Arithmétique et algèbre commutative

§1. Anneaux et corps.

1.1. *Définitions d'anneaux, corps, morphismes.*

On rappelle du cours d'algèbre multilinéaire qu'un ensemble de "scalaires" dans lequel addition, soustraction et multiplication sont possibles, et dont les éléments peuvent par exemple être utilisés comme coefficients dans une matrice, est appelé un *corps* si tout élément non nul est inversible (pour la multiplication), et que sans cette hypothèse on parle d'un *anneau*. On a vu les exemples de l'anneau $\mathbf{Z}$ des entiers, et l'anneau $K[X]$ de polynômes en X à coefficients dans un corps K, mais on verra dans ce cours que les possibilités pour définir des anneaux sont vastes.

1.1.1. Définition. *Un anneau est un ensemble R muni d'opérations '$+$' : $R \times R \to R$, '$-$' : $R \to R$, '$\times$' : $R \times R \to R$, ainsi que des constantes notées $0_R, 1_R \in R$, tel que soit vérifié pour tout $a, b, c \in R$:*
(1) $0_R + a = a = a + 0_R$,
(2) $(-a) + a = 0_R = a + (-a)$,
(3) $a + (b + c) = (a + b) + c$,
(4) $a + b = b + a$,
(5) $1_R \times a = a = a \times 1_R$
(6) $a \times (b \times c) = (a \times b) \times c$,
(7) $a \times (b + c) = (a \times b) + (a \times c)$,
(8) $(a + b) \times c = (a \times c) + (b \times c)$.
On appelle R un anneau commutatif si en plus pour tout $a, b \in R$:
(9) $a \times b = b \times a$.
On appelle un anneau R (commutatif ou non) un corps si
(10) $1_R \neq 0_R$, *et pour tout $a \in R$ avec $a \neq 0_R$ il existe $b \in R$ tel que $a \times b = 1_R = b \times a$.*
Un anneau commutatif qui est aussi un corps est appelé un corps commutatif.

On a omis dans cette définition quelques propriétés simples qui se déduisent facilement de celles données. Les axiomes (1)–(4) disent que R muni de '$+$' est un groupe abélien avec élément neutre 0_R, et $-a$ l'élément inverse de a pour tout a. En particulier $a \in R$ vérifie $a = a + a$ seulement si $a = 0_R$ (additionner $-a$ des deux cotés et simplifier), donc de $a \times 0_R = a \times (0_R + 0_R) = (a \times 0_R) + (a \times 0_R)$ on peut conclure que $a \times 0_R = 0_R$ pour tout $a \in R$, et on montre de la même façon que $0_R \times a = 0_R$. De $0_R = a \times 0_R = a \times ((-b) + b) = (a \times (-b)) + a \times b$ on déduit que $a \times (-b) = -(a \times b)$ et de la même façon $(-a) \times b = -(a \times b)$; en particulier $(-1_R) \times a = -a$ (donc au lieu de la négation '$-$' il suffirait de connaître la seule valeur $-1_R \in R$, mais le fait d'avoir cette opération facilite la formulation des axiomes).

Comme il est habituel, on écrira désormais ab au lieu de $a \times b$ (sauf dans certains rares cas où la juxtaposition ab serait ambiguë), on écrira pas de parenthèses dans les situations où les règles (3) ou (6) disent que les différents possibilités donnent le même résultat. On convient aussi que les parenthèses peuvent être omises dans une expression de la forme $(ab) + c$ ou $a + (bc)$ (c'est-à-dire multiplication a priorité sur addition) ou encore $(-a)b$ ou $-(ab)$ (les deux possibilités étant égales) ou $(-a)+b$ (soustraction unaire a priorité sur addition) ou $a+(-b)$ (pas de confusion possible). En fait on écrira $a-b$ pour $a+-b$, introduisant ainsi encore une opération '$-$' à deux arguments, et un nouveau potentiel d'ambiguïté que le lecteur saura néanmoins parfaitement résoudre sans que l'on lui explique comment (et il comprendra également qu'il ne faudra pas supprimer le '$\times$' dans $a \times -b$). Pour $n \in \mathbf{N}$ et $a \in R$ on introduit aussi la notation a^n, définie récursivement par $a^0 = 1_R$ et $a^{n+1} = a^n \times a$ pour tout $n \in \mathbf{N}$, comme abréviation.

1.1.2. Définition. *Soit R, S deux anneaux (éventuellement confondus). Une application $f : R \to S$ est un morphisme d'anneaux si elle vérifie, pour tout $a, b \in R$:*
(1) $f(a + b) = f(a) + f(b)$ *dans S,*
(2) $f(ab) = f(a)f(b)$ *dans S,*
(3) $f(1_R) = 1_S$.
Si R et S sont des anneaux commutatifs on appelle en tel f un morphisme d'anneaux commutatifs, et de façon similaire si R est S sont des corps (commutatifs) on appelle f un morphisme de corps (commutatifs).

On observe que $f(0_R) = f(0_R + 0_R) = f(0_R) + f(0_R)$ donc $f(0_R) = 0$ (le même type d'argument ne marche pas pour déduire condition (3) de (2), car $a = a^2$ a en général d'autres solutions que $a = 1_R$, par exemple $a = 0_R$; c'est la raison pour laquelle il est nécessaire d'exiger la condition (3) explicitement). Puis $0_S = f(0_R) = f(a + -a) = f(a) + f(-a)$ montre que $f(-a) = -f(a)$ pour tout $a \in R$. On peut conclure que si un morphisme d'anneaux $f : R \to S$ est appliqué à une expression quelconque dans R qui utilise uniquement le langage des anneaux (c'est-à-dire des éléments de R combinés avec les opérations et les constantes figurant dans la définition 1.1.1), alors le résultat sera égal à celui obtenu en appliquant f séparément à tous les éléments de R dans l'expression, et en combinant les avec les mêmes opérations et constantes (mais qui représente maintenant des opérations et des constantes dans S). À titre d'exemple, on montrera sans problème que $f\big((a-b^2)(ab+(-c+1_R)^3)\big) = (f(a)-f(b)^2)\times(f(a)f(b)+(-f(c)+1_S)^3)$; l'exemple montre que les abbréviations $a - b$ et a^n passent aussi bien "à travers f" que '+' et '×', mais il ne faut évidemment pas appliquer f aux exposants $2, 3$, qui ne désignent pas des éléments de R.

Comme *toute* notion de morphisme, deux morphismes d'anneaux $R \to S$ et $S \to T$ se composent pour donner un morphisme $R \to T$. Un morphisme d'anneaux $R \to S$ permet de traduire toute équation valable dans R en une équation valable dans S. Un autre morphisme $S \to R$ permettra une traduction dans l'autre sens, et si en plus les morphismes composés $R \to S \to R$ et $S \to R \to S$ sont l'identité sur R respectivement sur S, alors on a une correspondance entre R et S qui permet de les considérer comme parfaitement équivalent en tant que anneaux (ou en tant que corps, s'ils le sont). Cette idée est formalisée dans la notion d'un isomorphisme: c'est un morphisme qui admet un morphisme réciproque (une description valable pour tout type de morphisme). En fait (comme avec d'autre types de morphismes en algèbre) un isomorphisme d'anneaux est la même chose qu'un morphisme d'anneaux bijectif ; mais le point important reste que l'application réciproque soit aussi un morphisme d'anneaux.

1.1.3. Définition/Proposition. *Un morphisme d'anneaux $f : R \to S$ pour lequel il existe un autre morphisme $g : S \to R$ tel que $g(f(r)) = r$ pour tout $r \in R$ et $f(g(s)) = s$ pour tout $s \in S$ est appelé un isomorphisme d'anneaux. Pour qu'un morphisme d'anneaux f soit un isomorphisme, il faut et il suffit que f soit une application bijective, et dans ce cas $g = f^{-1}$ sera son morphisme réciproque.*

Preuve. Une application $g : S \to R$ satisfaisant les deux relations est précisément une application réciproque de f, et on sait bien qu'elle existe si et seulement si f est bijectif. Ce qui est à vérfier est que g sera un morphisme d'anneaux si f l'est. Or c'est facile : pour la premère condition on a $g(s + t) = g\big(f(g(s)) + f(g(t))\big) = g\big(f\big(g(s) + g(t)\big)\big) = g(s) + g(t)$, de façon similaire pour la seconde $g(s \times t) = g\big(f(g(s)) \times f(g(t))\big) = g\big(f\big(g(s) \times g(t)\big)\big) = g(s) \times g(t)$, et finalement $g(1_S) = g(f(1_R)) = 1_R$. □

La notion d'un isomorphisme peut être utile de deux manières. Quand on établit un isomorphisme entre deux anneaux construits différemment, on montre qu'ils sont malgré cela essentiellement le même anneau (on dit qu'ils sont isomorphes) ; on pourra par exemple ainsi montrer l'équivalence algébrique de différentes constructions du corps $\mathbf{C}$. Un autre type d'utilisation est quand on a un isomorphisme $R \to R$ (un *automorphisme* de R) distinct de l'identité : cela établit une *symétrie* de l'anneau R qui peut être utile pour comprendre ses propriétés. Un exemple de cette situation est la conjugaison complexe $\mathbf{C} \to \mathbf{C}$.

On remarque que les axiomes d'un anneau ou d'un anneau commutatif (c'est-à-dire (1)–(9) de la définition 1.1.1) sont tous de la forme d'*égalités*, valables pour tous les éléments de R *sans exception*. En fait, la théorie des anneaux commutatifs résume toutes les règles habituelles de réécriture d'expressions qui sont valables sans aucune considération des valeurs des (sous)-expressions, notamment qui ne font pas intervenir des divisions ou de simplifications par un facteur multiplicatif (car ces deux ne sont pas valables pour 0). Pour cette raison cette théorie est souvent le bon cadre pour des propriétés qui sont obtenues (en principe) par une (longue) chaîne d'égalités. Un exemple est la formule du binôme :

$$(x + y)^n = \sum_{i=0}^{n} \binom{n}{i} x^{n-i} y^i \qquad \text{pour } n \in \mathbf{N},$$

qui pour chaque n peut en principe être démontrée en écrivant simplement $(x + y)^n$ comme produit de n facteurs $x + y$, et en appliquant les règles distributives (7),(8), ainsi que d'autre règles pour regrouper les termes dans le résultat (évidemment on montre en réalité la formule pour tout n à la fois, avec un

argument par de récurrence). Cette simple considération de la démonstration montre que la formule du binôme est valable dans tout anneau commutatif R, avec $x, y \in R$ quelconques. En affirmant cela, on a l'obligation de s'expliquer sur les coefficients binomiaux $\binom{n}{i}$, qui sont après tout des éléments de $\mathbf{N}$ et non pas de R. Mais au même titre que 0_R et 1_R, il est clair que $2_R = 1_R + 1_R$ désigne un élément bien déterminé dans R, tout comme $3_R = 2_R + 1_R$, et ainsi de suite. On formule cela de façon précise.

1.1.4. Proposition/Définition. *Si R est un anneau, alors il existe un morphisme d'anneaux unique $\mathbf{Z} \to R : i \mapsto i_R$. Quand un nombre $i \in \mathbf{Z}$ représente un élément de R dans une expression, il désigne i_R.*

Preuve. Montrons d'abord l'unicité du morphisme, c'est-à-dire que chaque valeur i_R est bien déterminée. Déjà 0_R et 1_R sont donnés par la définition 1.1.2. Si i_R est bien défini pour $i \geq 0$, alors la condition 1.1.2(1) donne $(i+1)_R = i_R + 1_R$, donc par récurrence i_R est bien déterminé pour $i \in \mathbf{N}$; finalement $(-i)_R = -(i_R)$ fixe les images des nombre négatifs. Prouver que ceci définit vraiment un morphisme d'anneaux nécessite plus de travail, un peu pénible, mais à faire une fois pour toutes. Il s'agit d'évoquer la propriété spécifique de $\mathbf{Z}$ que ses opérations '+' et '×' peuvent toutes deux être exprimées en termes de l'opération "successeur" $i \mapsto i + 1$. Par construction l'application $f : i \mapsto i_R$ vérifie $f(i + 1) = f(i) + 1_R$ pour tout $i \in \mathbf{Z}$: pour $i \geq 0$ c'était la définition de $f(i + 1)$, et pour $i < 0$ on a, avec $k = -(i + 1) \geq 0$, que $f(i + 1) = f(-k) = -f(k) = -(f(k + 1) - 1_R) = -f(k + 1) + 1_R = f(-(k + 1)) + 1_R = f(i) + 1_R$. Pour en déduire que $f(a + b) = f(a) + f(b)$, on peut fixer a et faire d'abord récurrence sur $b \geq 0$ (car $f(a+0) = f(a) = f(a)+f(0)$ est clair, et de $f(a+b) = f(a)+f(b)$ on déduit $f(a+(b+1)) = f((a+b)+1) = f(a+b)+1_R = f(a)+f(b)+1_R = f(a)+f(b+1)$), et ensuite utiliser $f(a) = f((a-b)+b) = f(a-b)+f(b)$ pour conclure que $f(a - b) = f(a) - f(b) = f(a) + f(-b)_R$ aussi. La vérification que $f(ab) = f(a)f(b)$ pour tout $a, b \in \mathbf{Z}$ est similaire, en utilisant $a(b + 1) = ab + b$ dans $\mathbf{Z}$ pour réduire par récurrence le cas d'une multiplication à celui des additions déjà traité ; on laisse au lecteur le soin des fournir les détails. □

Le fait de pouvoir utiliser des entiers dans des expressions dans R est extrêmement commode ; sinon on serait obligé d'écrire par exemple $x + x + x$ au lieu de $3x$. La propriété que $i \mapsto i_R$ est un morphisme d'anneaux est essentielle pour justifier cette pratique, car sans elle il ne serait pas autorisé d'effecteur l'arithmétique usuelle sur les entiers lorsqu'ils désignent des éléments de R. Heureusement on n'a donc pas ce souci, et toutes les équations valables dans $\mathbf{Z}$ restent valables dans R. Ceci dit, la même chose n'est pas vraie pour leurs négations $a \neq b$, car le morphisme n'est pas toujours injectif : bien que $0 \neq 2$ dans $\mathbf{Z}$, il peut arriver que dans R on ait $0_R = 2_R$, comme il est le cas dans l'anneau $R = \mathbf{Z}/2\mathbf{Z}$. Dans un anneau on n'exclut même pas la possibilité $0_R = 1_R$ (mais elle est explicitement exclue pour un corps). Mais si c'est le cas, alors $a = 1_R a = 0_R a = 0$ pour tout $a \in R$, donc $R = \{0_R\}$ est l'*anneau trivial*. En général $n_R = 0$ entraîne $n_R a = 0$ pour tout $a \in R$. Dans la suite on n'écrira plus i_R mais simplement i.

Encore un peu de terminologie et notation. Si pour $a \in R$ il existe $b \in R$ tel que $ab = 1 = ba$, on dit que a est *inversible* dans R. Si c'est le cas, l'élément b est unique (en supposant qu'on ait aussi $ac = 1 = ca$, on conclut $c = 1c = (ba)c = b(ac) = b1 = b$), et est appelé l'inverse (multiplicatif) de a, noté $b = a^{-1}$. Cette notation suggère un prolongement de la notation a^n aux exposants négatifs par $a^{-n} = (a^{-1})^n$, et en effet on montre sans difficulté que cette ce prolongement conserve les propriétés habituelles, par exemple $a^n a^m = a^{n+m}$ pour tout $n, m \in \mathbf{Z}$. Mais contrairement aux notations précédentes, celle-ci n'est définie que si a est inversible. L'élément 1_R est toujours inversible (car $1_R 1_R = 1_R$), mais 0_R n'est jamais inversible (sauf si R est l'anneau trivial, où $0_R = 1_R$), car on a $0_R b = 0_R$ quel que soit $b \in R$. D'après l'axiome (10), R est un corps si et seulement si tous les éléments de R sont inversibles, sauf 0_R.

