \in \mathbb{Q}$.
2. Soit $g \in \mathbb{Z}[x]$ un polynôme primitif, $\alpha \in \mathbb{Q}$ tel que $\alpha \cdot g \in \mathbb{Z}[x]$. Alors $\alpha \in \mathbb{Z}$.
3. Considèrons deux polynômes d, f sur $\mathbb{Z}$. Si d est primitif et d divise f dans $\mathbb{Q}[x]$ alors d divise f dans $\mathbb{Z}[x]$.
4. Supposons que $d = \mathrm{pgcd}_{\mathbb{Q}[x]}(f,g)$ soit le p.g.c.d. dans l'anneau $\mathbb{Q}[x]$ de deux polynômes primitifs f et g de $\mathbb{Z}[x]$. Soit $d = \alpha \cdot d_0$ sa représentation de type 1). Montrer que : $d_0 = \mathrm{pgcd}_{\mathbb{Z}[x]}(f,g)$ dans l'anneau $\mathbb{Z}[x]$.
5. Soient f, $g \in \mathbb{Z}[x]$, $f = c(f)f_0$, $g = c(g)g_0$. Alors

$$\mathrm{pgcd}_{\mathbb{Z}[x]}(f,g) = \mathrm{pgcd}_{\mathbb{Z}}(c(f),c(g)) \cdot \mathrm{pgcd}_{\mathbb{Z}[x]}(f_0,g_0).$$

Correction ▼ [002280]

Exercice 2

Démontrer que tout morphisme d'un corps dans un anneau non-trivial est injectif.

Correction ▼ [002281]

Exercice 3

Soit R un anneau intègre dans lequel toute chaîne décroissante d'idéaux est finie. Démontrer que R est un corps.

Correction ▼ [002282]

Exercice 4

Montrer que dans un anneau fini tout idéal premier est maximal.

Correction ▼ [002283]

Exercice 5

Montrer que un idéal propre I de l'anneau A est premier ssi quand le produit de deux idéaux est contenue dans I, alors l'un de deux est contenu dans I. En déduire que si M est un idéal maximal de A, alors le seul idéal premier de A qui contient M^n est M.

Correction ▼ [002284]

Exercice 6

Soit A un anneau. Trouver les anneaux quotients

$$A[x]/(x), \quad A[x,y]/(x), \quad A[x,y]/(x,y), \quad A[x_1,x_2,\ldots,x_n]/(x_1,x_2,\ldots,x_n)$$

où (x), (x,y), $(x_1,x_2,\ldots,x_n)$ sont les idéaux engendrés réspectivement par x, x et y, x_1, x_2, ... ,x_n. Sous quelle condition sur l'anneau A ces idéaux sont-ils premiers (maximaux) ?

Correction ▼ [002285]

Exercice 7

1. Trouver le nombre d'éléments de l'anneau quotient $\mathbb{Z}[\sqrt{d}]/(m)$ où $m \in \mathbb{Z}$ et $m \neq 0$.
2. L'idéal principal endendré par 2 est-il premier dans l'anneau $\mathbb{Z}[\sqrt{d}]$?

Correction ▼ [002286]

Exercice 8

Soit A un anneau intègre. On appelle *élément premier* de A un élément qui engendre un idéal principal premier.

1. Montrer que un élément premier est irréductible.
2. D'après le cours tout élément irréductible dans un anneau factoriel est premier. Montrer que dans un anneau factoriel, tout idéal premier non nul contient un élément irréductible.
3. Nous avons vu que l'élément $3 \in \mathbb{Z}[\sqrt{-5}]$ est irréductible. Montrer que 3 n'est pas premier dans $\mathbb{Z}[\sqrt{-5}]$.
4. L'élément 2 est-il irréductible dans l'anneau $\mathbb{Z}[\sqrt{-5}]$?

