Théorème 45. Propriété universelle de l'anneau de polynômes en N indéterminées *Soit A un anneau et $N \geqslant 1$ un entier. Soit $\iota\colon A \to A[X_1, \ldots, X_N]$ le morphisme d'anneaux injectif naturel. Soit B un autre anneau. L'application*

$$\begin{array}{rcl} \mathrm{Hom}(A[X_1, \ldots, X_N], B) & \longrightarrow & \mathrm{Hom}(A, B) \times B^N \\ \varphi & \longmapsto & (\varphi \circ \iota, \varphi(X_1), \ldots, \varphi(X_N)) \end{array}$$

est bijective

Démonstration. Cela peut se démontrer de proche en proche en utilisant la propriété universelle de l'anneau de polynômes en une indéterminée et l'identification $A[X_1, \ldots, X_N] = A[X_1, \ldots, X_{N-1}][X_N]$.

On peut aussi en donner une démonstration directe formellement très similaire à la démonstration de la propriété universelle de l'anneau de polynômes en une indéterminée.

Les détails sont laissés aux personnes intéressées. □

Slogan. Se donner un morphisme de $A[X_1, \ldots, X_N]$ vers B, c'est se donner un morphisme de A vers B et N éléments de B.

Remarque. Avec les notations ci-dessus, si $A = B$, pour $\mathbf{a} \in A^N$, le morphisme $\varphi \in \mathrm{Hom}(A[X_1, \ldots, X_N], B)$ correspondant à $(\mathrm{Id}_A, \mathbf{a})$ est le morphisme d'évaluation en $\mathbf{a}$, noté $\mathrm{ev}_{\mathbf{a}}$ ou $P \mapsto P(\mathbf{a})$.

Remarque. Soit A un anneau *intègre* et $N \geqslant 1$ un entier. On a vu en exemple du cours (*cf.* aussi l'exercice 1.5.8) que $A[X]^\times$ est l'ensemble des polynômes constants inversibles dans A. De proche en proche, on en déduit que $A[X_1, \ldots, X_N]^\times$ est l'ensemble des polynômes constants inversibles dans A.

Exemple. Soit $\mathbf{K}$ un corps. On considère l'anneau $\mathbf{K}[X, Y]$ des polynômes en deux indéterminées à coefficients dans $\mathbf{K}$. En se rappelant que $\mathbf{K}[X, Y]$ est isomorphe à $(\mathbf{K}[X])[Y]$ (respectivement $(\mathbf{K}[Y])[X]$), on peut voir un élément de $\mathbf{K}[X, Y]$ comme un polynôme en une variable Y (respectivement X) à coefficients dans $\mathbf{K}[X]$ (respectivement $\mathbf{K}[Y]$) et ceci est souvent utile pour raisonner dans $\mathbf{K}[X, Y]$. Notamment, pour tout élément P de $\mathbf{K}[X, Y]$, on peut définit $\deg_Y(P)$ (respectivement $\deg_X(P)$) comme le degré de P vu comme polynôme en une variable à coefficients dans $\mathbf{K}[X]$ (respectivement $\mathbf{K}[Y]$). Par exemple, si $P = 1 + X^2Y + Y^3$, on a $\deg_X(P) = 2$ et $\deg_Y(P) = 3$. La proposition 37 s'applique (noter que $\mathbf{K}[X]$ et $\mathbf{K}[Y]$ sont intègres).

Montrons que les éléments X et Y de $\mathbf{K}[X, Y]$ sont premiers entre eux, c'est à dire : tout élément P qui divise X et Y est nécessairement un élément de $\mathbf{K}[X, Y]^\times = \mathbf{K}^\times$. Supposons l'existence de $Q \in \mathbf{K}[X, Y]$ tel que $X = PQ$. On en déduit $0 = \deg_Y(X) = \deg_Y(P) + \deg_Y(Q)$, donc nécessairement $\deg_Y(P) = 0$. De même, si P divise Y, on doit

avoir $\deg_X(P) = 0$. Au final, si P divise X et Y, on doit avoir $\deg_X(P) = \deg_Y(P) = 0$, soit $P \in \mathbf{K}$. Comme P divise X et Y, il ne peut pas être nul, donc finalement $P \in \mathbf{K}^\times$. Donc X et Y sont premiers entre eux.