1.1.5. Définition/Proposition. *Pour un anneau R, on désigne par $R^\times$ l'ensemble des ses éléments inversibles, qui muni de la multiplication forme un groupe, appelé le groupe multiplicatif de R.*

Preuve. La seule chose à montrer c'est que $R^\times$ est fermé pour la multiplication, car il est clair que $1 \in R^\times$ est élément neutre, l'associativité est garantie par les axiomes d'un anneau, et $a^{-1} \in R$ existe pour tout $a \in R^\times$ par définition de celui-ci, avec comme inverse a, donc $a^{-1} \in R^\times$. Mais le produit ab de deux inversibles $a, b \in R^\times$ est toujours inversible avec inverse $b^{-1}a^{-1}$, car $abb^{-1}a^{-1} = aa^{-1} = 1 = b^{-1}a^{-1}ab$. □

Il est grand temps de donner quelques exemples d'anneaux et de corps. L'anneau le plus fondamental est celui des entiers $\mathbf{Z}$. Les seuls éléments inversibles dans $\mathbf{Z}$ sont 1 et -1 (et chacun est son propre

inverse), donc $\mathbf{Z}$ est très loin d'être un corps. On peut rendre les entiers non nuls inversibles, en étendant $\mathbf{Z}$ aux nombres rationnels $\mathbf{Q}$, qui forment un corps (c'est le plus petit corps qui contient $\mathbf{Z}$). Les nombres réels $\mathbf{R}$ forment un corps plus grand (*beaucoup* plus grand du point de vue algébrique), et les nombres complexes $\mathbf{C}$ un corps encore plus grand (un tout petit peu plus grand du point de vue algébrique). (Il existe des corps encore beaucoup plus grand que $\mathbf{C}$, mais il faudrait un peu de préparation pour les décrire.) Les inclusions $\mathbf{Z} \to \mathbf{Q} \to \mathbf{R} \to \mathbf{C}$ sont des exemples de morphismes d'anneaux commutatifs (et de corps pour les deux derniers).

Des anneaux plus petits existent aussi : calcul modulaire fournit des anneaux $\mathbf{Z}/n\mathbf{Z}$ qui sont finis (un tel anneau existe pour tout entier $n > 0$, mais ce ne sont pas les seuls anneaux finis). Ces anneaux sont parfois des corps (on verra que c'est les cas quand n est un nombre premier). Le morphisme canonique $\mathbf{Z} \to \mathbf{Z}/n\mathbf{Z}$ (envoyant un nombre vers sa classe modulo n) est un exemple d'un morphisme d'anneaux non injectif (en revanche celui-ci est surjectif). On connaît aussi des anneaux de polynômes $R[X]$; on s'y est intéressé pour des questions en algèbre linéaire (valeurs propres) quand R est un corps, mais ces anneaux sont définis quand R est n'importe quel anneau. (Ceci dit, il faut mettre en garde que certaines propriétés qu'on attend des anneaux de polynômes ne sont valables que si R est commutatif ; aussi on verra que les bonnes propriétés arithmétiques auquel on s'est habitué lorsque R est un corps ne se généralisent pas aux anneaux commutatifs.) Des exemples d'un anneau non-commutatif sont donnés par les anneaux $\mathrm{End}(E)$ des endomorphismes d'un espace vectoriel E de dimension finie $d > 1$, ou encore ceux des matrices $n \times n$ (avec $n > 1$) sur un anneau R quelconque. Ces exemples ne sont jamais des corps, mais il existe néanmoins des corps non commutatifs, qui sont toujours infinis ; le plus connu est le corps $\mathbf{H}$ des quaternions (de Hamilton), qui est une extension non commutative du corps $\mathbf{C}$.

Une remarque est à sa place concernant les anneaux non commutatifs. Il ne sont pas un sujet important dans ce cours (d'où l'«algèbre commutative» du titre), et comme la théorie des anneaux commutatifs est assez différente de celle des anneaux non commutatifs, ils seront laissés à côté dès qu'on arrive aux résultats un peu détaillés. Il est vrai que l'étude de $\mathrm{End}(E)$ sera entreprise vers la fin de ce cours, mais ce n'est pas la théorie générale des anneaux non commutatifs qui sera mise en œuvre pour le faire. Si l'on considère au départ le cas non commutatif, c'est d'une part pour montrer que certains résultats sont d'une telle généralité qu'ils ne dépendent pas de l'hypothèse de la commutativité, et d'autre part pour indiquer plus précisément à quels moments cette hypothèse apporte une différence essentielle.

1.2. *Sous-anneaux, caractéristique, intégrité.*

Dans l'algèbre linéaire, et dans la théorie de groupes, l'étude de sous-structures (sous-espaces vectoriels, sous-groupes) est d'une importance fondamentale. La théorie des anneaux connaît une telle notion aussi, tout comme la théorie des corps.

1.2.1. Définition. *Si R est un anneau, une partie S de R est un sous-anneau de R si*
(1) pour tout $s, t \in S$ on a $s + t \in S$ et $-t \in S$,
(2) S est fermé pour la multiplication : pour tout $s, t \in S$ on a $st \in S$,
(3) $1_R \in S$.
Dans le cas où R et S sont des corps, on appelle S un sous-corps de R.

Dans la liste il manque la condition $0_R \in S$, mais cela résulte de $1_R \in S$, $-1_R \in S$ et $0_R = 1_R + -1_R$. Un sous-anneau S est donc fermé pour les opérations du langage des anneaux (qui *n'inclut pas* l'opération "inverse") et contient 0 et 1, donc S muni des restrictions adaptées des opérations, et les mêmes constantes 0 et 1 que R, peut être considéré comme un anneau en soi. En effet, les conditions (1)–(9) de la définition 1.1.1 étant toutes des égalités, leur validité dans R implique évidement celle dans S (et en particulier S sera commutatif si R est commutatif). Un anneau non commutatif peut avoir un sous-anneau commutatif (en fait on verra que tout anneau contient au moins un sous-anneau commutatif), et si S est un sous-anneau de R, chacun peut être un corps sans que l'autre ne le soit (le corps $\mathbf{Q}$ contient $\mathbf{Z}$ qui n'est pas un corps, et tout corps K est contenu dans l'anneau $K[X]$ qui n'est pas un corps). On vérifie qu'un sous-anneau S d'un corps est un sous-corps si et seulement si $a^{-1} \in S$ pour tout $a \in S \setminus \{0\}$.

1.2.2. Proposition. *Si $f : S \to R$ est un morphisme d'anneaux, l'image $f(S)$ est un sous-anneau de R.*

Preuve. Les conditions de la définition 1.1.2 impliquent que $f(S)$ est fermé pour '+' et '×' et contient 1_S ; or on a vu que $f(-a) = -f(a)$ pour tout $a \in S$, donc $f(S)$ est aussi fermé pour l'opération $t \mapsto -t$. □

Réciproquement, si S est sous-anneau de R, l'inclusion $S \to R$ est un morphisme (injectif) d'anneaux dont l'image est évidement S ; les sous-anneaux sont précisément les images de morphismes d'anneaux.

Il découle des propositions 1.1.4 et 1.2.2 que dans tout anneau R, l'ensemble des éléments i_R pour $i \in \mathbf{Z}$, c'est-à-dire l'image du morphisme $\mathbf{Z} \to R$, forme un sous-anneau, qui est le sous-anneaux minimal de R (et par ailleurs R lui-même est son sous-anneau maximal). Si le morphisme $\mathbf{Z} \to R$ est injectif, ce sous-anneau est isomorphe à $\mathbf{Z}$ et on dit que la *caractéristique* de l'anneau R, noté "char R", est 0. Sinon $\operatorname{char} R$ est plus petit entier $n > 0$ avec $n_R = 0_R$, et le sous-anneaux minimal de R est isomorphe à $\mathbf{Z}/n\mathbf{Z}$. Pour $m \in \mathbf{Z}$, l'équation $m_R = 0_R$ est donc vraie si et seulement si m est un multiple de $\operatorname{char} R$.

Les anneaux $\mathbf{Z}$ et ceux de la forme $\mathbf{Z}/n\mathbf{Z}$ sont égaux à leur sous-anneau minimal, et ces anneaux ne contiennent donc pas de sous-anneaux propres. Il st clair que le corps $\mathbf{Q}$ contient proprement $\mathbf{Z}$ (son sous-anneau minimal), mais celui-ci est loin d'être le seul sous-anneau propre de $\mathbf{Q}$. Un exemple d'un autre tel sous-anneau de $\mathbf{Q}$ est l'ensemble des fractions irréductibles $\frac{p}{q}$ dont le dénominateur q est impair ; cela résulte du fait que tout produit de nombres impairs est impair (ce qui permet des sommes et des produits d'être écrits avec dénominateur impair), et tout diviseur d'un nombre impair est impair (ce qui garantit qu'un dénominateur impair le reste après simplification d'une fraction à sa forme irréductible). Mais on pourra définir des sous-anneaux de $\mathbf{Q}$ de manière semblable, en remplaçant les nombres impairs comme dénominateurs par d'autres ensembles : par exemple par les puissances de 2, ou par les entiers n'ayant pas de facteurs premiers autres que 2 et 5 (ce qui donne le sous-anneau des nombres décimaux, c'est-à-dire ayant un développement décimal *fini*). En fait on pourra limiter les facteurs premiers dans les dénominateurs à *n'importe quel* sous-ensemble des nombres premiers pour obtenir un sous-anneau de $\mathbf{Q}$ (l'exemple avec les nombre impairs est obtenu en admettant tous les nombres premiers sauf 2), et cela montre que l'ensemble des sous-anneaux de $\mathbf{Q}$ est infini, et même *non dénombrable*.

Un autre exemple d'un sous-anneau, et qui est d'un intérêt particulier, est celui des *entiers de Gauss* $\mathbf{Z}[\mathbf{i}] = \{\, a + b\,\mathbf{i} : a, b \in \mathbf{Z} \,\}$ dans le corps $\mathbf{C}$. La définition des opérations dans $\mathbf{C}$ rend évident que les conditions pour un sous-anneau sont vérifiées. Comme aucun élément z de ce sous-anneau n'a $0 < |z| < 1$, on voit que $\mathbf{Z}[\mathbf{i}]^\times$ est réduit aux éléments $1, \mathbf{i}, -1, -\mathbf{i}$ de module 1, et c'est donc loin d'être un sous-corps de $\mathbf{C}$. On peut cependant former un sous-corps de $\mathbf{C}$ autour de $\mathbf{Z}[\mathbf{i}]$, le corps $\mathbf{Q}[\mathbf{i}] = \{\, a + b\,\mathbf{i} : a, b \in \mathbf{Q} \,\}$ des rationnels de Gauss (la formule $\frac{1}{a+b\,\mathbf{i}} = \frac{a-b\,\mathbf{i}}{a^2+b^2}$, pour $a, b \in \mathbf{Q}$ pas tous nuls, montre que $\mathbf{Q}[\mathbf{i}]$ est un corps). On peut trouver beaucoup de sous-anneaux d'une manière semblable. On voit sans problème que pour tout entier $n > 0$ l'ensemble $\mathbf{Z}[\sqrt{n}\,\mathbf{i}] = \{\, a + b\sqrt{n}\,\mathbf{i} : a, b \in \mathbf{Z} \,\}$ est aussi un sous-anneau de $\mathbf{C}$, avec comme inversibles seulement $1, -1$ si $n > 1$. On peut également considérer $\mathbf{Z}[\sqrt{n}\,] = \{\, a + b\sqrt{n} : a, b \in \mathbf{Z} \,\}$, qui est un sous-anneau de $\mathbf{R}$ pour essentiellement les mêmes raisons (à savoir les formes de $x_1 + x_2$, $-x_1$ et x_1x_2 où $x_i = a_i + b_i\sqrt{n} \in \mathbf{Z}[\sqrt{n}\,]$ pour $i = 1, 2$, par exemple $x_1x_2 = a_1b_1 + na_2b_2 + (a_1b_2 + a_2b_1)\sqrt{n} \in \mathbf{Z}[\sqrt{n}\,]$). Il est clair qu'il s'agit de $\mathbf{Z}$ quand $\sqrt{n}$ est entier (c'est-à-dire n un carré parfait), mais dans le cas contraire c'est un sous-ensemble dense de $\mathbf{R}$. Ses inversibles sont donnés par $\mathbf{Z}[\sqrt{n}\,]^\times = \{\, a + b\sqrt{n} : a^2 - nb^2 \in \mathbf{Z}^\times = \{1, -1\} \,\}$, dont on peut montrer que c'est le produit direct de $\mathbf{Z}^\times \subset \mathbf{Z}[\sqrt{n}\,]$ avec $\mathbf{Z}[\sqrt{n}\,]^\times \cap \mathbf{R}_{>0}$, et ce dernier facteur est un groupe cyclique (c'est-à-dire engendré par un seul élément) et infini (la partie dure à prouver est $\mathbf{Z}[\sqrt{n}\,]^\times \cap \mathbf{R}_{>0} \neq \{1\}$).

On vérifie sans problème que chaque anneau $\mathbf{Z}[\sqrt{n}\,\mathbf{i}]$ possède un automorphisme non trivial (c'est-à-dire distinct de l'identité) défini par $a + b\sqrt{n}\,\mathbf{i} \mapsto a - b\sqrt{n}\,\mathbf{i}$; il s'agit bien évidemment d'une restriction de la conjugaison complexe. Mais si on regarde de près ce qui fait que cette application soit un morphisme, on s'aperçoit que l'essentiel est que le nombre $\sqrt{n}\,\mathbf{i}$ partage avec son opposé $-\sqrt{n}\,\mathbf{i}$ la propriété d'avoir carré $-n \in \mathbf{Z}$ (quelle propriété intervient dans le calcul d'un produit $(a + b\sqrt{n}\,\mathbf{i})(c + d\sqrt{n}\,\mathbf{i})$). De ce point de vue il n'est pas étonnant que les anneaux $\mathbf{Z}[\sqrt{n}\,]$ (avec n pas un carré parfait) admettent eux aussi un automorphisme non trivial, défini par $a + b\sqrt{n} \mapsto a - b\sqrt{n}$. Mais cet automorphisme n'est pas une restriction de la conjugaison complexe, après tout $\mathbf{Z}[\sqrt{n}\,]$ est contenu dans les nombres réels. En fait, pour la restriction de la topologie de $\mathbf{R}$, cet automorphisme est une application qui est *partout discontinue*.

Ces exemples montrent que la recherche des sous-anneaux de R n'est pas très utile comme moyen d'obtenir des renseignements de la structure de R : d'une part il y a en général trop, et d'autre part un sous-anneau peut avoir des propriétés assez différentes que celles de R. On verra qu'il est beaucoup plus utile d'étudier les possibles *quotients* de R. En revanche, il est parfois utile de connaître certains anneaux S dans lesquels R se plonge (plus précisément, tel que R admette un morphisme injectif $R \to S$).

Outre la distinction entre éléments inversible et non inversibles, il y a un autre phénomène qui permet de distinguer différent types d'éléments de R, et qui est illustré par l'équation $2_R \times 5_R = 10_R = 0_R$ qui est valable dans l'anneau $R = \mathbf{Z}/10\mathbf{Z}$. Dans ce cas le produit de deux éléments non nuls de R donne l'élément nul de R, et on appellera ces éléments 2_R et 5_R des "diviseurs de zéro" dans R (mais pas "diviseur de 0", car 0 est multiple de *tout* élément de R). Ce phénomène un peu dérangeant ne se produit heureusement pas dans tout anneau, par exemple pas dans $\mathbf{Z}$, ni dans un corps ou dans un sous-anneau d'un corps.

1.2.3. Définition. *Si R est un anneau commutatif, un élément $a \in R$ est dit régulier si la condition $ab = 0$ pour $b \in R$ implique $b = 0$. Un élément non nul et non régulier est dit diviseur de zéro. Un anneau intègre est un anneau non trivial qui ne contient aucun diviseur de zéro.*

Un élément a est donc diviseur de zéro si et seulement s'il existe b tel que $ab = 0$, où a, b sont tous deux non-nuls. Un élément de R est soit nul, soit diviseur de zéro, soit régulier (sauf que dans l'anneau trivial l'unique élément est à la fois nul et régulier). Les anneaux intègre sont caractérisés par l'absence dus cas "diviseur de zéro", et il est clair que tout sous-anneau d'un anneau intègre est intègre.

On a volontairement exclu les anneaux non commutatifs de cette définition ; on pourrait y distinguer les diviseurs de zéro à gauche (dans le rôle de a) et les diviseurs de zéro à gauche (dans le rôle de b), mais le cas non-commutatif nous n'intéressera pas. En fait on accorde aussi un moindre intérêt aux anneaux avec diviseurs de zéro, du moins en ce qui concerne les questions de divisibilité (c'est ce que les mathématiciens appellent "l'arithmétique"). La raison est que si a est diviseur de zéro, alors même si m est multiple de a, il n'y a pas de quotient m/a unique, car on pourra toujours y ajouter un multiple de b avec $ab = 0$.