Correction ▼ [002287]

Exercice 9

1. Soit A un anneau principal, I un idéal de A. Montrer que tous les idéaux de l'anneau quotient A/I sont principaux.
2. Trouver tous les idéaux des anneaux suivants : $\mathbb{Z}/n\mathbb{Z}$, $\mathbb{Q}[x]/(f)$ où (f) est l'idéal principal engendré par un polynôme f.
3. Trouver les idéaux maximaux de $\mathbb{Z}/n\mathbb{Z}$ et de $\mathbb{Q}[x]/(f)$.

Correction ▼ [002288]

Exercice 10

Soit I et J deux idéaux de l'anneau A. Considérons la projection canonique
$\pi_I : A \to A/I$ et l'image $\bar{J} = \pi_I(J)$ de l'idéal J.

1. Montrer que $\bar{J}$ est un idéal de l'anneau quotient A/I.
2. Démontrer qu'on a l'isomorphisme suivant : $(A/I)/\bar{J} \cong A/(I+J)$.
   (*Indication :*. Considérer le morphisme $a+I \mapsto a+(I+J)$ de l'anneau A/I vers l'anneau $A/(I+J)$.)

Correction ▼ [002289]

Exercice 11

Soit f un morphisme de l'anneau A vers l'anneau B.

1. Montrer que l'image réciproque d'un idéal premier est aussi un idéal premier. Cette proposition est-elle vraie pour idéaux maximaux ?
2. Montrer par un exemple, que l'image $f(I)$ d'un idéal I de A n'est pas forcément un idéal de B. Démontrer cependant que si f est surjectif, alors $f(I)$ est un idéal pour tout idéal I de A. (Voir le cours.)
3. Toujours sous l'hypothèse que f est surjective, montrer que l'image d'un idéal maximal par f est soit B tout entier, soit un idéal maximal de B.
4. Considérons la reduction de polynômes sur $\mathbb{Z}$ modulo m : $r_m : \mathbb{Z}[x] \to \mathbb{Z}_m[x]$ et deux idéaux premiers principaux (x) et (x^2+1). Les idéaux $r_6((x))$ et $r_2((x^2+1))$ sont-ils premiers ?

Correction ▼ [002290]

Exercice 12

Soit A un anneau, B un sous-anneau de A, I un idéal de A.

1. Montrer que $B \cap I$ est un idéal de B, $B+I = \{b+i \,|\, b \in B,\ i \in I\}$ est un sous-anneau de l'anneau A et I est un idéal de ce sous-anneau.
2. Montrer que l'anneau quotient $B/(B \cap I)$ est isomorphe à l'anneau quotient $(B+I)/I$. (*Indication :* Considérer le composé de l'inclusion $B \to B+I$ avec la projection canonique $B+I \to (B+I)/I$.)

Correction ▼ [002291]