Montrons qu'en dépit de cela, l'idéal $\langle X, Y\rangle$ engendré par X et Y n'est pas égal à $\mathbf{K}[X, Y]$. C'est une différence fondamentale avec la situation sur $\mathbf{Z}$ ou sur $\mathbf{K}[X]$: le théorème de Bézout n'est pas vrai sur $\mathbf{K}[X, Y]$. L'égalité $\langle X, Y\rangle = \mathbf{K}[X, Y]$ entraîne en effet l'existence de $P, Q \in \mathbf{K}[X, Y]$ tels que $P.X + Q.Y = 1$. Évaluons cette dernière égalité en $(0, 0)$. On obtient $0 = 1$, contradiction.

À titre d'exercice, montrez que l'idéal $\langle X, Y\rangle$ est en fait le noyau du morphisme d'évaluation $P \mapsto P(0, 0)$ et que ce n'est pas un idéal engendré par un élément.

2.6 Anneaux quotient (Construire des anneaux à partir d'autres anneaux, partie 2)

Théorème 46. *Soit A un anneau, $\mathcal{I}$ un idéal de A. Il existe un anneau B et un morphisme surjectif $\pi\colon A \to B$ de noyau $\mathcal{I}$.*

Le couple (B, π) est unique à isomorphisme unique près, c'est-à-dire : soit (B_i, π_i), $i \in \{1, 2\}$, deux couples où B_i est un anneau commutatif et $\pi_i\colon A \to B_i$ un morphisme surjectif de noyau $\mathcal{I}$. Alors il existe un unique *isomorphisme d'anneaux $\varphi\colon B_1 \to B_2$ tel que $\varphi \circ \pi_1 = \pi_2$.*

L'anneau B de l'énoncé est appelé *anneau quotient* (de A par $\mathcal{I}$) et noté $A/\mathcal{I}$. Le morphisme π est appelé *morphisme quotient*. L'énoncé d'unicité nous permet moralement de parler de « l' » anneau quotient de A par $\mathcal{I}$ et « du » morphisme quotient.

Exemple. Soit A et B des anneaux, et $\mathcal{I}$ l'idéal $A \times \{0_B\}$ de l'anneau produit $A \times B$. Alors la projection $A \times B \to B$, $(a, b) \mapsto b$ est un morphisme surjectif de noyau $\mathcal{I}$. Donc le quotient $(A \times B)/\mathcal{I}$ s'identifie à B, et le morphisme quotient s'identifie à la projection $A \times B \to B$.

Exemples. 1) *(Une construction des quotients de $\mathbf{Z}$)* Soit N un entier strictement positif. Pour tout entier $a \in \mathbf{Z}$, soit $r_N(a)$ le reste de la division euclidienne de a par N. Soit $\mathcal{Q}$ l'anneau dont l'ensemble sous jacent est l'ensemble $\{0, 1, \ldots, N-1\}$ des entiers compris entre 0 et $N-1$, muni des lois $\oplus$ et $\otimes$ suivantes : si $a_1, a_2 \in \mathcal{Q}$, on pose $a_1 \oplus a_2 := r_N(a_1 + a_2)$ et $a_1 \otimes a_2 := r_N(a_1 \times a_2)$. On vérifie que $(\mathcal{Q}, \oplus, \otimes)$ est bien un anneau et que l'application $\mathbf{Z} \to \mathcal{Q}$ qui à $a \in \mathbf{Z}$ associe $r_N(a) \in \mathcal{Q}$ est un morphisme surjectif de noyau $N\mathbf{Z}$. Ainsi l'anneau $\mathcal{Q}$ est isomorphe à $\mathbf{Z}/N\mathbf{Z}$. En particulier $\mathbf{Z}/N\mathbf{Z}$ est fini de cardinal N.