1.2.4. Proposition. *Un élément régulier a de R est (multiplicativement) simplifiable, ce qui veut dire que la condition $ax = ay$ pour $x, y \in R$ entraîne $x = y$.*

Preuve. On a $0 = ax - ay = a(x - y)$, et comme a est régulier cela implique $x - y = 0$, et donc $x = y$. □

Dans un anneau intègre on peut donc, comme on en a l'habitude dans les corps, simplifier par tout élément non nul. Dans un anneau avec diviseurs de zéro par contre, on ne pourra simplifier qu'après avoir vérifié que l'élément par lequel on simplifie est régulier.

1.2.5. Proposition. *Tous élément inversible d'un anneau commutatif R est régulier.*

Preuve. Si a est inversible et $ab = 0$, alors $0 = a^{-1}0 = a^{-1}ab = b$. □

1.2.6. Corollaire. *Tout corps est un anneau intègre.*

Preuve. Un corps n'est pas l'anneau trivial, et tout élément non nul y est inversible, donc régulier. □

On verra plus tard (construction du corps des fractions) que tout anneau commutatif intègre peut être vu comme un sous-anneau d'un corps commutatif. Comme réciproquement tout sous-anneau d'un corps est intègre, cela permet donc de caractériser les anneaux commutatifs intègres comme les anneaux qui sont (isomorphes à) un sous-anneau d'un corps commutatif. En fait les propriétés concrètes du corps des fractions de R dépendent étroitement des propriétés arithmétiques de R, à l'instar de la relation entre $\mathbf{Z}$ et $\mathbf{Q}$ où déjà le calcul des fractions irréductibles se fait en termes du pgcd dans $\mathbf{Z}$; cela explique aussi notre intérêt particulier pour l'arithmétique des anneaux commutatifs intègres.

Il est intéressant d'observer que les propriétés d'un élément $a \in R$ d'être inversible ou régulier peuvent être caractérisés par des propriétés de l'opération $R \to R$ de multiplication par a, c'est-à-dire $x \mapsto ax$. Cette opération n'est pas un morphisme d'anneaux, mais c'est un endomorphisme du groupe additif $(R, +)$.

1.2.7. Proposition. *Soit R un anneau commutatif, $a \in R$ et $m_a : R \to R$ défini par $m_a(x) = ax$.*
(1) L'élément a est inversible dans R si et seulement si m_a est surjectif.
(2) L'élément a est régulier dans R si et seulement si m_a est injectif.

Preuve. Si m_a est surjectif il existe en particulier $b \in R$ tel que $m_a(b) = b$; alors $ab = 1$ et a possède b comme inverse. Réciproquement si a est inversible, alors pour tout $x \in R$ on a $m_a(a^{-1}x) = aa^{-1}x = x$, donc m_a est surjectif. Si m_a est injectif et $ab = 0$, alors $m_a(b) = ab = 0 = m_a(0)$ et donc $b = 0$ par l'injectivité de m_a. Réciproquement si a est régulier et $m_a(x) = m_a(y)$, cela veut dire $ax = ay$, ce qui d'après la proposition 1.2.4 entraîne $x = y$, donc m_a est injectif. □

1.2.8. Proposition. *Soit R un anneau commutatif qui est soit fini, soit il contient un sous-corps K tel que R, vu comme espace vectoriel sur K (la multiplication scalaire étant la multiplication de l'anneau R) est de dimension finie. Alors R est un corps si et seulement si R est intègre.*

Preuve. On sait déjà que tout corps est intègre, montrons donc l'implication réciproque dans les cas considérés. On suppose donc R un anneau intègre, dans lequel on considère $a \in R \setminus \{0\}$, qui est donc régulier. La proposition 1.2.7 nous dit que la multiplication $m_a : R \to R$ est injective. Si R est fini cela implique que m_a est aussi surjective (c'est une forme du principe des tiroirs : si $x \in R$ n'était pas dans l'image de m_a, alors m_a définirait une application $R \to R \setminus \{x\}$ dont l'ensemble d'arrivée est strictement plus petit que l'ensemble fini de départ, et ledit principe assure l'existence de $y \in R \setminus \{x\}$ ayant au moins deux antécédents, contredisant l'injectivité de m_a). Dans le cas où R est de dimension fini sur un sous-corps K, la multiplication m_a est un endomorphisme du K-espace vectoriel R, pour lequel (grâce à la dimension fine) l'injectivité entraîne également la surjectivité (c'est le théorème du rang : le noyau de m_a est de dimension 0, donc la dimension de son image est celle de l'espace entier, et m_a est surjectif). Et la surjectivité de m_a veut dire que a est inversible. □

La considération des anneaux finis $R = \mathbf{Z}/n\mathbf{Z}$ confirme cette proposition. D'un coté si n est composé, disons $n = ab$ avec $a, b > 1$ et donc aussi $a, b < n$, alors on aura $a_R b_R = n_R = 0_R$ avec $a_R, b_R \neq 0_R$, à l'instar de ce qu'on a vu pour $n = 10$, $a = 2$ et $b = 5$; dans ce cas R n'est pas intègre. Par contre si $R = \mathbf{Z}/p\mathbf{Z}$ où p est un nombre premier, alors pour tout $a \in \mathbf{Z}$ tel que $a_R \neq 0_R$, c'est-à-dire qui n'est pas multiple de p, on a $\operatorname{pgcd}(a, p) = 1$, donc il existe des coefficients (de Bezout) $s, t \in \mathbf{Z}$ avec $1 = as + pt$, et alors $a_r s_R = 1_R$ d'où a_R est inversible, et R est un corps. (On n'a pas eu besoin de la proposition 1.2.7.)

Un anneau R avec $\operatorname{char} R = n > 0$ contient $\mathbf{Z}/n\mathbf{Z}$ comme sous-anneau (minimal), et celui-ci possède des diviseurs de zéro si n est composé, donc R ne peut être intègre que si n est un nombre premier. Donc

1.2.9. Fait. *Un anneau intègre est soit de caractéristique* 0*, soit de caractéristique p avec p premier.* □

Ce fait explique l'intérêt particulier qu'on porte, parmi les caractéristiques non nulles, au cas de la caractéristique p avec p premier; en fait la phrase "caractéristique p" sera réservée à ce cas, et la précision "p premier" est souvent omise dans la pratique. En caractéristique p on a une circonstance remarquable :

1.2.10. Proposition. *Soit R un anneau commutatif de caractéristique p. Alors*

$$(x + y)^p = x^p + y^p. \qquad \text{pour tout } x, y \in R. \tag{1}$$

Par conséquence l'application $R \to R$ définie par $x \mapsto x^p$ est un morphisme d'anneaux, dit "de Frobenius".

Preuve. La dernière partie découle de la première, car $(xy)^p = x^p y^p$ et $1^p = 1$ sont valables dans tout anneau commutatif, indépendamment de la caractéristique. La première partie est obtenue de la formule du binôme dans R, en remarquant que le coefficient binomial $\binom{p}{k}$ est divisible par le nombre premier p pour $0 < k < p$, et donc $\binom{p}{k}_R = 0_R$. Voici deux preuve algébrique et combinatoire de cette divisibilité. Dans l'expression

$$\frac{p \times (p-1) \times \cdots \times (p-k+1)}{k \times (k-1) \times \cdots \times 1} = \binom{p}{k} \in \mathbf{N}, \tag{2}$$

aucun facteur du dénominateur $k!$ n'est divisible par p, donc le facteur premier p du numérateur divise le quotient. Alternativement on peut considérer l'action par permutations cycliques du groupe cyclique

d'ordre p sur la collection des $\binom{p}{k}$ k-sous-ensembles de $\{1, 2, \ldots, p\}$, dont les orbites, ne pouvant pas être réduites à un seul point, contiennent chacune précisément p de tels sous-ensembles distincts. □

Si $f : R \to S$ est un morphisme d'anneaux, le fait que la composée de morphismes $\mathbf{Z} \to R \to S$ donne l'unique morphisme $\mathbf{Z} \to S$ entraîne que la caractéristique de R est multiple de celle de S. En particulier si $\operatorname{char} S = 0$ on doit avoir $\operatorname{char} R = 0$, et dans l'autre sens si $\operatorname{char} R = p$ est un nombre *premier*, alors $\operatorname{char} S = p$ aussi, à moins que S ne soit l'anneau trivial (c'est-à-dire $\operatorname{char} S = 1$; on ne peut pas l'exclure car *tout* anneau possède un morphisme unique vers l'anneau trivial). La caractéristique donne donc une classification grossière des anneaux qui restreint les possibilités de morphismes entre eux. Une chaîne de surjections telle que $\mathbf{Z} \to \mathbf{Z}/12\mathbf{Z} \to \mathbf{Z}/6\mathbf{Z} \to \mathbf{Z}/3\mathbf{Z} \to \mathbf{Z}/1\mathbf{Z} = \{0\}$ montre que pour les morphismes surjectifs d'anneaux $R \to S$ on ne pourra pas déduire de l'intégrité de l'un de R et S l'intégrité de l'autre (mais dans le cas d'un morphisme injectif on a vu que S intègre implique R intègre).

Mentionnons finalement que étant donné deux anneaux R, S (et il est permis d'avoir $R = S$), on peut définir leur produit direct $R \times S$. C'est une construction fort simple de construire des anneaux, mais qui ne donnera jamais des nouveaux anneaux *intègres*. On munit le produit cartésien $R \times S$ d'une structure d'anneau (commutatif si R est S le sont) en définissant les opérations et les constantes composante par composante, par exemple $(r, s) \times (r', s') = (rs, r's')$ et $1_{R\times S} = (1_R, 1_S)$. Le fait qu'on n'obtient jamais un nouvel anneau intègre vient de l'égalité $(1_R, 0_S) \times (0_R, 1_S) = (0_R, 0_S) = 0_{R\times S}$ qui se produit quel que soit R, S, donc $R \times S$ possède toujours des diviseurs de zéro (sauf si R ou S est l'anneau trivial, auquel cas $R \times S$ est isomorphe à l'autre facteur). On définit également le produit $\prod_{i\in I} R_i$ d'une famille (finie ou non) d'anneaux, toujours avec les opérations séparés dans chaque composante, et l'anneau R^I qui en est un cas particulier en prenant $R_i = R$ pour tout i (comme un élément de R^I est spécifié en donnant indépendamment pour chaque $i \in I$ un élément $r_i \in R$, il s'agit de l'ensemble des fonctions $I \to R$).

Dans tous ces anneaux, un élément est diviseur de zéro dès qu'il possède au moins une composante nulle et aussi une composante non-nulle (pour une fonction dans R^I cela veut dire : dès qu'elle s'annule quelque part, mais pas partout), car il suffit de multiplier par un élément dont les composantes complémentaires sont nulles pour obtenir un produit nul. En vue de cette prolifération de diviseurs de zéro, il est plutôt étonnant est que, pour R intègre et infini, l'anneau de fonctions $R \to R$ possède des sous-anneaux *intègres* et assez grands, notamment le sous-anneau des fonction polynomiales (car on verra que celui-ci est alors isomorphe à l'anneau $R[X]$, qui est intègre). Cette circonstance met à l'évidence le fait qu'un diviseur de zéro a dans un anneau A n'est pas forcément diviseur de zéro dans tout sous-anneau S de A qui contient a : il se peut que tout $b \in R$ vérifiant $ab = 0$ se trouve dans $R \setminus S$.

1.3. *Idéaux, quotients.*

L'image d'un morphisme d'anneaux $f : R \to S$ est un sous-anneau S' de S, et on peut décomposer f comme la composée d'un morphisme d'anneaux $\tilde{f} : R \to S'$ et de l'inclusion $S' \to S$. Ce dernier facteur est évidemment injectif, et $\tilde{f}$ est par construction surjectif. Considérons maintenant le facteur surjectif.

Par définition de l'image, tout $s \in S'$ s'écrit $s = f(r)$ pour au moins un $r \in R$, et le fait que f est un morphisme implique que toute opération sur de tels s peut être exprimée en termes d'opérations dans R. Ceci permet donc de décrire le sous-anneau S' de S entièrement en termes de l'anneau R, ce qu'on va détailler maintenant.

La relation $r \sim r'$ sur R définie par la condition $f(r) = f(r')$ est clairement une relation d'équivalence. La classe de r est associée à $f(r) \in S'$; ainsi l'ensemble S' est ainsi en bijection avec l'ensemble des classes d'équivalence pour cette relation. La relation '$\sim$' elle-même est déterminée par la seule classe $\ker(f) = \{\, r \in R : f(r) = 0 \,\}$ associée à $0 \in S'$, car $f(r) = f(r')$ est équivalent à $f(r - r') = 0$, donc à $r - r' \in \ker(f)$. On appelle $\ker(f)$ le *noyau* de f, et c'est le même ensemble que le noyau de f vu comme morphisme de groupes additifs. En particulier $\ker(f)$ est un sous-groupe de $(R, +)$, mais tout tel sous-groupe ne peut pas être le noyau d'un morphisme d'anneaux. La caractérisation prise de ces ensemble est donné par la notion d'un *idéal* d'un anneau commutatif.

1.3.1. Définition. *Soit R un anneau commutatif. Une partie $I \subseteq R$ est un idéal de R si :*
(1) un sous-groupe de $(R, +)$: on a $0 \in I$, et I est fermé pour l'addition et pour la soustraction ;
(2) pour tout $a \in R$, l'ensemble I est fermé pour la multiplication par a : on a $ax \in I$ dès que $x \in I$.

Si on fait la comparaison avec la définition d'un sous-anneau, on voit qu'on a la condition d'être un sous-group additif dans les deux cas, mais que la condition de fermeture multiplicative est nettement plus forte dans le cas d'un idéal, car pour un sous-anneau il suffit d'être fermé que pour la multiplication par *ses propres éléments*. Par contre la condition de contenir 1_R qu'on impose aux sous-anneaux est absente pour les idéaux, et pour cause : si un idéal contient 1, il doit d'après la seconde condition contenir tout $a \in R$, et donc être égal à l'anneau R tout entier. Le cas $I = R$ est permis pour un idéal, mais pas très intéressant ; on appelle un idéal I *propre* si $I \neq R$, et un idéal propre ne contient donc jamais 1. En fait un idéal propre ne contient aucun élément inversible $u \in R^\times$, car s'il le faisait il devait aussi contenir $u^{-1}u = 1$. On voit donc que malgré la ressemblance de leurs définitions, les notions de sous-anneau de d'idéal sont assez différentes, et aucun idéal propre n'est sous-anneau de R.

Il est facile de vérifier que le noyau d'un morphisme d'anneaux $f : R \to S$ est toujours un idéal : comme $\ker(f)$ est aussi le noyau de f considéré comme du morphisme de groupes additifs, il est sous-groupe du groupe additif de R (en fait même sous-groupe distingué, mais cela ne rajoute rien pour un groupe commutatif), et pour $x \in \ker(f)$ et $a \in R$ on a $f(ax) = f(a)f(x) = f(a)0 = 0$ donc $ax \in \ker(f)$.

Réciproquement tout idéal de R peut figurer comme le noyau d'un morphisme d'anneaux défini sur R ; autrement dit, on n'a pas oublié d'exiger des conditions dans la définition 1.3.1.

1.3.2. Proposition [existence d'anneaux quotients]. *Soit R un anneau, et I un idéal. Il existe un morphisme d'anneaux surjectif $R \to S$ dont le noyau est égal à I.*

On construira en fait l'anneau S et le morphisme $R \to S$ à partir de R et de I ; on les appellera le quotient de R par I, noté $S = R/I$, et la *projection canonique* $R \to R/I$. Les éléments de R/I sont des *classes modulo* I, et la projection canonique associe à chaque élément $r \in R$ sa classe $r + I$ modulo I.

Preuve. Dans la théorie de groupes on construit le quotient R/I du groupe additif de R par son sous-groupe (distingué) I, et la projection canonique $R \to R/I$ comme morphisme de groupes additifs. Les éléments de R/I sont des sous-ensembles $a + I = \{\, a + i : i \in I \,\}$ de R (les classes), qui forment une partition de R (pour $a, b \in R$ on a soit $a + I = b + I$, ce qui arrive dès que $b \in a + I$, soit $a + I$ est $b + I$ sont disjoints), et la projection canonique est donnée par $a \mapsto a + I$. L'addition des classes est donnée par $(a + I) +_{R/I} (b + I) = (a + b) + I$, ce qui exprime précisément que la projection canonique est un morphisme de groupes. Cette addition est bien définie, car la classe $(a + b) + I$ ne dépend pas du choix des représentants a, b de leurs classes respectives. Il reste à munir R/I d'une multiplication '$\times_{R/I}$' qui en fasse un anneau, qui rende la projection canonique un morphisme d'anneaux.