Correction de l'exercice 1 ▲

1. Soit $f=\sum_{i=0}^{n}a_ix^i\in\mathbb{Q}[x]$. Soit $a_i=\frac{p_i}{q_i}$ le représentant irréductible de a_i. Soit $m=\mathrm{ppcm}(q_0,\dots,q_n)$. Notons $m=q_im_i$. Alors $f=\frac{1}{m}\sum a_im_ix^i$. En mettant en facteur $d=\mathrm{pgcd}(a_0m_0,\dots,a_nm_n)$, on obtient $f=\frac{d}{m}f_0$, où $f_0\in\mathbb{Z}[x]$ est primitif.
2. Notons $\alpha=\frac{p}{q}$, avec $\mathrm{pgcd}(p,q)=1$ et $q>0$. Soit $g_1=\alpha g$. On a $qg=pg_1$, donc $qc(g)=pc(g_1)$. On en déduit que $q|p$, et donc que $q=1$:$\alpha\in\mathbb{Z}$.
3. Soit $g\in\mathbb{Q}[x]$ tel que $f=dg$. Soit $g=\frac{p}{q}g_0$ la décomposition de g donnée par la question 1. Alors $qf=pdg_0$ donc $qc(f)=pc(d)c(g_0)=p$. Donc $q|p$ et finalement $q=1$. On en déduit que $g=pg_1\in\mathbb{Z}[x]$.
4. $d=\mathrm{pgcd}_{\mathbb{Q}}(f,g)=\frac{p}{q}d_0$. Alors d_0 est primitif et divise f et g sur $\mathbb{Q}$. Donc d_0 divise f et g sur $\mathbb{Z}$.
   Soit h un diviseur commun de f et g dans $\mathbb{Z}[x]$. On a $c(h)|c(f)=1$ donc h est primitif. Par ailleurs, h est un diviseur commun à f et g dans $\mathbb{Q}[x]$, donc $h|d_0$ dans $\mathbb{Q}[x]$. On en déduit que $h|d_0$ dans $\mathbb{Z}[x]$.
   Ainsi, d_0 est bien un pgcd de f et g dans $\mathbb{Z}[x]$.
5. Soit $d=\mathrm{pgcd}(c(f),c(g))$, $h=\mathrm{pgcd}(f,g)=c(h)h_0$, $h'=\mathrm{pgcd}(f_0,g_0)$.
   On a $d|c(f)$, $d|c(g)$, $h'|f_0$ et $h'|g_0$ donc $dh'|f$ et $h'|g$, et donc $dh'|h$.
   $c(h)|c(f)$ et $c(h)|c(g)$ donc $c(h)|d$. $h|f$, donc il existe $f_1\in\mathbb{Z}[x]$ tel que $f=h_0c(h)f_1$. On a alors $c(h)c(f_1)=c(f)$, et après simplification, on en déduit que $f_0=h_0f_1'$, avec $f_1'\in\mathbb{Z}[x]$: $h_0|f_0$. De même pour g : $h_0|g_0$. On en déduit que $h_0|h'$, et donc que $h|dh'$.

Correction de l'exercice 2 ▲

Soit K un corps, A un anneau non trivial, et $K\xrightarrow{\phi}A$ un morphisme d'anneaux. Soit $x\in K\setminus\{0\}$. On a $1=\phi(1)=\phi(xx^{-1})=\phi(x)\phi(x^{-1})\neq 0$ (car A n'est pas l'anneau trivial). Donc $\phi(x)\neq 0$. Ainsi $\ker\phi=\{0\}$, donc ϕ est injectif.

Correction de l'exercice 3 ▲

Soit $x\in R\setminus\{0\}$. Alors $(x)\supset(x^2)\supset(x^3)\supset$ est une suite décroissante d'idéaux. Elle est donc stationnaire à partir d'un certain rang : $\exists k\in\mathbb{N},(x^k)=(x^{k+1})$. En particulier, $\exists a\in R,k^{k+1}=ax^k$. Comme A est intègre, on en déduit que $ax=1$, donc $x\in R^\times$.
$R^\times=R\setminus\{0\}$ donc R est un corps.

Correction de l'exercice 4 ▲

Soit A un anneau fini, et I un idéal premier. Alors A/I est intègre, et fini (!), donc A/I est un corps (voir exercice **??**). Donc I est maximal.

Correction de l'exercice 5 ▲

On rappelle que le produit de deux idéaux I et J est l'idéal engendré par les produits de la forme ab avec $a\in I$, $b\in J$:

$$I\cdot J=\{\sum_{i=0}^{N}a_ib_i,N\in\mathbb{N},a_i\in I,b_i\in J\}$$

— Si I est un idéal premier : Soient J et K deux idéaux tels que $J\cdot K\subset I$. Alors si $J\not\subset I$, $\exists a\in x\setminus I$. Soit $y\in K$. On a $xy\in J\cdot K$ donc $xy\in I$. Comme I est premier, $x\in I$ ou $y\in I$. Mais $x\notin I$ donc $y\in I$. Ainsi $\forall y\in K,y\in I$: on a montré que : $J\not\subset I\Rightarrow K\subset I$. On a donc bien $J\subset I$ ou $K\subset I$.
— Si $\forall J,K$ idéaux, $(J\cdot K\subset I\Rightarrow J\subset I$ ou $K\subset I)$: Soit $a,b\in A$ avec $ab\in I$. Alors $(a)\cdot(b)=(ab)$ donc $(a)\subset I$ ou $(b)\subset I$ et donc $a\in I$ ou $b\in I$. I est donc premier.