2) *(Une construction des quotients d'un anneau de polynômes sur un corps)* Soit $\mathbf{K}$ un corps et $P \in \mathbf{K}[X]$ un polynôme non nul. Pour tout polynôme $A \in \mathbf{K}[X]$, soit $r_P(A)$ le reste de la division euclidienne de A par P. Soit $\mathcal{Q}$ l'anneau dont l'ensemble sous

jacent est l'ensemble $\mathbf{K}[X]_{\deg<\deg(P)}$ des polynômes de degré strictement inférieur à $\deg(P)$, muni des lois $\oplus$ et $\otimes$ suivantes : si $A_1, A_2 \in \mathcal{Q}$, on pose $A_1 \oplus A_2 := r_P(A_1 + A_2)$ et $A_1 \otimes A_2 := r_P(A_1 \times A_2)$. On vérifie que $(\mathcal{Q}, \oplus, \otimes)$ est bien un anneau et que l'application $\mathbf{K}[X] \to \mathcal{Q}$ qui à $A \in \mathbf{K}[X]$ associe $r_P(A) \in \mathcal{Q}$ est un morphisme surjectif de noyau $P\mathbf{K}[X]$. Ainsi l'anneau $\mathcal{Q}$ est isomorphe à $\mathbf{K}[X]/P\mathbf{K}[X]$.

3) *(Une généralisation englobant les deux exemples précédents)* Soit A un anneau et $\mathcal{I}$ un idéal de A. Pour $x, y \in A$, la notation $x = y \pmod{\mathcal{I}}$ signifie $x - y \in \mathcal{I}$.

Supposons qu'on ait identifié dans A un « système de représentants modulo $\mathcal{I}$ », c'est à dire une partie S de A et une application $r\colon A \to S$ telle que

1. pour tout $a \in A$, $r(a) = a \pmod{\mathcal{I}}$;
2. pour tous $s_1, s_2 \in S$, on a $s_1 = s_2 \pmod{\mathcal{I}} \Leftrightarrow s_1 = s_2$.

Soit $\mathcal{Q}$ l'anneau dont l'ensemble sous jacent est S muni des lois $\oplus$ et $\otimes$ suivantes : si $s_1, s_2 \in \mathcal{Q}$, on pose $s_1 \oplus s_2 := r(s_1 + s_2)$ et $s_1 \otimes s_2 := r(s_1 \times s_2)$. On vérifie que $(\mathcal{Q}, \oplus, \otimes)$ est bien un anneau et que l'application $A \to \mathcal{Q}$ qui à $x \in A$ associe $r(x) \in \mathcal{Q}$ est un morphisme surjectif de noyau $\mathcal{I}$. Ainsi l'anneau $\mathcal{Q}$ est isomorphe à $A/\mathcal{I}$.

Pour peu que S et $r\colon A \to S$ soit suffisamment « effectifs », ceci peut fournir un moyen pratique de calculer dans $A/\mathcal{I}$. **Attention cependant** à la confusion fréquente signalée dans la remarque ci-dessous.

Remarque. ***L'une des confusions les plus fréquentes dans la manipulation des quotients*** est indéniablement la suivante : en reprenant les notations précédentes, penser (consciemment ou non) que puisque $S \subset A$ peut être vu comme ensemble sous-jacent de $A/\mathcal{I}$, l'anneau quotient $A/\mathcal{I}$« $=$ » S peut être vu comme un sous-anneau de A ; c'est rarement le cas, et basiquement c'est du au fait que les lois $\oplus$ et $\otimes$ définie sur S ne coincident pas avec les lois sur S induites par celles de A (pour lesquelles S n'est d'ailleurs en général pas stable).

Par exemple, si N est un entier strictement positif, $\mathbf{Z}/N\mathbf{Z}$ ne peut pas être un sous-anneau de $\mathbf{Z}$. Penser que si c'était le cas, on aurait $1_{\mathbf{Z}/N\mathbf{Z}} = 1_{\mathbf{Z}}$ et, comme $N \cdot 1_{\mathbf{Z}/N\mathbf{Z}} = 0_{\mathbf{Z}/N\mathbf{Z}} = 0_{\mathbf{Z}}$, on aurait $N \cdot 1_{\mathbf{Z}} = 0_{\mathbf{Z}}$. Manifestation classique de cette confusion : écrire, pour $x, y \in \mathbf{Z}/N\mathbf{Z}$, des choses du genre $x \leqslant y$ (ça n'a pas de sens).