Pour que la projection canonique devienne morphisme d'anneaux, il faut que $(a + I) \times_{R/I} (b + I) = (ab) + I$ pour tout $a, b \in R$. Cette équation servira de définition de la multiplication, mais il est nécessaire de vérifier que la classe $(ab) + I$ ne dépende pas du choix de a, b dans leurs classes, sinon la définition serait contradictoire (c'est le point crucial de la démonstration, le reste est facile). Soit donc $a' \in a + I$ et $b' \in b + I$ deux autres représentants de ces classes ; il existe donc $x, y \in I$ tels que $a' = a + x$ et $b' = b + y$. Il s'agit de montrer que $(a'b') + I = (ab) + I$, ce qui sera le cas si $a'b' \in (ab) + I$. Or on a $a'b' = (a + x)(b + y) = ab + ay + xb + xy$, et les termes ay, xb, et xy sont tous les trois dans I, car chacun des ces produits contient au moins un facteur dans I, qui est un idéal. La somme de ces termes reste dans I, ce qui montre que $a'b' \in (ab) + I$ comme voulu.

Pour compléter la structure d'anneau de R/I on définit 0 et 1 respectivement comme les classes $0 + I$ et $1 + I$, et $-(a + I)$ est l'inverse additif de $a + I$, à savoir $(-a) + I$. Comme toutes les opérations sont définies en utilisant des représentants des classes, et les axiomes d'un anneau (commutatif) sont toutes des égalités inconditionnelles, chacun découle pour R/I directement de celui pour R ; à titre d'exemple on a pour l'axiome (7) de distributivité : $(a+I)\times((b+I)+(c+I)) = (a+I)\times((b+c)+I) = (a(b+c))+I = (ab+ac)+I = ((ab)+I)+((ac)+I) = ((a+I)\times(b+I))+((a+I)\times(c+I))$ (tout cela devient plus lisible en écrivant $\overline{x}$ pour $x + I$; on obtient : $\overline{a} \times (\overline{b} + \overline{c}) = \overline{a} \times \overline{b + c} = \overline{a(b + c)} = \overline{ab + ac} = \overline{ab} + \overline{ac} = (\overline{a}\,\overline{b}) + (\overline{a}\,\overline{c})$). Ayant vérifié que R/I est un anneau, il est clair que la projection canonique $R \to R/I$ qui à $a \in R$ associe sa classe $a + I$ dans R/I est un morphisme d'anneaux (c'est l'essence même de définir les opérations sur les classes en termes de représentants), qui est surjectif et dont le noyau est I. □

L'anneau R lui-même est un idéal de R, et le quotient R/R est l'anneau trivial (une raison importante pour ne pas interdire l'anneau trivial est justement pour assurer la validité générale de la construction d'un anneau quotient). Mais pour un idéal propre I, le quotient R/I n'est pas trivial. Une conséquence de la caractérisation des idéaux comme des noyaux de morphismes est que pour un morphisme d'anneaux $f : S \to R$ l'image réciproque $f^{-1}(I) = \{ s \in S : f(s) \in I \}$ d'un idéal (propre) I de R est un idéal (propre) de S : c'est le noyau du morphsime composé $S \to R \to R/I$. Si f est l'inclusion d'un sous-anneau $S \subseteq R$, ceci dit que l'intersection d'un idéal propre I avec un sous-anneau S est toujours un idéal propre de S.

En revenant sur la définition d'un idéal, on pourra dire, même si il n'y a pas d'implication dans un sens ou l'autre, que ses conditions sont en général plus difficile à satisfaire que celles d'un sous-anneau. On a déjà observé qu'un idéal propre de R ne saura contenir aucun élément de $R^\times$. Si R est un corps, cela veut dire que la seule possibilité pour un idéal propre est $I = \{0\}$, qui en effet en est un (comme c'est le cas dans tout anneau non trivial, car c'est le noyau de l'identité $R \to R$). En particulier $\mathbf{Q}$, dont on a vu qu'il a de très nombreux sous-anneaux, ne possède, étant un corps, que les deux idéaux $\mathbf{Q}$ et $\{0\}$.

Néanmoins il existe une simple construction qui produit un idéal à partir d'un élément $a \in R$ quelconque, à savoir l'ensemble $aR = \{ ar : r \in R \}$ de tous les multiples de a (la vérification que c'est un idéal est facile), appelé l'*idéal principal* engendré par a. Cet idéal ne sera pas toujours différent quand a change, et on à $aR = R$ pour tout $a \in R^\times$. Mais si a n'est pas inversible, aR est un idéal propre (car 1 n'est multiple de a que si a est inversible), et on voit en particulier que dans les anneaux commutatifs R qui ne sont pas des corps, des idéaux propres et non nuls existent toujours. On verra que l'étude de la structure de R repose en grande partie sur l'étude de ses idéaux, et donc de ses possibles quotients R/I.

Il résulte du fait que $\{0\}$ est le seul idéal propre d'un corps K que tout morphisme de corps est *injectif*, et plus généralement tout morphisme d'anneaux $K \to R$ est injectif, sauf si R est l'anneau trivial. Les relations entre les corps se résument donc essentiellement aux extensions de corps, le plongement d'un corps dans un corps plus grand. Il ne faut néanmoins pas oublier qu'il y a aussi les automorphismes d'un corps K (morphismes bijectifs $K \to K$), et ils jouent un rôle central dans la théorie structurelle des corps dite théorie de Galois ; c'est une belle théorie, mais qu'on ne traitera pas dans ce cours, ni dans le programme de la Licence de mathématiques. Du point de vue des anneaux (commutatifs intègres), le cas des corps est le plus simple possible, car "toute l'arithmétique a disparu" : tous les éléments non nuls sont (devenus) inversibles, d'où aucune question de divisibilité intéressante se pose.

Le cas des idéaux principaux montre qu'on peut "construire" des idéaux en commençant avec un petit ensemble, et en y rajoutant d'autres éléments exigés par la définition d'idéal. Une autre construction dans le même esprit est la somme de deux (ou plusieurs) idéaux : si I, J sont deux idéaux (par exemple des idéaux principaux) on peut former $I + J = \{ i + j : i \in I, j \in J \}$, dont on voit facilement que c'est un idéal, et en fait le plus petit idéal qui englobe à la fois I et J comme sous-ensemble. En fait, pour une partie quelconque P de R, il existe un plus petit idéal I de R qui contient P, appelé l'idéal engendré par P : il est formé des éléments qui s'écrivent comme une somme (forcément finie : rien dans la théorie des anneaux ne permet former des sommes infinies) de produits de la forme rp avec $p \in P$ et $r \in R$. Ce sont donc les *combinaisons R-linéaires* d'éléments de P, ce qui montre la ressemblance avec le construction d'un espace vectoriel $\mathrm{Vect}(S)$ engendré par un ensemble S de vecteurs. Cet idéal I peut aussi être décrit comme l'intersection de tous les idéaux qui contiennent P (et parmi lesquels figure bien sûr I lui même...). C'est une description valable qui plaira à certains esprits ; elle est même parfois utile.

On voit que des idéaux peuvent être contenu dans un idéal plus grand. Par exemple dans $\mathbf{Z}$ l'idéal principal $a\mathbf{Z}$ est contenu dans un autre tel idéal $b\mathbf{Z}$ si et seulement si a est un multiple de b (attention au fait que le plus petit idéal $a\mathbf{Z}$ est associé au nombre le plus grand (en valeur absolue). Dans ce cas un morphisme $\mathbf{Z}/a\mathbf{Z} \to \mathbf{Z}/b\mathbf{Z}$ est défini, en réduisant les restes modulo a encore une fois modulo son diviseur b ; la composée $\mathbf{Z} \to \mathbf{Z}/a\mathbf{Z} \to \mathbf{Z}/b\mathbf{Z}$ est égale à l'unique (en canonique) morphisme $\mathbf{Z} \to \mathbf{Z}/b\mathbf{Z}$.

En général le noyau $J = \ker(g \circ f)$ d'un morphisme composé $R \xrightarrow{f} S \xrightarrow{g} T$ d'anneaux contient de façon évidente le noyau $I = \ker(f)$ du premier morphisme appliqué : pour $i \in I$ on a $f(i) = 0_S$ donc $g(f(i)) = g(0_S) = 0_T$ et $i \in J$. Réciproquement si on a une inclusion $I \subseteq J$ d'idéaux, on peut définir un morphisme $R/I \to R/J$ qui envoie chaque classe $a + I$ dans R/I vers la classe $a + J$ qui le contient ; la situation is le même que pour $\mathbf{Z}/a\mathbf{Z} \to \mathbf{Z}/b\mathbf{Z}$ ci-dessus. La règle suivante généralise cette définition.

1.3.3. Proposition. *Soit I un idéal de l'anneau commutatif R, et $\pi : R \to R/I$ la projection canonique. Si $f : R \to S$ est un morphisme d'anneaux tel que $I \subseteq \ker(f)$, alors il existe un morphisme d'anneaux unique $\bar{f} : R/I \to S$ tel que $\bar{f} \circ \pi = f$, c'est-à-dire tel qu'on ait $\bar{f}(a+I) = f(a)$ pour tout $a \in R$.*

Preuve. L'équation $\bar{f}(a+I) = f(a)$ définit déjà toutes les valeurs de l'application $\bar{f}$, donc son unicité est évidente. Mais chaque valeur est définie plusieurs fois, donc if faut vérifier que ces définitions ne se contredisent pas : si $a+I = a'+I$, alors $f(a') = f(a)-f(a-a') = f(a)-0 = f(a)$ car $a-a' \in I \subseteq \ker(f)$. La vérification que c'est un morphisme est facile : $\bar{f}(\pi(a)+\pi(b)) = \bar{f}(\pi(a+b)) = f(a+b) = f(a)+f(b) = \bar{f}(\pi(a))+\bar{f}(\pi(b))$; pour '$\times$' au lieu de '$+$' c'est exactement pareil, et $\bar{f}(1_{R/I}) = \bar{f}(\pi(1_R)) = f(1_R) = 1_S$. □

En fait *tout* morphisme d'anneaux $g : R/I \to S$ peut être ainsi obtenu, car il suffit de poser $f = g \circ \pi$ et appliquer la proposition pour retrouver $\bar{f} = g$, d'après l'unicité. Il s'agit donc de *la* manière de définir un morphisme d'anneau qui part d'un anneau quotient R/I ; il suffit de définir un morphisme f sur R dont il faut s'assurer qu'il s'annule sur I, c'est-à-dire $\ker(f) \supseteq I$. On dit qu'un tel f "passe au quotient modulo I" pour donner le morphisme $\bar{f}$. En appliquant ceci à la situation où $\bar{f}$ est surjectif on obtient

1.3.4. Corollaire. *Les idéaux de R/I sont en bijection avec les idéaux de R contenant I.*

Preuve. Si $\bar{J}$ est un idéal de R/I, l'idéal correspondant de R le noyau J du morphisme composé $R \xrightarrow{\pi} R/I \to (R/I)/\bar{J}$, c'est-à-dire $J = \pi^{-1}(\bar{J}) = \{\, j \in R : \pi(j) \in \bar{J} \,\}$, qui contient évidemment I. Réciproquement pour tout idéal $J \supseteq I$ la projection canonique $R \to R/J$ passe au quotient modulo I, et donne donc un morphisme $R/I \to R/J$ dont le noyau $\bar{J} = \pi(J)$ correspond à J ; ceci établit la bijection. □

Illustrons ce passage au quotient en considérant l'exercice suivant : "Soit V un espace vectoriel réel de dimension n, et $\phi \in \mathrm{End}(V)$ un endomorphisme qui vérifie $\phi^2 = -\mathrm{id}_V$, montrer alors que n est pair." En considérant pourquoi $n = 1$ est impossible, on voit que "*réel*" est essentiel (dans le cas complexe on aurait un contre-exemple avec ϕ la multiplication par $\mathbf{i}$ dans un espace de dimension 1). Plusieurs preuves sont alors possibles (par exemple en utilisant $(\det\phi)^2 = \det\phi^2 = (-1)^n$), mais celle qui suit a l'avantage de révéler la vraie nature de la situation, en montrant que V devient un espace vectoriel *complexe* (et donc de dimension réelle paire) si on décrète que ϕ décrit la multiplication par $\mathbf{i}$.

On considère deux morphismes d'anneaux sur l'anneau $\mathbf{R}[X]$ des polynômes réels, $f : \mathbf{R}[X] \to \mathbf{C}$ la substitution $X := \mathbf{i}$, et $g : \mathbf{R}[X] \to \mathrm{End}(V)$ la substitution $X := \phi$ (pour une constante $c \in \mathbf{R}$ on pose $g(c) = c\,\mathrm{id}_V$). Dans les deux cas le polynôme X^2+1 est dans le noyau, mais aucun polynôme de degré 0 ou 1 ne l'est. Il en découle que $\ker(f) = \ker(g) = (X^2+1)\mathbf{R}[X]$, l'idéal principal engendré par X^2+1. En appelant I cet idéal, on trouve par passage au quotient $\mathbf{R}[X]/I$ des morphismes $\bar{f} : \mathbf{R}[X]/I \to \mathbf{C}$ et $\bar{g} : \mathbf{R}[X]/I \to \mathrm{End}(V)$, qui sont injectifs parce que I est exactement le noyau de f et de g. Comme f est clairement surjectif, $\bar{f}$ l'est aussi, et donc un isomorphisme $\mathbf{R}[X]/I \xrightarrow{\sim} \mathbf{C}$. Alors, en composant l'application inverse de $\bar{f}$ avec $\bar{g}$, on obtient un morphisme d'anneaux $\mathbf{C} \to \mathrm{End}(V)$, qui envoie $1 \mapsto \mathrm{id}_V$ et $\mathbf{i} \mapsto \phi$. On peut vérifier qu'un tel morphisme est précisément ce qui est nécessaire pour définir une multiplication scalaire complexe ; on a donc muni V d'une structure de $\mathbf{C}$-espace vectoriel, comme voulu.

Dans le cas du morphisme f, on vient de voir qu'un morphisme *surjectif* donne lieu, après passage au quotient par son propre noyau $\ker(f)$, à un isomorphisme d'anneaux. Ceci est vrai en général, et en plus on peur rendre tout morphisme d'anneaux surjectif en remplaçant l'anneau S d'arrivée par son sous-anneau $f(R)$ qui est l'image du morphisme f. On obtient alors le théorème suivant.

1.3.5. Théorème d'isomorphisme. *Pour tout morphisme d'anneau $f : R \to S$, on a un isomorphisme canonique $R/\ker(f) \xrightarrow{\sim} f(R)$, et f est la composée des morphismes $R \xrightarrow{\pi} R/I \xrightarrow{\sim} f(R) \to S$.*

Preuve. Le morphisme f passe au quotient modulo son propre noyau $\ker(f)$, donnant $\bar{f} : R/\ker(f) \to S$, et $\ker(\bar{f}) = \pi(\ker f) = \{0_{R/I}\}$. Alors $\bar{f}$ est injectif et son image est celle $f(R)$ de f. Considéré comme application $R/\ker(f) \to f(R)$, ce $\bar{f}$ est donc un isomorphisme, l'isomorphisme canonique du théorème. □

Comme on peut associer à chaque idéal I de R l'anneau quotient R/I, chaque propriété de certains anneaux donne lieu à une propriété correspondante pour les idéaux. Cela s'applique en particulier aux propriétés d'être un corps ou un anneau intègre.

1.3.6. Définition. *Soit I un idéal d'un anneau commutatif R. On appelle I un idéal maximal si R/I est un corps, et on appelle I un idéal premier si R/I est un anneau intègre.*

1.3.7. Proposition. *Soit I un idéal d'un anneau commutatif R.*
(1) I est idéal maximal si c'est un idéal propre qui est maximal (pour l'inclusion d'idéaux) parmi les idéaux propres : un idéal $J \supseteq I$ vérifie soit $J = I$ soit $J = R$.
(2) I est idéal premier c'est un idéal propre tel que $ab \in I$ pour $a, b \in R$ entraîne que l'un au moins de a, b appartient à I.
(3) Si I est idéal maximal, alors I est aussi idéal premier.

Preuve. Le point (3) est une traduction directe du corollaire 1.2.6. Le point (2) en est une de la définition d'un anneau intègre, car une paire de diviseurs de zéro dans R/I serait une paire de classes $x+I, y+I$ tous deux distincts de $0_{R/I}$, donc $x, y \notin I$, tels que leur produit $xy+I$ soit égal à $0_{R/I}$ donc $xy \in I$; dire qu'une telle paire n'existe pas veut dire que $ab \in I$ ne se produit que si $a \in I$ ou $b \in I$. Finalement la condition dans le point (1) exprime, compte tenu du corollaire 1.3.4, que R/I est un anneau commutatif possédant précisément deux idéaux, $\{0_{R/I}\}$ et R/I, et on a vu que c'est une propriété qui caractérise les corps. □

On peut traduire l'argument de le point (1) termes de l'anneau R lui même. Si I est idéal propre et maximal pour cette propriété, et $a \notin I$, alors $I + aR$ est un idéal qui contient strictement I, donc égal à R tout entier. En particulier on peut écrire $1 = i + ab$ avec $i \in I$ et $B \in R$, et la classe $b + I$ est l'inverse de $a + I$ dans R/I car $1_R \in ab + I = 1_{R/I}$ (on dit que b est "un inverse de a *modulo* I", même si $a \notin R^\times$).