On a $M^n=M\cdot M^{n-1}$. Donc si I est premier et contient M^n alors I contient M ou M^{n-1}, et par une récurrence finie, on obtient que I contient M. Ainsi : $M\subset I\subsetneq A$. Comme M est maximal on en déduit que $M=I$.

Correction de l'exercice 6 ▲

— $A[X]/(X)$: X est unitaire donc on dispose de la division euclidienne par X. On vérifie (comme dans le cours) que chaque classe a un et un seul représentant de degré 0. On en déduit que $A[X]/(X)$ est en bijection avec A. Il reste alors à remarquer que cette bijection est un morphisme d'anneaux.
Une autre façon de dire la même chose est de remarquer que l'application $\phi : A[X] \to A$, $P \mapsto P(0)$ est un morphisme d'anneaux. $\ker\phi = (X)$ et $\operatorname{Im}\phi = A$. Comme $A/\ker\phi \sim \operatorname{Im}\phi$, on a bien $A[X]/(X) \sim A$.

— On peut considérer $\phi : A[X,Y] \to A[Y]$, $P \mapsto P(0,Y)$. C'est un morphisme d'anneaux. En séparant les termes ne dépendant que de Y des autres, on peut mettre tout polynôme P de $A[X,Y]$ sous la forme $P = P_1(Y) + XP_2(X,Y)$ où $P_1 \in A[Y]$ et $P_2 \in A[X,Y]$. Alors $\phi(P) = 0$ ssi $P_1 = 0$, ssi $P = XP_2$, c'est à dire $P \in (X)$. Ainsi $\ker\phi = (X)$. Par ailleurs, tout polynôme P de $A[Y]$ peut être vu comme un polynôme $\tilde{P}$ de $A[X,Y]$. Alors $P = \phi(\tilde{P})$, donc $\operatorname{Im}\phi = A[Y]$. Finalement : $A[X,Y]/(X) \sim A[Y]$.

— $A[X,Y]/(X,Y)$: Soit $\phi : A[X,Y] \to A$, $P \mapsto P(0,0)$. ϕ est un morphisme d'anneaux, et avec les notations précédentes, pour $P = P_1(Y) + XP_2(X,Y)$, avec $\phi(P) = 0$, on a $P_1(0) = 0$, donc $Y|P_1(Y)$. Ainsi, P est la somme de deux polynômes, l'un multiple de X, l'autre multiple de Y donc $P \in (X,Y)$. Réciproquement, si $P \in (X,Y)$, alors $P(0,0) = 0$. Donc $\ker\phi = (X,Y)$. $\forall a \in A\phi(a) = a$ donc ϕ est surjective. Finalement $A[X,Y]/(X,Y) \sim A$.

— $A[X_1,\dots,X_n]/(X_1,\dots,X_n)$: Soit $\phi\ : A[X_1,\dots,X_n] \to A$, $P \mapsto P(0)$. ϕ est un morphisme d'anneaux. En regroupant tous les termes dépendant de X_n, puis tous les termes restant dépendant de X_{n-1}, et ainsi de suite jusqu'aux termes dépendant seulement de X_1, et enfin le terme constant, tout polynôme $P \in A[X_1,\dots,X_n]$ peut se mettre sous la forme $P = X_nP_n + X_{n-1}P_{n-1} + \cdots + X_1P_1 + p_0$, avec $P_i \in A[X_1,\dots,X_i]$ (et $p_0 \in A$). On en déduit que $\ker\phi = (X_1,\dots,X_n)$. Par ailleurs $\forall a \in A, \phi(a) = a$, donc $A[X_1,\dots,X_n]/(X_1,\dots,X_n) \sim A$.