Remarque. À propos des notations des éléments des anneaux quotients. Il n'y a pas réellement de notation standardisée. La notation la plus courante consiste certainement à noter un élément d'un quotient $A/\mathcal{I}$ « comme si » c'était un élément de A (plus précisément, π étant le morphisme quotient, on identifie $x \in A/\mathcal{I}$ à $a \in A$ tel que $x = \pi(a)$) et à se rappeler que l'on calcule en fait dans $A/\mathcal{I}$ et non dans A. C'est très pratique pour alléger l'écriture mais du point de vue pédagogique cela crée assez facilement de graves confusions quand on manque d'expérience dans la manipulation des quotients (*cf.* en particulier la remarque précédente).

Au moins lorsque plusieurs quotients sont en jeu, ce qui arrive fréquemment (*cf.* le théorème chinois ci-dessous), il est prudent de distinguer clairement les morphismes quotients

et les éléments des différents quotients. Pour ce faire, on pourra noter par exemple $a \pmod I$ (un peu lourd) ou $[a]_\mathcal{I}$ l'image de a par le morphisme quotient $A \to A/\mathcal{I}$. Si $n \in \mathbf{Z}$ et $\mathcal{I} = n\mathbf{Z}$, j'écrirai $[a]_n$ pour $[a]_{n\mathbf{Z}}$. On écrira alors par exemple $[3]_4 + [2]_4 = [1]_4$.

En liaison avec les exemples ci-dessus, soulignons que dans certain cas, d'autres représentations intéressantes des éléments du quotient peuvent exister ; *cf.* notamment le cas de $\mathbf{K}[X]/P\mathbf{K}[X]$ discuté un peu plus tard.

Remarque. D'après les propositions 20 et 27, si $\pi\colon A \to A/\mathcal{I}$ est le morphisme quotient, $\mathcal{J} \mapsto \pi(\mathcal{J})$ est une bijection naturelle de l'ensemble des idéaux de A contenant $\mathcal{I}$ sur l'ensemble des idéaux de $A/\mathcal{I}$, qui induit une bijection de l'ensemble des idéaux premiers de A contenant $\mathcal{I}$ sur l'ensemble des idéaux premiers de $A/\mathcal{I}$.

Définition. (déjà utilisée ci-dessus) Soit A un anneau, $\mathcal{I}$ un idéal de A. Pour $(x, y) \in A^2$, la notation $x = y \pmod{\mathcal{I}}$ (ou $x \Leftrightarrow y \pmod{\mathcal{I}}$) se lit « x est congru à y modulo $\mathcal{I}$ », ou « x est égal à y modulo $\mathcal{I}$ » et signifie que $x - y \in \mathcal{I}$.

Démonstration. Démonstration de l'existence On prend pour ensemble sous-jacent à B l'ensemble quotient de A pour la relation d'équivalence $\mathcal{R}_\mathcal{I}$ sur A définie par

$$\forall x \in A, \quad \forall y \in A, \quad x \,\mathcal{R}_\mathcal{I}\, y \iff x = y \pmod{\mathcal{I}}.$$

Soit alors $\pi\colon \begin{array}{ccc} A & \longrightarrow & B \\ x & \longmapsto & \overline{x} \end{array}$ l'application qui à $x \in A$ associe sa $\mathcal{R}_\mathcal{I}$-classe d'équivalence. Pour $x, y \in A$, on pose $\overline{x} + \overline{y} := \overline{x+y}$ et $\overline{x} \times \overline{y} := \overline{x \times y}$.