On a vu qu'un idéal propre I de R intersecte tout sous-anneau S en un idéal propre de celui-ci. Mais si I est maximal dans R, son intersection $I \cap S$ n'est pas forcément maximal dans S, comme le montre l'exemple $I = \{0\} \subset \mathbf{Q}$, unique idéal maximal du corps $\mathbf{Q}$, mais dont l'intersection avec $\mathbf{Z}$ (qui est toujours $\{0\}$) n'est pas maximal dans $\mathbf{Z}$, car $\mathbf{Z}/\{0\} \cong \mathbf{Z}$ n'est pas un corps. Ceci est une des raisons pour s'intéresser aux idéaux premiers, car contrairement à la maximalité, le fait d'être idéal premier est préservé dans les sous-anneaux.

1.3.8. Proposition. *L'intersection d'un idéal premier avec un sous-anneau S est un idéal premier de S.*

Preuve. Si I est idéal premier de R et S une sous-anneau, alors R/I est un anneau intègre, et l'intersection $I \cap S$ est le noyau du morphisme composé $S \to R \to R/I$. Par le théorème d'isomorphisme 1.3.5, le quotient $S/(I \cap S)$ est isomorphe à un sous-anneau de R/I, à savoir à l'image du morphisme composé, et un tel sous-anneau est toujours intègre. Donc $I \cap S$ est un idéal premier de S. □

En fait il n'est pas difficile d'obtenir ce même résultat en utilisant la description des idéaux premiers de la proposition 1.3.7 directement. Si $ab \in I$ entraîne que $a \in I$ ou $b \in I$, alors $ab \in I \cap S$ avec $a, b \in S$ entraîne aussi que $a \in I \cap S$ ou $b \in I \cap S$; l'idéal propre $I \cap S$ dans S y sera donc un idéal premier. Mais il est utile de s'habituer à des raisonnements plus indirects tels que la preuve donnée ci-dessus, car ils touchent souvent plus clairement à l'essentiel de la situation. Ici la propriété "idéal premier" dans un anneau R est héritée dans un sous-anneau S (contrairement à "idéal maximal"), car c'est le cas de la propriété "anneau intègre" (et ce n'est pas le cas de la propriété "corps").

Finalement on peut définir encore quelques autres opérations sur l'ensemble des idéaux de R. Si I, J sont des idéaux, leur intersection $I \cap J$ sera un idéal aussi. Pour le prouver, il suffit de vérifier les conditions de fermeture de la définition 1.3.1, mais comme chaque idéal est séparément fermé pour les opérations concernées, il est impossible pour ces opérations de sortir de l'intersection. L'argument marche aussi pour l'intersection d'une famille quelconque d'idéaux, même infinie : elle donne toujours un idéal.

Une dernière opération sur les idéaux est celle du produit IJ de deux idéaux : c'est l'idéal *engendré par* l'ensemble des produits $\{ xy : x \in I, y \in J \}$; on a $IJ \subseteq I \cap J$ car chaque générateur xy est dans $I \cap J$. Pour les idéaux $n\mathbf{Z}$ de $\mathbf{Z}$, dont on verra que ce sont tous les idéaux de $\mathbf{Z}$, ces opérations se calculent de façon explicite : pour des entiers $m, n \in \mathbf{N}$ on a $(m\mathbf{Z}) + (n\mathbf{Z}) = \mathrm{pgcd}(m, n)\mathbf{Z}$, ainsi que $(m\mathbf{Z}) \cap (n\mathbf{Z}) = \mathrm{ppcm}(m, n)\mathbf{Z}$ et $(m\mathbf{Z})(n\mathbf{Z}) = mn\mathbf{Z}$.

L'opération du produit de deux idéaux ne jouera pas de rôle dans ce cours, mais elle peut servir pour expliquer partiellement la terminologie "idéal premier". Déjà dans l'exemple de $\mathbf{Z}$ on peut voir que c'est

la seule des opérations qui produit un nouvel idéal à partir d'un seul : on a $I + I = I$, $I \cap I = I$, mais en général $II = I^2$ n'est pas égal à I. Si I et J sont des idéaux propres, et si IJ est distinct de I et de J (ce qui est presque toujours vrai, et toujours dans $\mathbf{Z}$), alors IJ n'est jamais un idéal premier : il suffit de prendre $a \in I \setminus IJ$ et $b \in J \setminus IJ$ pour trouver $ab \in IJ$ qui contredit la condition d'être idéal premier. Dans une certaine classe importante d'anneaux commutatifs, les anneaux de Dedekind, la réciproque est aussi vraie : tout idéal propre qui n'est pas premier est un produit d'idéaux propres. On a dans ces anneaux même un théorème de factorisation unique d'idéaux : tout idéal propre et non nul s'écrit de façon unique (à l'ordre près) comme produit d'idéaux premiers. Ce théorème, qui est valable même dans des anneaux qui ne connaissent pas forcément une factorisation unique d'*éléments* en facteurs irréductibles, explique aussi le terme "idéal" : ce sont des "nombre idéaux" pour lesquels les propriétés de factorisation sont meilleures que pour les vrais nombres (c'est-à-dire les éléments de l'anneau de Dedekind R).

On termine avec quelques remarques concernant les anneaux non-commutatifs, qu'on a laissés de côté jusqu'ici dans cette section. Pour eux, la condition pour un sous-groupe additif de pouvoir être le noyau d'un morphisme d'anneaux est qu'il soit fermé aussi bien pour la multiplication à gauche que pour celle à droite par un élément quelconque ; on parle dans ce cas d'un idéal bilatère. Les résultats concernant les anneaux quotient tels que proposition 1.3.3–théorème 1.3.5 restent valables dans les anneaux non-commutatifs simplement en remplaçant le terme "idéal" par "idéal bilatère".

Mais ce qui change de façon importante est la manière dont les éléments engendrent des idéaux. On peut former à partir d'un $a \in R$ les groupes additifs $aR = \{ ar : r \in R \}$ et $Ra = \{ ra : r \in R \}$, mais ils ne sont chacun fermé que pour la multiplication d'un seul côté ; il sont appelé des idéaux à droite respectivement à gauche, qui sont utile pour certains buts, mais ne permettent pas de former un anneau quotient. Si l'on forme la fermeture de ces ensembles aussi pour la multiplication de l'autre côté on trouve un ensemble plus grand $RaR = \{ rar' : r, r' \in R \}$, mais qui n'est pas en général un sous-groupe additif. Le plus petit idéal bilatère qui contient a est le sous-groupe engendré par RaR. Mais il est bien possible qu'il s'agisse de R tout entier même si a n'est pas inversible. Par conséquent, le fait de n'avoir que deux idéaux bilatères $\{0\}$ et R *ne caractérise pas* les corps parmi les anneaux non-commutatifs ; du coup la notion d'idéal bilatère maximal n'a pas grand intérêt pour ces anneaux. Par exemple l'anneau $\mathrm{End}(E)$ des endomorphismes d'un espace vectoriel de dimension finie > 1, qui n'est pas un corps et contient même beaucoup de diviseurs de zéro, a néanmoins $\{0\}$ et $\mathrm{End}(E)$ comme seuls idéaux bilatères.

1.4. *Anneaux de polynômes (et quelques variations).*

On rappelle les propriétés principales des anneaux $R[X]$ de polynômes un une indéterminée sur un anneau R. En même temps on mentionnera aussi l'anneau des séries formelles $R[[X]]$ dont la définition est similaire (mais qui nous intéressera moins par la suite), et on comparera certaines de leurs propriétés.

1.4.1. Caractérisation. *Soit R un anneau, et X un symbole sans signification préalable par rapport à R. L'anneau $R[X]$ de polynômes en X à coefficients dans R vérifie les propriétés suivantes, et est caractérisé par ces propriétés :*

(1) $R[X]$ contient R comme sous-anneau, en un élément désigné par X,
(2) X commute avec tout $a \in R$ (comme élément de $R[X]$) : $Xa = aX$,
(3) pour chaque $P \in R[X]$, il existe une suite $(c_i)_{i\in\mathbf{N}}$ unique, avec $c_i = 0$ pour tout i suffisamment grand, tel que $P = \sum_{i\in\mathbf{N}} c_i X^i$, somme qui n'a qu'un nombre fini de termes non nuls.

La condition (3) fournit une écriture pour tout élément de $R[X]$ comme combinaison R-linéaire (à gauche) de la famille $(X^i)_{i\in\mathbf{N}}$ des monômes en X ; c'est une famille qui est infinie, mais dont chaque combinaison ne peut effectivement utiliser qu'un nombre fini d'éléments. Comme $X^0 = 1$, il est clair que cette combinaison, qui est unique, est $a = aX^0$ pour un élément $a \in R$, et en particulier cela fixe les éléments $0, 1 \in R[X]$. Les propriétés additives d'un anneau et la loi distributive assurent que l'addition vérifie les règles $(\sum_{i\in\mathbf{N}} c_i X^i)+(\sum_{i\in\mathbf{N}} d_i X^i) = \sum_{i\in\mathbf{N}}(c_i+d_i)X^i$ et $-(\sum_{i\in\mathbf{N}} c_i X^i) = \sum_{i\in\mathbf{N}}(-c_i)X^i$. Pour la multiplication, les lois distributives assurent que $(\sum_{i\in\mathbf{N}} c_i X^i)\times(\sum_{i\in\mathbf{N}} d_i X^i) = \sum_{i\in\mathbf{N}}\sum_{j\in\mathbf{N}} c_i X^i d_j X^j$, où la double somme reste effectivement finie. D'après la condition (2), on a pour chaque terme de cette somme $c_i X^i d_j X^j = c_i d_j X^i X^j = c_i d_j X^{i+j}$. Après cette transformation on obtient pour le produit une

combinaison R-linéaire des monômes, mais avec des monômes répétés dans plusieurs termes ; on peut regrouper les termes avec le même monôme, pour obtenir l'expression $\sum_n p_n X^n$, où le coefficient p_n est donné par $p_n = \sum_{i=0}^{n} c_i d_{n-i}$. Ainsi les conditions déterminent toute la structure d'anneau de $R[X]$.

La preuve de l'*existence* d'un tel anneau $R[X]$ se fait par la construction d'un modèle, dont on montre qu'il définit bien un anneau avec les propriétés mentionnées. Comme l'une de ces propriétés est qu'un élément $P \in R[X]$ est déterminé par la suite $(c_i)_{i\in\mathbf{N}}$ de coefficients dans l'écriture $P = \sum_{i\in\mathbf{N}} c_i X^i$, qui sont nuls au delà d'un certain indice (on dira : ils sont *presque tous nuls*, où "presque tous" veut dire "à un nombre fini d'exceptions près"), on peut prendre pour ce modèle l'ensemble de suites $(c_i)_{i\in\mathbf{N}}$ avec $c_i \in R$ presque tous nuls. On a déjà constaté que les axiomes des anneaux et les propriétés voulues permettent de déduire des formules définissant les opérations arithmétiques en termes de ces suites de coefficients. On pourra démontrer sans difficulté dans le modèle que les coefficients d'une suite formée comme la somme ou le produit de deux autres suites sont presque tous nuls (on a donc bien des lois de composition internes), et que tous les axiomes d'anneaux et propriétés voulues sont vérifiés. Considérons à titre d'exemple l'associativité de la multiplication : il suffit de montrer l'égalité dans les produits $a(bc)$ et $(ab)c$ des coefficients d'un monôme quelconque X^n, quels coefficients sont $\sum_{i=0}^{n}\sum_{j=0}^{n-i} a_i b_j c_{n-i-j}$ et $\sum_{l=0}^{n}\sum_{i=0}^{l} a_i b_{l-i} c_{n-l}$; ces deux sommes sont égales, comme on voit en posant $l = i + j$.

On voit également sans difficulté que l'anneau $R[X]$ sera commutatif si (et seulement si) R l'est. Ceux qui s'intéressent uniquement à ce cas (qui est de loin le plus intéressant) pourraient rajouter la qualification "commutatif" pour R et $R[X]$ dans la caractérisation du dernier, ce qui rend évidemment sa condition (2) superflue. Si on a ici choisi de donner la définition sans hypothèse de commutativité, c'est surtout pour indiquer que cela n'empêche pas la définition de $R[X]$, mais que cette définition fera dans tous les cas commuter X avec tous les autres polynômes (on le déduit facilement de la condition (2)).

Dans la pratique on travaille avec $R[X]$ en utilisant exclusivement sa caractérisation, en oubliant le modèle des suites ; à cet égard la situation est similaire à celle des nombres complexes, qui ne sont jamais identifiés à des couples de nombre réels (ou à quelque autre modèle qui aurait pu être utilisé pour construire $\mathbf{C}$). Ainsi, si Y est un autre symbole indépendant de R, on n'identifie pas l'anneau de polynômes $R[Y]$ avec $R[X]$, bien qu'ils soient construits en utilisant le même modèle : les éléments de $R[Y] \setminus R$ seront toujours désignés en utilisant des expressions utilisant le symbole Y au lieu de X.

L'importance de ces considérations est que, $R[X]$ étant un anneau, il est parfaitement possible de considérer un anneau de polynômes à coefficients dans $R[X]$, et dans ce cas il faudra choisir un autre symbole, comme Y, pour désigner la nouvelle indéterminée (c'est la raison qu'on a exigé dans la caractérisation 1.4.1 que le symbole X soit sans signification par rapport à R). Selon la caractérisation de l'anneau $R[X][Y]$ ainsi formé, tous ses éléments admettent une description unique comme combinaison $R[X]$-linéaire de puissances Y^j de Y, leurs coefficients étant comme éléments de $R[X]$ des combinaisons R-linéaires de puissances X^i de X. Par distributivité ce type d'expression peut être réécrit comme une combinaison R-linéaire de *monômes* X^iY^j (en général un monôme en une collection de symboles est un produit de puissances de ces symboles). Ainsi X et Y obtiennent des statuts égaux, et le résultat est appelé l'anneau $R[X,Y]$ des polynômes en deux indéterminées, X et Y, à coefficients dans R. La construction se généralise évidemment à un nombre quelconque d'indéterminées. Le fait qu'on peut considérer ces anneaux comme étant obtenus en rajoutant une indéterminée à la fois permet d'en établir certaines propriétés en faisant une récurrence sur le nombre d'indéterminées.

Avant d'étudier $R[X]$ en plus de détail, on fera une petite digression pour indiquer deux constructions d'anneau qui sont assez similaires à celle de $R[X]$. Dans $R[X]$, l'élément X est toujours régulier, mais jamais inversible : il suffit d'observer que la multiplication d'un polynôme par X a pour effet un décalage de ses coefficients (le coefficient de X^i devient celui de X^{i+1}, et 0 est rajouté devant comme coefficient de X^0), ce qui est une opération injective, mais qui n'a pas dans son image le polynôme $X^0 = 1$. On peut définir un anneau dans lequel au contraire X est inversible, et où tout élément s'écrit de façon unique comme combinaison R-linéaire des puissances de X d'exposant *positif ou négatif* ; cet anneau est noté $R[X, X^{-1}]$ et appelé l'anneau de *polynômes de Laurent* en X à coefficients dans R. Comme pour $R[X]$ les propriétés cherchées fixent les règles d'addition et de multiplication ; notamment le coefficient de X^n dans un produit $(\sum_{i\in\mathbf{Z}} c_i X^i)\times(\sum_{i\in\mathbf{Z}} d_i X^i)$ sera donné par $\sum_{i\in\mathbf{Z}} c_i d_{n-i}$, une somme qui est formellement

infinie, mais qui n'aura pour chaque n qu'un nombre fini de termes non nuls grâce au fait que c'est ainsi pour l'expression $\sum_{i\in\mathbf{Z}} c_i X^i$. Le modèle formé des suites $(c_i)_{i\in\mathbf{Z}}$ d'éléments de R, indicées par tous les entiers mais dont les coefficients de chacune sont presque tous nuls, montre l'existence d'un tel anneau.