Comme un idéal est premier (resp. maximal) ssi le quotient est intègre (resp. un corps), on en déduit que

— dans $A[X]$, (X) est premier ssi A est intègre, maximal ssi A est un corps,
— dans $A[X,Y]$, (X) est premier ssi A est intègre, et n'est jamais maximal,
— dans $A[X_1,\dots,X_n]$, $(X_1,\dots,X_n)$ est premier ssi A est intègre, maximal ssi A est un corps.

Correction de l'exercice 7 ▲

Soit $\alpha = a + b\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$. Soit $a = mp + a'$ la division euclidienne de a par m, et $b = mq + b'$ celle de b par m. Alors $\alpha = m(p + q\sqrt{d}) + a' + b'\sqrt{d}$. On en déduit que chaque classe du quotient $\mathbb{Z}[\sqrt{d}]/(m)$ a un représentant dans

$$\mathscr{C} = \left\{a + b\sqrt{d},\ (a,b) \in \{0,\dots,m-1\}^2\right\}$$

Par ailleurs si deux éléments $a + b\sqrt{d}$ et $a' + b'\sqrt{d}$ de cet ensemble sont dans la même classe, alors $\exists c,d \in \mathbb{Z}$, $a + b\sqrt{d} = (a' + b'\sqrt{d}) + m(c + d\sqrt{d})$. On en déduit que $a = a' + mc$ et $b = b' + md$, et donc $a = a'$, $b = b'$. Ainsi chaque classe de $\mathbb{Z}[\sqrt{d}]/(m)$ a un représentant unique dans $\mathscr{C}$. $\mathbb{Z}[\sqrt{d}]/(m)$ et $\mathscr{C}$ sont donc en bijection : en particulier, $\mathbb{Z}[\sqrt{d}]/(m)$ a m^2 éléments.
Remarque : on a

$$\mathbb{Z}[\sqrt{d}] \sim \mathbb{Z}[X]/(X^2 - d).$$

En effet l'application $\phi : \mathbb{Z}[X]/(X^2 - d) \to \mathbb{Z}[\sqrt{d}]$, $\bar{P} \mapsto P(\sqrt{d})$ est bien définie (si $\bar{(}P) = \bar{Q}$, alors $P(\sqrt{d}) = Q(\sqrt{d})$), et c'est un morphisme d'anneaux. De plus, si $\phi(P) = 0$, notons $P = Q(X^2 - d) + (aX + b)$ la division euclidienne de P par $X^2 - d$. En évaluant en $\sqrt{d}$, on a $a\sqrt{d} + b = 0$ donc $R = 0$. On en déduit que $(X^2 - d)|P$, i.e. $\bar{P} = 0$. On en déduit que $\ker\phi = \{0\}$, donc ϕ est injective. Par ailleurs $\forall (a,b) \in \mathbb{Z}^2, \phi(a + bX) = a + b\sqrt{d}$ donc ϕ est surjective.

Si d est pair, comme $\sqrt{d} \cdot \sqrt{d} = |d| \in (2)$ alors que $\sqrt{d} \notin (2)$, (2) n'est pas premier.
Si d est impair : $(1 + \sqrt{d})(1 + \sqrt{d}) = (1 + d) + 2\sqrt{d} \in (2)$, mais $(1 + \sqrt{d}) \notin (2)$ donc (2) n'est pas premier.
Remarque : $\mathbb{Z}[\sqrt{d}]/(2) \sim \mathbb{Z}_2[X]/(X^2 + \bar{d})$. $(X^2 + \bar{d})$ est X^2 ou $X^2 + 1$. Aucun de ces deux polynômes n'est irréductible. Donc le quotient ne saurait être intègre.