On vérifie que ceci est bien défini, qu'on obtient ainsi deux lois de composition interne sur B qui en font un anneau, d'éléments neutres $\overline{0_A}$ pour la première loi et $\overline{1_A}$ pour la seconde lois, et que π est un morphisme d'anneaux surjectif de noyau $\mathcal{I}$. Le plus laborieux dans ce qui précède est certainement la première étape, c'est à dire vérifier que les définitions du paragraphe précédent sont valides. Les étapes suivantes en sont une conséquence quasi-immédiate si l'on comprend bien ce qu'il y a à démontrer. Noter que pour la première étape, il s'agit de montrer que pour tous $x, y, x', y' \in A$ tels que $\overline{x} = \overline{x'}$ et $\overline{y} = \overline{y'}$, on a $\overline{x+y} = \overline{x'+y'}$ et une propriété analogue pour la multiplication.

L'unicité découlera de la démonstration du théorème suivant. □

Remarque. Avec les notations ci-dessus, le fait que π soit bien défini et soit un morphisme d'anneaux se traduit concrètement par la compatibilité des congruences modulo $\mathcal{I}$ à l'addition et à la multiplication : si $x = y \pmod{\mathcal{I}}$ et $z = t \pmod{\mathcal{I}}$ alors $x + z = y + t \pmod{\mathcal{I}}$ et $xz = yt \pmod{\mathcal{I}}$.

La notion d'anneau quotient n'est en un certain sens rien d'autre qu'une « incarnation abstraite » du calcul modulaire (ou calcul des congruences).

Remarque. Il y a deux raisons pour lesquelles je ne développe pas plus en détail la démonstration de l'existence. Premièrement, et à l'instar d'autres démonstrations de résultats de ce chapitre, c'est typiquement le genre d'exercice de manipulation des définitions que

vous devriez être capable de faire en autonomie. Deuxièmement, l'auteur de ces lignes est intimement convaincu que la connaissance de la construction « abstraite » de l'anneau quotient n'est strictement d'aucune utilité pour manipuler des quotients dans la pratique, et peut même avoir tendance à obscurcir considérablement l'appréhension de la notion de quotient ; cette remarque ne se limite pas à la notion de quotient d'anneaux et fait écho à la remarque qui suit l'énoncé du théorème 22 du chapitre 1 du cours (pour mémoire : disponible en ligne sur le site du cours).

Théorème 47. PROPRIÉTÉ UNIVERSELLE DE L'ANNEAU QUOTIENT - THÉORÈME DE FACTORISATION *Soit A un anneau, $\mathcal{I}$ un idéal de A, $\pi\colon A \to A/\mathcal{I}$ le morphisme quotient.*

Soit B un anneau et $\varphi\colon A \to B$ un morphisme d'anneaux dont le noyau contient $\mathcal{I}$. Alors il existe un unique morphisme d'anneaux $\psi\colon A/\mathcal{I} \to B$ tel que $\psi \circ \pi = \varphi$

En outre :

- *ψ est surjectif si et seulement si φ est surjectif ;*
- *ψ est injectif si et seulement si $\mathrm{Ker}(\varphi) = \mathcal{I}$.*

En particulier, si φ est surjectif de noyau $\mathcal{I}$, il existe un unique isomorphisme d'anneaux $\psi\colon A/\mathcal{I} \xrightarrow{\sim} B$ tel que $\varphi = \psi \circ \pi$.

Ce théorème est un outil de base fondamental pour travailler avec des anneaux quotient, notamment pour constuire des morphismes de source un anneau quotient.

Slogan. Se donner un morphisme d'anneaux de $A/\mathcal{I}$ vers B, c'est se donner un morphisme d'anneaux de A vers B dont le noyau contient $\mathcal{I}$.

De façon un peu moins informelle : A anneau et $\mathcal{I}$ idéal étant fixés (soit $\pi\colon A \to A/\mathcal{I}$ le morphisme quotient), pour tout anneau B, l'application qui à $\psi \in \mathrm{Hom}(A/\mathcal{I}, B)$ associe $\psi \circ \pi \in \mathrm{Hom}(A, B)$ permet d'identifier $\mathrm{Hom}(A/\mathcal{I}, B)$ et $\{\varphi \in \mathrm{Hom}(A, B), \quad \mathcal{I} \subset \mathrm{Ker}(\varphi)\}$.