Une variation différente sur la définition de $R[X]$ est basée sur le constat que, si on ne dispose que des puissances positives de X, la formule $p_n = \sum_{i=0}^{n} c_i d_{n-i}$ définissant le coefficient de X^n dans un produit est une vraie somme finie ; par conséquence l'hypothèse que les coefficients c_i ou d_j sont presque tous nuls *n'est pas nécessaire* pour qu'elle ait un sens. On pourra donc utiliser la même formule pour définir un produit de deux suites *quelconques* de coefficients $(c_i)_{i\in\mathbf{N}}$ et $(d_i)_{i\in\mathbf{N}}$ (et pour l'addition il est bien sûr de même). Ainsi on peut, dans la construction du modèle de $R[X]$, omettre la condition "presque tous nuls", et obtenir un anneau (beaucoup) plus grand qui contient $R[X]$; cet anneau s'appelle l'anneau $R[[X]]$ des *séries formelles* en X à coefficients dans R. La vérification des axiomes d'un anneau est identique à celle pour le modèle de $R[X]$, car c'est une vérification d'égalités qui se fait coefficient par coefficient, où les formules sont les mêmes. Il est habituel de désigner, par analogie aux polynômes, l'élément de $R[[X]]$ correspondant à la suite $(c_i)_{i\in\mathbf{N}}$ par $\sum_{i\in\mathbf{N}} c_i X^i$, mais ce n'est qu'une convention de notation : la somme n'étant plus "essentiellement finie" (sauf cas exceptionnel où la série formelle est en fait un polynôme en X), on *ne peut pas lui donner un sens dans le langage des anneaux*. Par conséquent, on n'a pour l'anneau $R[[X]]$ aucune caractérisation comme celui de $R[X]$, utilisant seulement ce langage.

Revenons à l'anneau de polynômes $R[X]$. Un outil fondamental dans l'étude de $R[X]$ est la fonction "degré en X" : $\deg_X : R[X] \to \{-\infty\} \cup \mathbf{N}$, qui est définie par $\deg_X(0) = -\infty$ pour le polynôme nul, et par $\deg_X(\sum_{i\in\mathbf{N}} c_i X^i) = \max\{\, i \in \mathbf{N} : c_i \neq 0 \,\}$ pour tout autre polynôme (l'ensemble dont on prend le maximum étant fini, et non vide dans ce cas). Sur l'ensemble $\{-\infty\} \cup \mathbf{N}$ on ne se servira que de l'opération '+' (où $-\infty + d = -\infty$ pour tout d) et de la relation d'ordre (où $-\infty$ est évidemment le plus petit de tous). On ne prendra donc pas la différence de deux degrés (sauf si le polynôme nul est exclus).

Si $P \in R[X]$ est non nul, on appellera *coefficient dominant* de P le coefficient c_d de X^d dans P, où $d = \deg_X(P)$ (on a $c_d \neq 0$ par définition), et le terme $c_d X^d$ est le *terme dominant* de P (ces notions ne sont pas définies pour le polynôme nul). Un *polynôme unitaire* est un polynôme non nul dont le coefficient dominant est 1.

1.4.2. Proposition. *Si R est un anneau, et $P, Q \in R[X]$, on a*
(1) $\deg_X(P+Q) \leq \max(\deg_X(P), \deg_X(Q))$, *et*
(2) $\deg_X(PQ) \leq \deg_X(P) + \deg_X(Q)$.
Si l'anneau R est intègre, la relation (2) peut être précisée : $\deg_X(PQ) = \deg_X(P) + \deg_X(Q)$.

Preuve. Ces énoncés sont des conséquences directes des définitions. Un coefficient de $P+Q$ ne peut être non nul que si l'un au moins des coefficients correspondants de P et de Q l'est, ce qui donne l'inégalité (1) (mais réciproquement un coefficient de $P+Q$ peut être nul sans que les coefficients correspondants de P, Q le sont, d'où on ne peut pas affirmer une égalité). La formule $c_n = \sum_{i=0}^{n} p_i q_{n-i}$ pour le coefficient de X^n dans un produit de polynômes montre que $c_n = 0$ pour $n > \deg_X(P) + \deg_X(Q)$ (aucun terme $p_i q_{n-i}$ ne peut être non nul), ce qui donne l'inégalité (2). Cette inégalité est certainement une égalité dans les cas où $P = 0$ ou $Q = 0$ (car $-\infty + d = -\infty$). Supposons maintenant le cas contraire, et posons $n = \deg_X(P) + \deg_X(Q)$. Les contributions à c_n autres que $p_{\deg_X(P)} q_{\deg_X(Q)}$ sont nulles pour une même raison que ci-dessus. Mais cette contribution restante est le produit des coefficients dominants de P et de Q, qui sont non nulles, et si R est intègre cela entraîne $c_n \neq 0$ et donc $\deg_X(PQ) = n$. □

L'argument montre qu'un polynôme dont le coefficient dominant est régulier dans R est régulier dans $R[X]$ (la condition est suffisante, mais pas nécessaire). On en déduit en particulier :

1.4.3. Corollaire. *Si R est un anneau intègre, alors $R[X]$ est aussi intègre.*

Cette propriété indique un contraste important entre la construction de $R[X]$ et celles de produits directs d'anneaux et d'anneaux de fonctions à valeurs dans R, qui elles ne conservent pas l'intégrité ; c'est une raison pour laquelle celle des polynômes nous intéressera beaucoup plus. C'est aussi un exemple d'une propriété qui se propage par récurrence aux anneaux de polynômes en plusieurs indéterminées : si R est intègre, alors tout anneau $R[X_1, \ldots, X_n]$ est aussi intègre. Une autre conséquence de la proposition

est une description des éléments inversibles dans un anneau de polynômes, du moins dans le cas où R est intègre : comme $\deg_X(1) = 0$, et on ne peut avoir $\deg_X(P)+\deg_X(Q) = 0$ que si $\deg_X(P) = 0 = \deg_X(Q)$, un élément inversible et son inverse doivent être de degré 0, et donc tous deux dans R. Par conséquent :

1.4.4. Corollaire. *Si R est un anneau intègre, alors $R[X]^\times = R^\times$.*

L'exemple $(1 + 2X)^2 = 1 + 4X + 4X^2 = 1$ dans $(\mathbf{Z}/4\mathbf{Z})[X]$, donc $(1 + 2X) \in (\mathbf{Z}/4\mathbf{Z})[X]^\times$, montre qu'on ne peut pas se passer de l'hypothèse de l'intégrité de R dans ce corollaire.

On remarque que $R[X, X^{-1}]$ et $R[[X]]$ sont également intègres si (et seulement si) R est intègre. Pour $R[X, X^{-1}]$ cela peut être démontré en définissant $\deg_X : R[X, X^{-1}] \to \{-\infty\} \cup \mathbf{Z}$ de la même façon que pour $R[X]$, et pour quelle notion de degré la proposition et sa démonstration restent valables sans modification. Pour $R[[X]]$ on ne saura pas définir le degré (sauf en admettant $+\infty$ comme valeur, ce qui enlèverait toute utilité de la notion). Par contre on peut définir une notion "duale", la *valuation* d'une série formelle, dont la valeur est dans $\mathbf{N} \cup \{+\infty\}$: c'est $+\infty$ pour la série nulle, et $\min\{\, i \in \mathbf{N} : c_i \neq 0 \,\}$ pour toute autre série $\sum_{i\in\mathbf{N}} c_i X^i$ (contrairement au maximum, le minimum existe pour toute partie non vide de $\mathbf{N}$). La valuation possède une propriété analogue à la proposition 1.4.2 mais avec l'ordre opposé, notamment on a $\mathrm{val}(PQ) = \mathrm{val}(P)+\mathrm{val}(Q)$ pour $P, Q \in R[[X]]$ si R est un anneau intègre, ce qui entraîne que $R[[X]]$ est un anneau intègre. On pourrait en fait démontrer le corollaire 1.4.3 pour $R[X]$ en utilisant la valuation (qui est aussi définie pour les polynômes) au lieu du degré. Pour les éléments inversibles il y a des différences avec le cas de $R[X]$. Il est clair que X est inversible dans $R[X, X^{-1}]$, mais c'est à peu près la seule différence avec $R[X]$; on peut montrer que si R est intègre, $R[X, X^{-1}]^\times$ est le produit direct de $R^\times$ et du groupe multiplicatif cyclique $\{\, X^i : i \in \mathbf{Z} \,\}$ engendré par X. Dans $R[[X]]$ au contraire X n'est pas inversible, mais c'est plutôt une exception : on peut montrer que si R est intègre, $R[[X]]^\times$ est formé de tous les éléments dont le coefficient de X^0 (dit son *coefficient constant*) appartient à $R^\times$.

1.5. *Propriétés d'anneaux de polynômes.*

La propriété la plus fondamentale des anneaux de polynômes $R[X]$ est la possibilité de faire correspondre l'élément X à un élément x presque quelconque dans un anneau qui contient R, à la seule condition que x commute avec tout $a \in R$; ainsi X peut jouer le rôle d'un élément inconnu ou "générique" dans les calculs, et ceci est à la fois l'origine historique des polynômes et la motivation de la construction de $R[X]$.

1.5.1. Théorème. *Soit $f : R \to S$ un morphisme d'anneaux, et $s \in S$ un élément qui commute avec le sous-anneau $f(R)$ (c'est-à-dire $sf(r) = f(r)s$ pour tout $r \in R$). Alors f s'étend à un morphisme d'anneaux unique $f_s : R[X] \to S$ tel que $f_s(X) = s$. Ce morphisme envoie $\sum_{i\in\mathbf{N}} c_i X^i \mapsto \sum_{i\in\mathbf{N}} f(c_i)s^i$.*

Ce théorème est formulé de façon la plus générale possible, mais dans la pratique on se sert souvent des cas spéciaux. D'abord si S est un anneau commutatif, et sinon même si le sous-anneau $f(R)$ est *central* dans S (ses éléments commutent avec tout élément de S), alors la condition de commutation sera toujours vérifiée. Le plus souvent R est un sous-anneau d'un anneau commutatif S, voire égal à S, et f le morphisme d'inclusion (l'identité $R \to S$). Dans ce cas le théorème affirme qu'on peut lire systématiquement une valeur fixée s à la place de X (c'est-à-dire *substituer* s pour X), ce qui transforme toutes les opérations d'anneaux sur les polynômes en les mêmes opérations sur les valeurs obtenues (ce qui est l'essence d'un morphisme d'anneaux). Ainsi l'indéterminée X se spécialise de façon arbitraire.

Une situation moins évidente où le théorème s'applique est avec R un corps commutatif, $S = \mathrm{End}(E)$ pour un espace vectoriel sur R, et $f : R \to \mathrm{End}(E)$ l'application qui envoie $\lambda \in R$ vers l'homothétie $\lambda\,\mathrm{id}_E$ de E de facteur λ. Dans ce cas S n'est pas commutatif mais $f(R)$ est central dans S ; le théorème affirme alors que la substitution d'un endomorphisme fixé $\phi \in \mathrm{End}(E)$ dans les polynômes de $R[X]$ définit un morphisme d'anneaux $R[X] \to \mathrm{End}(E)$ (dont les valeurs s'appellent polynômes de l'endomorphisme ϕ).

Preuve. L'énoncé donne déjà la formule pour f_s, qui par l'unicité de l'expression $\sum_{i\in\mathbf{N}} c_i X^i$ pour un polynôme est bien définie ; il s'agit juste de vérifier qu'elle définit un morphisme d'anneaux. Pour des

polynômes $P = \sum_{i\in\mathbf{N}} p_i X^i$ et $Q = \sum_{j\in\mathbf{N}} q_j X^j$, on a

$$\begin{aligned} f_s(P) \times f_s(Q) &= \sum_{i,j\in\mathbf{N}} f(p_i)s^i f(q_j)s^j = \sum_{i,j\in\mathbf{N}} f(p_i)f(q_j)s^i s^j \qquad \text{par la commutation de } f(R) \text{ avec } s, \\ &= \sum_{i,j\in\mathbf{N}} f(p_i q_j)s^{i+j} = f_s(\sum_{i,j\in\mathbf{N}} p_i q_j X^{i+j}) = f_s(PQ). \end{aligned}$$

On laisse la vérification (plus simple) pour l'addition comme exercice, et $f_s(1) = f(1)s^0 = 1$ est clair. □

Une application simple de ce théorème dit qu'un morphisme d'anneaux $f : R \to S$ s'étend à un morphisme d'anneaux de polynômes $R[X] \to S[X]$ qui envoie $X \in R[X]$ vers $X \in S[X]$, autrement dit où f opère seulement sur les coefficients des polynômes. En particulier on pourra toujours considérer des polynômes dans $R[X]$ comme des polynômes à coefficients dans un *sur-anneau* S de R (c'est-à-dire qui contient R comme sous-anneau), et on peut également "quotienter par un idéal" I de R pour passer de $R[X]$ à $(R/I)[X]$. En général le morphisme f_s du théorème se compose d'un tel passage au quotient par $\ker(f)$ suivi d'une substitution pour X de l'élément s du sur-anneau S de l'anneau des coefficients.

La notation f_s dans le théorème n'est pas très commode dans le cas fréquent où f est l'identité ou une inclusion d'anneaux (à laquelle on ne donne en général pas de nom explicite). Comme dans ce cas $f_s(P)$ est la valeur obtenue en substituant s pour X dans le polynôme P, on utilisera dans ce cours la notation $P[X := s]$ (le symbole ':=', qui est emprunté à l'informatique, se prononce "devient").

L'auteur de ce cours motive son refus de la notation un peu plus courte $P(s)$, pourtant utilisée presque partout dans la littérature, ainsi.

- Cette notation est basée sur, et renforce, la confusion entre un polynôme et une fonction polynomiale.
- Elle est mal lisible, voire ambiguë, quand le polynôme P et/ou la valeur s sont donnés non par des lettres mais par des expressions ; par exemple si $P = 3X^2+3$ et $s = y-5$, une application stricte de la notation $P(s)$ donne $(3X^2+7)(y-5) = 3(y-5)^2+7$, ce qui est moins heureux que $(3X^2+7)[X := y-5] = 3(y-5)^2+7$.
- La confusion possible mène certains a ne jamais écrire un produit $Q(X-a)$, mais toujours $(X-a)Q$.
- L'omission du nom de l'indéterminée pour laquelle on substitue pose des difficultés quand il y en a plusieurs. On peut étendre la notation à $P \in R[X,Y]$ en écrivant $P(s,t)$ pour $P[X := s][Y := t]$, mais pour le polynôme correspondant $P' \in R[X][Y]$ on aurait $P(s,t) = P'(t)(s)$ (ce qui est tellement perfide que personne ne l'écrit) et il est même impossible de seulement substituer s pour X dans P' (mais en utilisant P on pourra écrire $P(s,Y)$ pour l'obtenir); comparer cela avec $P[X := s]$.
- Pour certains, l'utilisation de la notation $P(s)$ remet même en cause le droit d'écrire simplement P quand aucune substitution n'est voulue, et ils introduiraient par exemple $P(X) \in R[X]$ et $S(X,Y) \in R[X,Y]$ au lieu de $P \in R[X]$ et $S \in R[X,Y]$. Certes, cela permet d'éviter la confusion signalée ci-dessus, en écrivant $P(X) = Q(X)(X-a) = (X-a)Q(X)$ au lieu de $P = Q(X-a) = (X-a)Q$. On peut encore distinguer deux écoles : les orthodoxes, pour qui un polynôme en X *ne peut pas* être désigné sans écrire '(X)', et qui ne donnent aucune signification à P tout seul, et les modérés qui se permettent parfois d'écrire P, et qui maintiennent que l'égalité $P(X) = P$ est naturelle, car la substitution de X pour X dans P redonne P. On pourrait y rajouter l'égalité $X(P) = P$, qui est vraie pour les des raisons similaires, mais moins populaire.

On peut caractériser l'image $f_s(R[X])$ du morphisme de substitution comme le plus petit sous-anneau de S qui contient $f(R) \cup \{s\}$. Pour le voir, remarquons qu'un sous-anneau de $R[X]$ qui contient $R \cup \{X\}$ contiendra aussi tout les monômes X^n et est donc égal à $R[X]$ tout entier, et que si $S' \subseteq S$ est un sous-anneau de S contenant $f(R)$ et s, alors $f_s^{-1}(S')$ est un tel sous-anneau de $R[X]$, d'où $f_s^{-1}(S') = R[X]$ et $f_s(R[X]) \subseteq S'$. Cela mène à la notation suivante dans le cas que R est sous-anneau de S.