Correction de l'exercice 8 ▲

— Si $x \in A$ est premier : soit $a,b \in A$ tels que $ab = x$. Alors $ab \in (x)$ donc $a \in (x)$ ou $b \in (x)$. On en déduit que $a \sim x$ ou $b \sim x$. Donc x est irréductible.

— A est supposé factoriel. Soit I un idéal premier. Soit $x \in I$ et $x = p_1 \dots p_k$ “la” factorisation de x en produit d'irréductibles. Alors $(p_1 \cdots p_{n-1})p_n \in I$ donc $(p_1 \cdots p_{n-1}) \in I$ ou $p_n \in I$. si p_n in I, I contient un irréductible. Sinon, $(p_1 \cdots p_{n-2})p_{n-1} \in I$. Par une récurrence finie, l'un au moins des $p_i \in I$, donc I contient un irréductible.

— Dans $\mathbb{Z}[\sqrt{-5}]$, $9 \in (3)$. Pourtant $9 = (2+\sqrt{-5})(2-\sqrt{-5})$ et $(2 \pm \sqrt{-5}) \notin (3)$. Donc (3) n'est pas premier.

— 2 est irréductible : $2 = z_1 z_2$ avec $z_i \in \mathbb{Z}[\sqrt{-5}]$, alors $|z_1|^2|z_2|^2 = 4$, donc $\{|z_1|^2, |z_2|^2\} = \{1,4\}$ ou $\{2,2\}$. Dans le premier cas, on a affaire à une factorisation triviale. Le second est impossible, puisque l'équation $a^2 + 5b^2 = 2$ n'a pas de solution entière (a,b).
Par ailleurs, $(1+\sqrt{-5})(1+\sqrt{-5}) = 6 \in (2)$, mais $(1 \pm \sqrt{-5}) \notin (2)$ donc 2 n'est pas premier dans $\mathbb{Z}[\sqrt{-5}]$.

Correction de l'exercice 9 ▲

1. Soit $\mathscr{J}$ un idéal de A/I. Soit π la projection canonique $A \to A/I$, et $J = \pi^{-1}(\mathscr{J})$. J est un idéal de A qui est principal donc $\exists a \in A, J = (a)$. Montrons que $\mathscr{J} = (\pi(a))$.
On a $\pi(a) \in \mathscr{J}$ donc $(\pi(a)) \subset \mathscr{J}$. Soit $\alpha \in \mathscr{J}$, et b un représentant de α, i.e. $b \in A$ et $\pi(b) = \alpha$. Alors $b \in J = (a)$, donc $\exists k \in A, b = ka$. Alors $\pi(b) = \pi(ka) = \pi(k)\pi(a)$, donc $\pi(b) \in (\pi(a))$. Donc $\mathscr{J} \subset (\pi(a))$.
Finalement, $\mathscr{J} = (\pi(a))$. On en déduit que A/I est principal.
2. — $\mathbb{Z}/n\mathbb{Z}$: Soit I un idéal de $\mathbb{Z}/n\mathbb{Z}$. I est principal, donc $\exists a \in \mathbb{Z}, I = (\bar{a})$. Or $(\bar{a}) = \{\alpha\bar{a}, \alpha \in \mathbb{Z}/n\mathbb{Z}\} = \{\bar{p}\bar{a}, p \in \mathbb{Z}\} = \{\overline{pa}, p \in \mathbb{Z}\}$. Donc $\pi^{-1}(I) = \{pa + qn, (p,q) \in \mathbb{Z}^2\}$ est l'idéal engendré sur $\mathbb{Z}$ par a et n donc l'idéal engendré par $d = (\mathrm{pgcd}(n,a))$. On en déduit que $I = (\bar{d})$. En particulier, I est engendré par un diviseur de n.
Soit maintenant d_1 et d_2 deux diviseurs (positifs) de n tels que $(\bar{d_1}) = (\bar{d_2})$. On a $\pi^{-1}((d_1)) = d_1\mathbb{Z} = d_2\mathbb{Z}$ donc $d_1 = d_2$.
Ainsi, les idéaux de $\mathbb{Z}/n\mathbb{Z}$ sont engendrés par les diviseurs de n, et deux diviseurs distincts engendrent deux idéaux distincts : il y a donc autant d'idéaux dans $\mathbb{Z}/n\mathbb{Z}$ que de diviseurs de n.
— $\mathbb{Q}[X]/(f)$: On raisonne de la même manière : la remarque clef étant si $I = (\bar{g})$ est un idéal de $\mathbb{Q}[X]/(f)$, alors $\pi^{-1}(I) = (f,g) = (\mathrm{pgcd}(f,g))$.
3. Les idéaux maximaux sont ceux pour lesquels le quotient est un corps, (donc aussi ceux pour lesquels le quotient est intègre puisque $\mathbb{Z}/n\mathbb{Z}$ est fini). On a le diagramme suivant ($I = (\bar{d})$) :