Slogan. Pour montrer que l'anneau B est isomorphe à l'anneau quotient $A/\mathcal{I}$, il suffit de construire un morphisme surjectif $A \to B$ de noyau $\mathcal{I}$.

Démonstration. On va démontrer le théorème 47 en remplaçant $\pi\colon A \to A/\mathcal{I}$ par n'importe quel morphisme d'anneaux $\pi\colon A \to C$ surjectif de noyau $\mathcal{I}$. Ceci montrera l'unicité dans le théorème 46 ainsi que le théorème 47.

Choisissons une section ensembliste $s\colon C \to A$ de π, c'est-à-dire une application $C \to A$ telle que $\pi \circ s = \mathrm{Id}_C$.

ATTENTION, il n'est pas possible en général de prendre pour s un morphisme d'anneaux.

REMARQUE POUR LES PURISTES : on utilise l'axiome du choix ; en fait et plus précisément, l'existence d'une section ensembliste pour toute application surjective est une des formes sous lesquelles on peut énoncer l'axiome du choix.

Supposons l'existence de ψ comme dans l'énoncé. On a alors

$$\varphi \circ s = \psi \circ \pi \circ s = \psi$$

d'où l'unicité d'un tel morphisme ψ (oui, en dépit du choix arbitraire de s).

Montrons à présent que $\psi := \varphi \circ s$ est bien un morphisme d'anneaux.

Soit $c, c' \in C$. Alors $s(c + c')$ et $s(c) + s(c')$ ont même image par π, à savoir $c + c'$. Donc $s(c + c') - (s(c) + s(c')) \in \mathcal{I}$.

Comme $\mathcal{I} \subset \mathrm{Ker}(\varphi)$, on a bien $\varphi(s(c+c')) = \varphi(s(c)+s(c'))$. Comme φ est un morphisme d'anneaux, on en déduit

$$\varphi(s(c + c')) = \varphi(s(c)) + \varphi(s(c'))$$

d'où

$$\psi(c + c') = \psi(c) + \psi(c').$$

De même $s(cc')$ et $s(c)s(c')$ ont même image par π, à savoir cc'. Donc $s(cc') - s(c)s(c') \in \mathcal{I}$. On en déduit $\varphi(s(cc'))) = \varphi(s(c)s(c'))$.

Enfin $s(1_C)$ et 1_A ont même image par π, à savoir 1_B. Donc $\varphi s(1_C) = \varphi(1_A) = 1_B$, donc $\psi(1_C) = 1_B$.

Montrons que $\varphi \circ s \circ \pi = \varphi$. Soit $a \in A$. Alors $\pi \circ s \circ \pi(a) = \pi(a)$, donc $s \circ \pi(a) - a \in \mathrm{Ker}(\pi)$. On en déduit $\varphi(s \circ \pi(a)) = \varphi(a)$.

Si φ est surjective, comme $\psi\pi = \varphi$, ψ est également surjective.

Si ψ est surjective, comme $\psi\pi = \varphi$ et π est surjective, ψ est également surjective.

On a $\mathrm{Ker}(\psi) = \pi(\mathrm{Ker}(\varphi))$, donc ψ est injective si et seulement si $\pi(\mathrm{Ker}(\varphi) = \{0\}$ si et seulement si $\mathrm{Ker}(\varphi)$ est contenu dans $\mathrm{Ker}(\pi)$. Comme $\mathrm{Ker}(\pi) = \mathcal{I}$ et $\mathcal{I}$ est contenu dans $\mathrm{Ker}(\varphi)$, on obtient le résultat. □

Comme corollaire immédiat du théorème précédent, on obtient divers « théorèmes d'isomorphisme ». Basiquement, un théorème d'isomorphisme identifie sous certaines hypothèses deux quotients construits « différemment ».