1.5.2. Définition. *Soit R un sous-anneau de S, et $s \in S$ un élément qui commute avec R. Alors $R[s]$ désigne le sous-anneau $\{ P[X := s] : P \in R[X] \}$ de S, le plus petit sous-anneau de S contenant R et s.*

Cette définition confirme les notations comme $\mathbf{Q}[\mathbf{i}]$ et $\mathbf{Z}[\sqrt{n}]$ utilisées précédemment. Continuons avec des applications directes du théorème 1.5.1. On en déduit facilement que $R[X]$ possède un très grand degré de symétrie, tout au moins quand R est commutatif.

1.5.3. Corollaire. *Soit R un anneau commutatif et $a \in R$. L'application $R[X] \to R[X]$ donnée par $P \mapsto P[X := X + a]$ est un automorphisme de $R[X]$, dont la réciproque est $P \mapsto P[X := X - a]$.*

Le théorème 1.5.1, appliqué avec $S = R[X]$, affirme que $P \mapsto P[X := X + a]$ définit un morphisme d'anneaux $R[X] \to R[X]$, et d'après l'unicité dans le théorème, la seul chose qui reste à vérifier est que

les morphismes composés $P \mapsto P[X := X + a][X := X - a]$ et $P \mapsto P[X := X - a][X := X + a]$ envoient $X \mapsto X$, ce qui est évident. On remarque que l'hypothèse de commutativité de R (ou au moins que a soit central dans R) est nécessaire pour qu'un morphisme de substitution qui envoie $X \mapsto X - a$ puisse exister : X commute dans $R[X]$ avec tous les éléments de R, donc son image par un morphisme doit obligatoirement avoir la même propriété (par rapport aux images des éléments de R). Une remarque similaire (et même plus directe) s'applique à la substitution $X := a$, que nous considérons par la suite.

La situation la plus simple d'application du théorème 1.5.1 est avec S un sur-anneau commutatif de R. Le fait qu'on a alors des morphismes de substitution pour tout $s \in S$ permet de combiner tous ces morphismes en un morphisme d'anneaux vers l'anneau (hautement non-intègre) S^S des fonctions $S \to S$.

1.5.4. Proposition/Définition. *Soit R un sous-anneau d'un anneau commutatif S. L'application $F_S : R[X] \to S^S$ qui associe à $P \in R[X]$ la fonction $s \mapsto P[X := s]$ est un morphisme d'anneaux. Cette fonction $F_S(P) : S \to S$ associée à P est appelée fonction polynomiale de P (dans S), et l'image $F_S(R[X]) \subseteq S^S$ du morphisme forme l'anneau des fonctions polynomiales $S \to S$ à coefficients dans R.*

Preuve. Pour qu'une application $f : R \to S^I$ d'un anneau R vers un anneau de fonctions S^I soit un morphisme d'anneaux, il faut et il suffit que pour tout $i \in I$ l'application $R \to S$ donnée par $a \mapsto f(a)(i)$ soit un morphisme. L'affirmation dans l'énoncé est donc une conséquence directe du théorème 1.5.1. □

Revenons au simple morphisme $R \to S$ donné par $P \mapsto P[X := s]$. Dans le cas $S = R$ il est clair que ce morphisme ne peut jamais être injectif (car tout élément de S est déjà dans l'image du sous-anneau R de $R[X]$), et plus généralement il sera assez souvent non injectif (si R est un corps par exemple, il faudrait que S soit de dimension infinie en tant que R-espace vectoriel pour pouvoir obtenir l'injectivité.) La question de déterminer le noyau d'un morphisme de substitution se pose donc naturellement. Cela donne une relation entre un élément $s \in S$ (qui détermine une substitution) et un polynôme $P \in R[X]$ du noyau de la substitution, qu'on exprimera en disant que s est racine de P. C'est équivalent à dire que s est un élément de S où s'annule la fonction polynomiale $S \to S$ de P (c'est-à-dire $F(P)$ de 1.5.4).

1.5.5. Définition. *Soit R un sous-anneau d'un anneau commutatif S. Un élément $s \in S$ est racine d'un polynôme $P \in R[X]$ si $P[X := s] = 0$.*

Un élément $a \in R$ est toujours racine du polynôme $X - a$, et donc (parce que le noyau de la substitution est un idéal de $R[X]$) de tout polynôme dans l'idéal principal engendré par $X - a$. En fait, cet idéal est précisément l'ensemble des polynômes ayant a comme racine.

1.5.6. Proposition. *Soit R un anneau commutatif et $a \in R$. Le noyau du morphisme $R[X] \to R$ de substitution de a pour X est égal à l'idéal principal $(X - a)R[X]$ engendré par $X - a$. Autrement dit, a est une racine d'un polynôme $P \in R[X]$ si et seulement si $X - a$ divise P.*

Preuve. On peut considérer cette proposition comme conséquence de la division euclidienne par un polynôme unitaire (à savoir $X - a$), dont on parlera plus tard. Mais on peut l'obtenir aussi par le raisonnement plus élémentaire suivant. Le résultat est évident pour $a = 0$, car la substitution $X := 0$ envoie un polynôme $\sum_i c_i X^i$ vers son coefficient constant c_0, pendant que l'image $XR[X]$ de la multiplication par X contient tous les polynômes dont le coefficient constant est nul. Pour le cas général, on écrit la substitution $X := a$ comme la composée de l'isomorphisme $\phi : R[X] \to R[X]$ de substitution $X := X + a$, suivi du morphisme $p : R[X] \to R$ de substitution $X := 0$. Or $\ker(p \circ \phi)$ est l'image réciproque par ϕ de $\ker(p) = XR[X]$, qui est clairement l'idéal principal $\phi^{-1}(X)R[X] = (X - a)R[X]$. □

1.5.7. Proposition. *Soit R un anneau commutatif intègre. Si $P \in R[X]$ possède une racine $a \in R$, alors P s'écrit de façon unique $P = (X - a)Q$ dans $R[X]$, et l'ensemble des racines de P dans R est la réunion de $\{a\}$ et l'ensemble des racines de Q.*

Preuve. Les hypothèses impliquent $P \in (X - a)R[X]$ d'après la proposition précédente, ce qui établit l'existence de Q. L'unicité de Q est une conséquence du fait que $R[X]$ est intègre (corollaire 1.4.3) et $X - a \neq 0$. Un élément $b \in R$ est racine de P si et seulement si $0 = P[X := b] = ((X - a)Q)[X := b] = (X - a)[X := b] \times Q[X := b] = (b - a)Q[X := b]$ dans R. Comme R est intègre, cette condition est vérifiée seulement si l'un des deux facteurs est nul, c'est-à-dire si $b = a$ ou si b est racine de Q. □

1.5.8. Corollaire. *Si R est un anneau commutatif intègre, aucun polynôme non nul $P \in R[X]$ ne peut posséder plus que $\deg_X(P)$ racines dans R, ou dans un sur-anneau commutatif intègre S de R.*

Preuve. L'ensemble de racines de P dans S ne change pas si l'on considère P comme élément de $S[X]$ via l'inclusion $R[X] \subseteq S[X]$; on peut donc supposer $R = S$. Comme $\deg_X(P) \in \mathbf{N}$, on peut appliquer un argument de récurrence sur $\deg_X(P)$. Si $\deg_X(P) = 0$, alors P est un élément non nul de $R \subseteq R[X]$ (c'est-à-dire, un *polynôme constant* non nul), et donc $P[X := a] = P \neq 0$ pour tout $a \in R$; par conséquent P n'a aucune racine. Supposons maintenant $\deg_X(P) > 0$. Si P ne possède aucune racine le corollaire est vérifié. Sinon, soit $a \in R$ une racine de P ; on applique la proposition précédente, où on a $\deg_X(Q) = \deg_X(P) - 1$ d'après la proposition 1.4.2, donc Q ne possède pas plus que $\deg_X(P) - 1$ racines dans R, et la réunion dans la proposition ne contient pas plus que $\deg_X(P)$ éléments. □

On remarque que les hypothèses du commutativité et d'intégrité sont essentielles dans ce corollaire et la proposition précédente. La notion de racine exige déjà la commutativité de S, mais on pourrait la définir si R est central dans un anneau non-commutatif S (de sorte que $P[X := s]$ ait un sens) ; dans ce cas l'exemple du polynôme réel X^2+1 qui possède dans le corps non-commutatif $\mathbf{H}$ (où $\mathbf{R}$ est central) des "racines" $\mathbf{i}$, $-\mathbf{i}$, $\mathbf{j}$, $-\mathbf{j}$, $\mathbf{k}$, $-\mathbf{k}$ (en une infinité d'autres) montre le défaut de ces énoncés. Et si on exige la commutativité, mais pas l'intégrité, on trouve pour le "même" polynôme $X^2+1 \in (\mathbf{Z}/65\mathbf{Z})[X]$ les 4 racines $8, 18, 47, 57 \in \mathbf{Z}/65\mathbf{Z}$ (ou plus simple, $X^2 - 1 \in (\mathbf{Z}/8\mathbf{Z})[X]$ possède les 4 racines $1, 3, 5, 7 \in \mathbf{Z}/8\mathbf{Z}$). On verra même que pour n'importe quel polynôme $P \in R[X]$ avec $\deg_X(P) \geq 2$ on peut construire des sur-anneaux non intègres de R où P possède autant de racines qu'on veut. Si on regarde de près ce qui "cloche" dans ces exemples, c'est la proposition 1.5.7. Dans $\mathbf{H}[X]$, on a $(X+\mathbf{i})(X-\mathbf{i}) = X^2+1 = (X+\mathbf{j})(X-\mathbf{j})$, mais aucun des deux facteurs $X+\mathbf{j}$, $X-\mathbf{j}$ de la dernière expression n'est divisible (à gauche ou à droite) par $X+\mathbf{i}$ (et si on essaye de "substituer" $X := \mathbf{i}$ dans l'égalité $X^2+1 = (X+\mathbf{j})(X-\mathbf{j})$, elle devient fausse). Dans $(\mathbf{Z}/8\mathbf{Z})[X]$ le phénomène est similaire (on a $(X-1)(X-7) = X^2-1 = (X-3)(X-5)$ sans que $X-1$ ne divise ni $X-3$ ni $X-5$), mais l'explication est un peu différente: l'égalité $X^2 - 1 = (X-3)(X-5)$ permet bien de substituer $X := 1$ donnant $0 = 2 \times 4 \in \mathbf{Z}/8\mathbf{Z}$, mais sans produire des facteurs nuls.

1.5.9. Corollaire. *Soit R un sous-anneau d'un anneau commutatif intègre S. Le morphisme $R[X] \to S^S$ associant à $P \in R[X]$ sa fonction polynomiale $S \to S$ est injectif si et seulement si S est infini.*

Preuve. Comme $P \neq 0$ ne peut avoir plus de $\deg_X(P)$ racines dans S d'après le corollaire 1.5.8, sa fonction polynomiale ne peut pas être nulle (c'est-à-dire s'annuler en chaque $s \in S$) si S est infini. Réciproquement, comme $R[X]$ est toujours infini (les monômes X^i sont tous distincts car R n'est pas l'anneau trivial), si S est fini, alors le morphisme $R[X] \to S^S$ est forcément non injectif. □

1.5.10. Théorème. *Soit R un anneau commutatif intègre, et $G \subseteq R^\times$ un sous-groupe multiplicatif fini. Alors G est cyclique, c'est-à-dire il existe (au moins un) $a \in G$ tel que $G = \{ a^i : 0 \leq i < n \}$ où $n = \#G$.*

Preuve. La preuve de ce résultat classique est une étonnante mélange d'éléments des théories d'anneaux et des groupes. La partie théorie d'anneaux se limite à l'énoncé du corollaire 1.5.8, et les hypothèses sur R servent uniquement à cela. La partie théorie des groupes est une considération élémentaire sur la notion d'ordre d'un élément, qu'on rappelle rapidement. L'ordre d'un élément d'un groupe fini H divise toujours $\#H$, en particulier G ne contient que des éléments d'ordre d divisant n. Si a est d'ordre d, le sous-groupe qu'il engendre $\langle a \rangle = \{ a^i : 0 \leq i < d \}$ est isomorphe au groupe additif $\mathbf{Z}/d\mathbf{Z} = C_d$. Soit $\phi(d)$ le nombre d'éléments x d'ordre d dans ce groupe C_d ; pour chaque tel x on a $\#\langle x \rangle = d$ donc forcément $\langle x \rangle = C_d$. Si dans un groupe H on a deux éléments x, y du même ordre d mais avec $\langle x \rangle \neq \langle y \rangle$, alors les ensembles d'éléments d'ordre d de ces sous-groupes cycliques sont *disjoints*, car un élément commun engendrerait à la fois $\langle x \rangle$ et $\langle y \rangle$ ce qui n'est pas possible. Par conséquent si H contient k sous-groupes cycliques différents d'ordre d, il contiendra $k\phi(d)$ éléments d'ordre d. Le groupe additif $\mathbf{Z}/n\mathbf{Z}$ contient un sous-groupe cyclique d'ordre d pour tout diviseur d de n (à savoir les multiples de n/d), d'où

$$n = \sum_{d|n} \phi(d). \tag{3}$$

Mais G contient *au plus un* sous-groupe cyclique d'ordre d pour tout diviseur d, car tous les d éléments d'un tel sous-groupe sont racines du polynôme $X^d - 1$, et le corollaire 1.5.8 interdit d'en avoir davantage. En comptant les éléments de G selon leur ordre multiplicatif, on voit que n est la somme des $\phi(d)$ où d parcourt les diviseurs de n pour lesquels G contient effectivement un sous-groupe cyclique d'ordre d, mais d'après la formule (3) cela n'est possible que si la somme porte sur tous les $d|n$. Il existe donc en particulier un sous-groupe cyclique de G d'ordre n, qui bien évidemment ne peut pas être autre que G. □

Dans un anneau commutatif intègre les éléments de $R^\times$ qui sont d'ordre fini (est c'est toujours le cas pour les éléments d'un sous-groupe fini) sont appelés *racines de l'unité*, car ils sont racine d'un polynôme de la forme $X^n = 1$. Quand R est une sous-anneau de $\mathbf{C}$, le théorème 1.5.10 peut être obtenu de façon plus directe, en observant que dans $\mathbf{C}$ les racines de l'unité sont tous sur le cercle unité, et en considérant pour un sous-groupe fini G de $\mathbf{C}^\times$ l'élément avec le plus petit argument strictement positif, qui est toujours générateur de G.

Pour cette raison le théorème est surtout intéressant en caractéristique p, où une telle construction n'existe pas. Pour un entier $n > 0$, on appelle *racine primitive modulo* n tout entier a tel que la classe de a modulo n soit générateur du groupe multiplicatif $(\mathbf{Z}/n\mathbf{Z})^\times$. Bien sur une telle racine primitive n'existe que si $(\mathbf{Z}/n\mathbf{Z})^\times$ est cyclique, mais théorème 1.5.10 affirme que c'est toujours le cas si n est un nombre premier (ce ne sont pas les seuls cas où $(\mathbf{Z}/n\mathbf{Z})^\times$ est cyclique ; une classification complète existe, mais ne sera pas abordée ici). Aucune formule n'est connue qui produit une racine primitive modulo p, mais elles sont en général assez facile à trouver, car le nombre $\phi(p-1)$ de classes de telle racines est suffisamment grand par rapport à $\#(\mathbf{Z}/p\mathbf{Z})^\times = p-1$ pour en trouver rapidement en essayant au hasard $a = 2, 3, 5, 6, \ldots$ (ceci n'est plus vrai quand p est tellement grand que la factorisation de $p-1$, nécessaire pour *tester* si un nombre est racine primitive modulo p, devient pratiquement infaisable). On pourrait croire qu'une connaissance abstraite de la structure cyclique de $(\mathbf{Z}/p\mathbf{Z})^\times$ ne peut être utile sans la connaissance concrète d'un générateur, mais le corollaire suivant montre le contraire.

1.5.11. Corollaire. *Si $p \neq 2$ est un nombre premier, alors la congruence $x^2 \equiv -1 \pmod{p}$ possède des solutions $x \in \mathbf{Z}$ si et seulement si $p \equiv 1 \pmod{4}$.*

Preuve. L'anneau $\mathbf{Z}/p\mathbf{Z}$ est une corps commutatif, et dans un anneau intègre R de caractéristique $\neq 2$ un élément a est d'ordre 4 dans $R^\times$ si et seulement s'il est racine de $X^2 + 1$ (car a est racine de $X^4 - 1 = (X^2+1)(X+1)(X-1)$ mais $a \notin \{-1, 1\}$). Or $(\mathbf{Z}/p\mathbf{Z})^\times$ est un groupe cyclique d'ordre $p-1$ d'après le théorème 1.5.10, et il possède donc dès éléments d'ordre 4 si et seulement si 4 divise $p-1$. □

La recherche effective des solutions x à la congruence $x^2 \equiv -1 \pmod{p}$ peut se faire en calculant différentes images de l'application $a \mapsto a^{\frac{p-1}{4}}$ dans $a \in (\mathbf{Z}/p\mathbf{Z})^\times$; comme c'est un morphisme de groupes dont l'image est le sous-groupe $\{ x : x^4 = 1 \}$ qui est cyclique d'ordre 4, on a chaque fois une chance sur deux de tomber sur une valeur distinct de 1 et -1, qui sera alors une solution.