$$\begin{tikzcd}
\mathbb{Z} \arrow[r, "\pi_1"] \arrow[rr, bend left, "\pi_2\circ\pi_1"] \arrow[d, "\pi"] & \mathbb{Z}/n\mathbb{Z} \arrow[r, "\pi_2"] & (\mathbb{Z}/n\mathbb{Z})/I \\
\mathbb{Z}/d\mathbb{Z} \arrow[urr, "\sim"'] & &
\end{tikzcd}$$

En effet, π_1 et π_2 sont des morphismes d'anneaux, et $\ker(\pi_2 \circ \pi_1) = d\mathbb{Z}$. Donc $(\mathbb{Z}/n\mathbb{Z})/I$ est un corps ssi d est premier.
De même, $(\mathbb{Q}[X]/(f))/I$ est un corps ssi $I = (\bar{g})$ où g est un facteur premier de f.

Correction de l'exercice 10 ▲

1. Soit $\alpha, \beta \in \bar{J}$ et $\lambda, \mu \in A/I$. Alors $\exists a, b \in J$, $l, m \in A$, $\alpha = \pi(a), \beta = \pi(b), \lambda = \pi(l), \mu = \pi(m)$. On a donc $\lambda\alpha + \mu\beta = \pi(la + mb)$. Or $la + mb \in J$ (car J est un idéal), donc $\lambda\alpha + \mu\beta \in \bar{J}$. Donc $\bar{J}$ est un idéal de A/I.

2. Comme dans l'exercice 9, on a le diagramme suivant :

$$\begin{tikzcd} A \arrow[r, "\pi_1"] \arrow[rr, bend left, "\pi_2\circ\pi_1"] \arrow[d, "\pi"] & A/I \arrow[r, "\pi_2"] & (A/I)/\bar{J} \\ A/(I+J) \arrow[urr, "\sim"'] & & \end{tikzcd}$$

En effet, si $x \in \ker(\pi_2 \circ \pi_1)$, alors $\pi_1(x) \in \ker \pi_2 = \bar{J}$, donc $\exists y \in A, \pi_1(x) = \pi_1(y)$. Alors $x - y \in \ker \pi_1 = I$, donc $\exists z \in I, x = y + z$: on a donc $x \in I + J$. Réciproquement, si $x \in I + J$, alors $\exists (x_1, x_2) \in I \times J, x = x_1 + x_2$. Alors $\pi_1(x) = \pi_1(x_2) \in \bar{J}$, donc $\pi_2 \circ \pi_1(x) = 0$.
Donc $\ker(\pi_2 \circ \pi_1) = I + J$. Donc $A/(I+J) \sim (A/I)/\bar{J}$.