Théorème 48. Théorèmes d'isomorphisme

1. *Soit $\varphi\colon A \to B$ un morphisme d'anneaux.*
   (a) *Le morphisme φ induit un isomorphisme de $A/\mathrm{Ker}(\varphi)$ sur l'anneau $\mathrm{Im}(\varphi)$. En particulier, si φ est surjectif, φ induit un isomorphisme de $A/\mathrm{Ker}(\varphi)$ sur B. De manière générale, l'anneau quotient $A/\mathrm{Ker}(\varphi)$ est toujours isomorphe à un sous-anneau de B.*
   (b) *Supposons φ surjectif. Soit $\mathcal{J}$ un idéal de B. Alors la composition de φ avec le morphisme quotient $B \to B/\mathcal{J}$ induit un isomorphimse de $A/\varphi^{-1}(\mathcal{J})$ sur $B/\mathcal{J}$.*

(c) *Supposons φ surjectif. Soit $\mathcal{I}$ un idéal de A. Alors la composition de φ avec le morphisme quotient $B \to B/\varphi(\mathcal{I})$ induit un isomorphisme de $A/(\mathcal{I}+\mathrm{Ker}(\varphi))$ sur $B/\varphi(\mathcal{I})$.*

2. *Soit $\mathcal{I}$ un idéal de A. On note $\pi_{\mathcal{I},X}\colon A[X] \to (A/\mathcal{I})[X]$ l'unique morphisme qui envoie X sur X et qui induit le morphisme $A \to (A/\mathcal{I})[X]$ donné par la composition des flèches naturelle $A \to A/\mathcal{I} \to (A/\mathcal{I})[X]$. Soit $\mathcal{J}$ un idéal de $A[X]$. Alors la composition du morphisme $\pi_{\mathcal{I},X}$ avec le morphisme quotient $(A/\mathcal{I})[X] \to (A/\mathcal{I})[X]/\pi_{\mathcal{I},X}(\mathcal{J})$ induit un isomorphisme de $A[X]/(\mathcal{I}\cdot A[X]+\mathcal{J})$ sur $(A/\mathcal{I})[X]/\pi_{\mathcal{I},X}(\mathcal{J})$.*

Remarque. Si $\varphi\colon A \to B$ est un morphisme d'anneaux non surjectif, on peut toujours se ramener au cas surjectif en remplaçant B par le sous-anneau $\mathrm{Im}(\varphi)$.

Remarque. On reprend les notations de l'énoncé. La définition du morphisme $\pi_{\mathcal{I},X}$ utilise la propriété universelle de l'anneau de polynômes en une indéterminée. Concrètement, le morphisme $\pi_{\mathcal{I},X}$ s'obtient en réduisant modulo $\mathcal{I}$ les coefficients d'un polynôme à coefficients dans A. Plus précisément, si $\pi_{\mathcal{I}}\colon A \to A/\mathcal{I}$ est le morphisme quotient et $P = \sum_{n=0}^{+\infty} a_n X^n \in A[X]$, alors $\pi_{\mathcal{I},X}(P) = \sum_{n=0}^{+\infty} \pi_{\mathcal{I}}(a_n)X^n \in (A/I)[X]$

Démonstration. 1(a) découle aussitôt du théorème 47. 1(b) et 1(c) découlent de 1(a) en calculant les noyaux des compositions de morphismes considérées (calcul laissé à titre d'exercice).

Montrons l'assertion 2. La remarque précédente montre que le morphisme $\pi_{\mathcal{I},X}$ est surjectif. L'assertion 2 découlera alors de 1(c) une fois montré l'égalité $\mathrm{Ker}(\pi_{\mathcal{I},X}) = \mathcal{I}\cdot A[X]$. Soit $\mathcal{I}[X] \subset A[X]$ l'ensemble des polynômes à coefficients dans $\mathcal{I}$. On vérifie que $\mathcal{I}[X]$ est un idéal de $A[X]$ contenant $\mathcal{I}$, et que tout idéal de $A[X]$ contenant $\mathcal{I}$ contient $\mathcal{I}[X]$. Ainsi $\mathcal{I}\cdot A[X] = \mathcal{I}[X]$. Le fait que $\mathrm{Ker}(\pi_{\mathcal{I},X}) = \mathcal{I}[X]$ découle alors aussitôt de la remaque précédente. □

Exemple. Soit $\pi\colon \mathbf{Z}[X] \to \mathbf{C}$ l'unique morphisme d'anneaux qui envoie X sur i. L'image de π est l'anneau des entiers de Gauss $A = \mathbf{Z}[i]$, qui contient $\mathbf{Z}$ comme sous-anneau. Soit p un nombre premier. On s'intéresse à la question suivante : l'idéal $p\cdot A$ est-il un idéal premier de A ? On verra plus tard que dans le cas de l'anneau $\mathbf{Z}[i]$ cette question est équivalente à demander si p est un élément irréductible de $\mathbf{Z}[i]$.

On va répondre à cette question en calculant le quotient $A/p.A$ sous une autre forme, en utilisant notamment le théorème précédent.

Tout d'abord, montrons que le noyau de π est l'idéal $(X^2+1)\cdot\mathbf{Z}[X]$.

On a $\pi(X^2+1) = i^2+1 = 0$ donc $X^2+1 \in \mathrm{Ker}(\pi)$. Comme $\mathrm{Ker}(\pi)$ est un idéal, $\mathrm{Ker}(\pi)$ contient nécessairement l'idéal engendré par X^2+1, soit $(X^2+1)\cdot\mathbf{Z}[X]$.

Montrons l'inclusion réciproque $\mathrm{Ker}(\pi) \subset (X^2+1)\cdot\mathbf{Z}[X]$. Soit $P \in \mathrm{Ker}(\pi)$. Le polynôme X^2+1 étant **UNITAIRE**, on peut appliquer le théorème de division euclidienne et on obtient l'existence de $Q, R \in \mathbf{Z}[X]$, avec $\deg(R) < \deg(X^2+1) = 2$, tels que $P = (X^2+1).Q + R$. En appliquant à cette égalité le morphisme d'évaluation en i, on obtient $0 = 0.Q(i) + R(i)$, soit $R(i) = 0$. Comme $\deg(R) < 2$, il existe $a, b \in \mathbf{Z}$ tels que $R = aX + b$. Ainsi $ai + b = 0$. Par identification des parties réelle et imaginaire, on obtient $a = b = 0$, soit $R = 0$ et $P = (X^2+1).Q$ ce qui conclut.

Noter que $p \cdot A$ est l'image par π de l'idéal $\mathcal{I} = p\mathbf{Z}[X]$. Une application du 1(c) du théorème 48 montre alors que la composition de π avec le morphisme quotient $A \to A/p\cdot A$ induit un isomorphisme $A/p\cdot A \xrightarrow{\sim} \mathbf{Z}[X]/\langle p, X^2+1\rangle$.

Maintenant, si on note $n \mapsto [n]_p$ le morphisme quotient $\mathbf{Z} \to \mathbf{Z}/p\mathbf{Z}$, le 2 du théorème 48 montre que $\mathbf{Z}[X]/\langle p, X^2+1\rangle$ est lui-même isomorphe à $(\mathbf{Z}/p\mathbf{Z})[X]/\langle X^2 + [1]_p\rangle$. Ainsi, en utilisant le théorème 58, $p\cdot A$ est un idéal premier de A si et seulement si $A/p\cdot A$ est intègre si et seulement si $(\mathbf{Z}/p\mathbf{Z})[X]/\langle X^2+[1]_p\rangle$ est intègre si et seulement si $\langle X^2+[1]_p\rangle$ est un idéal premier de $(\mathbf{Z}/p\mathbf{Z})[X]$.

Comme p est premier, $\mathbf{Z}/p\mathbf{Z}$ est un corps. Ainsi $\langle X^2+[1]_p\rangle$ est un idéal premier de $(\mathbf{Z}/p\mathbf{Z})[X]$ si et seulement si $X^2+[1]_p$ est irréductible, et comme ce polynôme est de degré 2, cela équivaut à la condition que $X^2+[1]_p$ n'a pas de racine.

En résumé : $p\cdot\mathbf{Z}[i]$ est un idéal premier de $\mathbf{Z}[i]$ si et seulement si -1 n'est pas un carré modulo p. On (re)verra un peu plus tard comment cette dernière condition s'exprime explicitement en termes de congruences.