Correction de l'exercice 11 ▲

1. Soit $J \subset B$ un idéal premier de B. Soient $a, b \in A$ tels que $ab \in f^{-1}(J)$. Alors $f(a)f(b) = f(ab) \in J$ donc $f(a) \in J$ ou $f(b) \in J$. Ainsi, $a \in f^{-1}(J)$ ou $b \in f^{-1}(J)$. On en déduit que $f^{-1}(J)$ est premier.
   Cette proposition n'est pas vraie pour les idéaux maximaux. Par exemple, $A = \mathbb{Z}$, $B = \mathbb{Q}[X]$, $f(k) = k$, et $J = (X)$. Alors $f^{-1}(J) = \{0\}$ n'est pas maximal.
2. Prenons $A = \mathbb{Z}$, $B = \mathbb{Q}$, $f(k) = k$. $f(\mathbb{Z}) = \mathbb{Z}$ n'est pas un idéal de $\mathbb{Q}$ ($1 \in \mathbb{Z}$, $\frac{1}{2} \in \mathbb{Q}$ et pourtant $1 \times \frac{1}{2} \notin \mathbb{Z}$)
   Supposons f surjectif. Soit $x, y \in f(I)$, $a, b \in B$. Il existe $x_0, y_0 \in I$ tels que $x = f(x_0)$ et $y = f(y_0)$. De plus, comme f est surjectif, $\exists a_0, b_0 \in A$ tels que $a = f(a_0)$ et $b = f(b_0)$. Alors $ax + by = f(a_0)f(x_0) + f(b_0)f(y_0) = f(a_0x_0 + b_0y_0)$ et comme I est un idéal, $(a_0x_0 + b_0y_0) \in I$, donc $(ax + by) \in f(I)$.
   $f(I)$ est donc bien un idéal de B.
3. Soit I un idéal maximal de A et $J = f(I)$. Supposons $J \neq B$. Soit K un idéal de B tel que $J \subset K$. Alors $I \subset f^{-1}(K)$, donc $f^{-1}(K) = I$ ou $f^{-1}(K) = A$. Dans le premier cas, on $K = f(f^{-1}(K)) = J$, dans le second cas, on a $K = f(f^{-1}(K)) = f(A) = B$. L'idéal J est donc maximal.
4. $(X+2)(X+3) = X^2 + 5X$ dans $\mathbb{Z}_6[X]$, donc $(X + \bar{2})(X + \bar{3}) \in (X)$, mais $(X + \bar{2}) \notin (X)$ et $(X + \bar{3}) \notin (X)$, donc $r_6((X))$ n'est pas premier dans $\mathbb{Z}_{36}[X]$.
   $(X+1)^2 = (X^2 + 1)$ dans $\mathbb{Z}_2[X]$, or $(X+1) \notin (X^2+1)$, donc $r_2((X^2+1))$ n'est pas premier dans $\mathbb{Z}_2[X]$.

Correction de l'exercice 12 ▲

1. Soit $J = B \cap I$. Soit $x, y \in J$, $a, b \in B$, alors $ax + by \in B$ puisque B est un sous-anneau de A. $ax + by \in I$ puisque I est un idéal. On en déduit que J est un idéal.
   $B + I$ est stable par addition (car B et I le sont). Soit $\alpha = a + x \in B + I$ et $\beta = b + y \in B + I$. Alors $\alpha\beta = (ab) + (ay + bx + xy) \in B + I$, donc $B + I$ est stable par multiplication. $1 \in B + I$, donc $B + I$ est un sous anneau de A. $I \subset B + I$, et I est absorbant pour la multiplication dans A, donc aussi dans B : Iest un idéal de $B + I$.
2. On a le diagramme (de morphismes d'anneaux) suivant :

$$\begin{tikzcd} B \arrow[r, "i"] \arrow[rr, bend left, "\phi"] \arrow[d, "\pi_0"] & B+I \arrow[r, "\pi"] & (B+I)/I \\ B/\ker\phi \arrow[urr, "\sim"'] & & \end{tikzcd}$$

   Or, pour $x \in B$, on a : $x \in \ker\phi \Leftrightarrow x = i(x) \in \ker\pi = I$. Donc $\ker\phi = B \cap I$, et par suite :

$$B/(B \cap I) \sim (B+I)/I.$$