Finalement on rappelle la division euclidienne des polynômes, qui aura d'importantes conséquences dans la suite. La formulation classique de la division euclidienne, et la plus concrète, est la suivante.

1.5.12. Proposition. *Soit $A, B \in R[X]$ avec $B \neq 0$ ayant un coefficient dominant inversible dans R. Alors il existe $Q, r \in R[X]$ tels que $A = BQ + r$ et $\deg_X(r) < \deg_X(B)$, et le couple (Q, r) est unique.*

La preuve de cette proposition, qui peut être faite par récurrence sur $\deg_X(A)$ en commençant avec les cas trivial $\deg_X(A) < \deg_X(B)$, devient encore plus simple si on en la reformule en termes d'idéaux. D'abord un peu de notation : l'idéal principal $PR[X]$ d'un anneau commutatif de polynômes engendré par un polynôme P est habituellement noté par (P), surtout dans des contextes qui demandent un idéal, comme dans $R[X]/(P)$. Un petit détail : la proposition 1.5.12 n'exige pas la commutativité de R, et ce n'est pas nécessaire (on cherche un quotient Q à droite ; celui à gauche peut être différent). La proposition suivante reste vraie pour R non commutatif en lisant "idéal à droite" pour "idéal" (sous-groupe additif fermé pour multiplication à droite), et pour (U) l'idéal à droite $UR[X]$ des multiples à droite de U.

1.5.13. Proposition. *Si $I \subseteq R[X]$ est un idéal qui contient un polynôme unitaire U qui est de degré minimal parmi les éléments de $I \setminus \{0\}$, alors I est l'idéal principal (U) de $R[X]$, et la restriction de la projection canonique $R[X] \to R[X]/I$ à $R[X]_{<\deg(U)} = \{ Q \in R[X] : \deg_X(Q) < \deg_X(U) \}$ est bijective.*

Cette proposition implique la précédente, car si B a un coefficient dominant $c \in R^\times$, alors l'idéal principal $I = (B)$ engendré par B contient le polynôme unitaire $U = Bc^{-1}$ et aucun polynôme non nul de degré inférieure à $\deg_X(B)$, et l'existence de $Q \in R[X]$ avec $A = BQ + r$ équivaut à $r \equiv A \pmod{I}$, donc l'existence et l'unicité de r résulte de la bijectivité dans la proposition 1.5.13. L'unicité de Q en découle car B est régulier dans $R[X]$ (car son coefficient dominant est inversible et donc régulier dans R).

Preuve. Soit $\phi : R[X]_{<\deg(U)} \to R[X]/I$ la restriction mentionnée, qui est un morphisme de groupes additifs. Alors l'injectivité de ϕ est conséquence de la relation $R[X]_{<\deg(U)} \cap I = \{0\}$ qui est donnée, son surjectivité du fait qu'un représentant P de degré minimal d'une classe dans R/I ne peut être ailleurs que dans $R[X]_{<\deg(U)}$: si P avait terme dominant cX^d avec $d \geq \deg_X(U)$, on trouverait dans la même classe modulo I le polynôme $P - UcX^{d-\deg_X(U)}$ qui est de degré strictement plus bas. On a clairement $(U) \subseteq I$, et pour l'inclusion inverse il suffit de remarquer que l'argument ci-dessus montre que pour tout $x \in I$, le représentant r de degré minimal de la classe $x + (U)$ est dans $R[X]_{<\deg(U)} \cap I$, et donc $r = 0$. □

La formulation des deux propositions cache l'aspect algorithmique du calcul du reste r dans la proposition 1.5.12 (qui est aussi le représentant de degré minimal dans la proposition 1.5.13), mais il est assez clair dans la démonstration : on remplace de façon itérative le représentant P d'une classe modulo (U), avec terme dominant cX^d, par un représentant $P - UcX^{d-\deg_X(U)}$ de degré plus bas, jusqu'à ce que $\deg_X(P) < \deg_X(U)$. Le processus ressemble beaucoup à la division longue des entiers.

1.5.14. Corollaire. *Si K est un corps commutatif, tout idéal de $K[X]$ est principal.*

Preuve. Comme $\{0\}$ est principal, il suffit de montrer que tout idéal $I \neq \{0\}$ vérifie l'hypothèse de la proposition 1.5.13. Mais il suffit de choisir $B \in I \setminus \{0\}$ et $U = Bc^{-1}$ avec c le coefficient dominant de B. □

Cette propriété, dite "principalité", rend la structure de $K[X]$ particulièrement simple, et ses propriétés arithmétiques très proches de celles de $\mathbf{Z}$. Remarquons que cette propriété distingue ces $K[X]$ des anneaux $R[X]$ avec R un anneau commutatif intègre qui n'est pas un corps, car ces derniers possèdent toujours des idéaux non principaux : si $a \in R$ est non inversible, l'idéal I de $R[X]$ engendré par a et X n'est pas principal : aucun polynôme de degré > 0 engendre un idéal contenant a, et tout polynôme dans $I \cap R = aR$ engendre un idéal contenu dans le noyau de la projection $R[X] \to (R/aR)[X]$, qui ne contient donc pas X. La principalité faut donc défaut notamment aux anneaux comme $\mathbf{Z}[X]$ et $K[X, Y]$.

§2. Arithmétique dans les anneaux commutatifs intègres.

Dans ce chapitre nous allons étudier les questions d'arithmétique, c'est-à-dire concernant la relation de la relation de divisibilité, notée $a \mid b$: a divise b, c'est-à-dire il existe $q \in R$ tel que $aq = b$. On se restreindra au cas des anneaux commutatifs intègres, car dans ces anneaux la relation $a \mid b$ avec $a \neq 0$ implique l'existence d'un *unique* quotient q, qui sera noté $q = b/a$ (la notation ba^{-1} pour le quotient est proscrite, sauf dans le cas peu intéressant où $a \in R^\times$). On commence avec le cas archétypique de l'anneau $\mathbf{Z}$.

2.1. *Arithmétique dans* $\mathbf{Z}$*, algorithme d'Euclide, congruences, théorème chinois.*

Les questions d'arithmétique dans les anneaux commutatifs intègres sont en grande partie inspirées par la situation dans $\mathbf{Z}$. Ceci dit, l'anneau $\mathbf{Z}$ possède beaucoup de propriétés, qui ne sont pas toujours partagées par les anneaux où ces questions se posent. Il est donc utile de revoir le développement de la théorie dans $\mathbf{Z}$, et d'essayer isoler des propriétés clés dont dépendent certains résultats, pour pourvoir déterminer dans quelles classes d'anneaux ces résultats restent valables. On verra que les anneaux qui possèdent une division euclidienne, comme $K[X]$ avec K un corps commutatif, ou encore $\mathbf{Z}[\mathbf{i}]$, sont les plus proches de $\mathbf{Z}$, en termes de propriétés partagés. D'autres anneaux partagent des parties moins importantes des propriétés de $\mathbf{Z}$. Disons d'emblée que la propriété de *factorialité*, l'existence d'une factorisation *unique* en nombres premiers, qu'on pourrait croire élémentaire, est en fait pas du tout une évidence, et qu'elle fait défaut à certains anneaux qui en premier aperçu semblent très proche de $\mathbf{Z}$, comme $\mathbf{Z}[\sqrt{5}]$ ou $\mathbf{Z}[\sqrt{5}\,\mathbf{i}]$.

2.1.1. Propriété. *Les seuls idéaux de* $\mathbf{Z}$ *sont les idéaux principaux ; ce sont les idéaux* $n\mathbf{Z}$ *pour* $n \geq 0$.

En fait, ce sont déjà les seuls sous groupes additifs de $\mathbf{Z}$. Mais c'est sous cette formulation de principalité que la propriété est partagée par certains autres anneaux, comme $K[X]$. Dans $\mathbf{Z}$ elle est liée à son caractère ordonné, car on voit facilement que dans un sous-groupe additif H de $\mathbf{Z}$ la distance entre un élément de H et le suivant doit toujours être constante, d'où le plus petit élément > 0 de H engendre H tout entier. Mais sous cette forme l'argument se généralise mal ; par contre, on peut le formuler ainsi : si $d \in H \setminus \{0\}$ est de valeur absolue minimal, et si $h \in H$ était un élément non contenu dans l'idéal principal $d\mathbf{Z}$ engendré par d, alors on pourrait réduire h modulo $d\mathbf{Z}$ pour trouver un élément de $H \setminus \{0\}$ de valeur absolue plus petit que $|d|$, donnant une contradiction. Ainsi la propriété essentielle est la suivante.

2.1.2. Propriété. *Pour tout* $n \in \mathbf{Z} \setminus \{0\}$*, toute classe de* $\mathbf{Z}/n\mathbf{Z}$ *possède (au moins) un représentant strictement plus petit en valeur absolue que* n.

Si on cherche à adapter cette propriété à d'autres anneaux, on pourrait remplacer "valeur absolue" par tout autre attribut des éléments pour lequel il est impossible de descendre indéfiniment (c'est-à-dire tel qu'il n'existe pas des suite infinie pour laquelle l'attribut décroît strictement) ; on l'a vu pour $K[X]$, où le degré prend la place de la valeur absolue. La propriété qu'on obtiendra ainsi caractérisera les "anneaux euclidiens", car l'opération de réduction modulo les multiples de n pour trouver un représentant (reste) qui soit strictement plus petit que n (en valeur absolue) est connue comme la division euclidienne.

Pour trouver la factorialité de $\mathbf{Z}$ il faut d'abord définir les nombres premiers : ce sont les nombres $p > 1$ ne permettant pas d'écriture $p = xy$ avec $x, y \in \mathbf{Z} \setminus \mathbf{Z}^\times$ (on rappelle que $\mathbf{Z}^\times = \{-1, 1\}$). Puis il faut montrer que tout nombre $n > 1$ s'écrit comme un produit (fini) de nombres premiers, pas forcément distincts ; cela se fait facilement par récurrence sur n, car soit n est premier et un "produit à un facteur" convient, soit $n = xy$ avec $1 < x, y < n$ et l'hypothèse de récurrence fournit des écritures de x et de y comme produits de nombres premiers, qui se combinent pour donner une telle écriture pour n. Finalement il faut montrer que cette écriture est unique, à permutation de ses facteurs près. Le point crucial est :

2.1.3. Lemme d'Euclide. *Si un nombre premier* p *divise un produit* ab*, alors* p *divise au moins un des facteurs* a, b*. Par conséquent si* $p \mid a_1 \cdots a_k$*, alors* $p \mid a_i$ *pour au moins un des facteurs* a_i *du produit.*

On voit facilement que c'est une propriété nécessaire pour l'unicité des factorisations : si p divisait $n = ab$ sans diviser ni a ni b, on en déduirait immédiatement de $p(n/p) = n = ab$ deux factorisations de n (en factorisant n/p, a, et b) dont la première contient un facteur p, mais la seconde n'en contient aucun.

Pour voir que le lemme d'Euclide est aussi suffisant pour l'unicité des factorisations, on considère deux factorisations différentes $p_1 \cdots p_k = n = q_1 \cdots q_l$ de $n > 1$ en nombres premiers. Alors le premier facteur p_1 à gauche doit diviser au moins un des facteurs q_j à droite, et en fait y être égal, car la définition interdit à un nombre premier d'être divisible par un *autre* nombre premier. Du coup on peut simplifier l'équation par $p_1 = q_j$ et déduire par récurrence que la suite $q_1, \ldots, q_l$ est une permutation de $p_1, \ldots, p_k$ (et donc en particulier l'égalité $k = l$ des nombres de facteurs dans les factorisations).

Il reste à démontrer le lemme d'Euclide. On peut le faire de différentes manières, mais la théorie d'anneaux suggère une preuve particulièrement simple qui n'utilise que la principalité de $\mathbf{Z}$. Le lemme d'Euclide dit précisément que pour un nombre premier p, l'idéal $p\mathbf{Z}$ des multiples de p est un idéal premier. Mais la définition d'un nombre premier implique que $p\mathbf{Z}$ est maximal parmi les idéaux *principaux* propres (si $d\mathbf{Z}$ était un idéal propre contenant strictement $p\mathbf{Z}$, alors d serait un diviseur de p avec d et p/d non inversibles). Alors la propriété 2.1.1 assure que $p\mathbf{Z}$ est en effet un idéal maximal, et donc un idéal premier (voir les remarques qui suivent la définition 1.3.6).

La factorialité permet de comprendre de façon particulièrement simple la structure de $\mathbf{Z}$ par rapport à la relation de divisibilité. Si pour a et b on donne leurs factorisations respectives en nombre premiers, alors pour voir si $a \mid b$, on peut commencer à simplifier par des facteurs premiers qui sont présents dans les deux factorisations ; il restera une relation $p_1 \cdots p_k \mid q_1 \cdots q_l$ où $p_i \neq q_j$ pour tout i, j. Or une telle relation de divisibilité n'est valable que si $k = 0$ (c'est-à-dire avec un produit vide à gauche, dont la valeur est 1), car sinon p_1 ne divise aucun des q_j. On conclut que pour $a, b \neq 0$, on a la relation $a \mid b$ si et seulement si tout nombre premier apparaît au moins aussi souvent dans la factorisation de b que dans la factorisation de a. Désignons pour $a \in \mathbf{Z} \setminus \{0\}$ et tout nombre premier p par $v_p(a)$ l'ordre de multiplicité de p comme facteur de a, c'est-à-dire $\max\{\, i \in \mathbf{N} : p^i \mid a \,\}$, nombre qui est bien défini, et qui n'est non nul que pour un nombre fini de valeurs de p (à savoir les facteurs premiers de a). Alors on a

$$a = \prod_{p \in \mathrm{Pr}} p^{v_p(a)}, \qquad \text{et} \qquad a \mid b \iff \forall p \in \mathrm{Pr} : v_p(a) \leq v_p(b) \qquad \text{pour } a, b \in \mathbf{Z}_{>0}. \tag{4a, b}$$

Le produit parcourt l'ensemble infini Pr des nombres premiers, mais il est néanmoins bien défini car ses facteurs sont presque tous 1. L'égalité (4a) montre que $\mathbf{Z}_{>0}$ est en bijection avec l'ensemble $\mathbf{N}^{(\mathrm{Pr})}$ des suites $(v_p)_{p \in \mathrm{Pr}}$ d'entiers naturels indicées par les nombres premiers et presque tous nuls, via l'application $a \mapsto (v_p(a))_{p \in \mathrm{Pr}}$, dont la réciproque est $(v_p)_{p \in \mathrm{Pr}} \mapsto \prod_{p \in \mathrm{Pr}} p^{v_p}$. Si l'on munit $\mathbf{N}^{(\mathrm{Pr})}$ de son ordre partiel "par composante", c'est-à-dire $(v_p)_{p \in \mathrm{Pr}} \leq (w_p)_{p \in \mathrm{Pr}}$ si et seulement si $v_p \leq w_p$ pour tout $p \in \mathrm{Pr}$, alors (4b) affirme que c'est un isomorphisme d'ensembles partiellement ordonnés $(\mathbf{Z}_{>0}, \mid) \to (\mathbf{N}^{(\mathrm{Pr})}, \leq)$.

Comme $(\mathbf{N}^{(\mathrm{Pr})}, \leq)$ possède des bornes inférieures et supérieures qu'on peut déterminer composante par composante, on peut conclure à l'aide de cet isomorphisme que pour $a, b \in \mathbf{Z}_{>0}$ il existe aussi des bornes inférieures et supérieures pour la divisibilité, c'est-à-dire un diviseur commun de a, b divisible par tout autre diviseur commun, en un multiple commun de a, b divisant tout autre multiple commun. Comme $x \mid y$ implique $x \leq y$ dans $\mathbf{Z}_{>0}$, la borne inférieure est en particulier le plus grand des diviseurs communs et s'appelle $\mathrm{pgcd}(a, b)$, et la borne supérieure est le plus petit des multiples communs, et s'appelle $\mathrm{ppcm}(a, b)$ (on n'explique pas la permutation des dernières lettres dans ces abréviations). On obtient :

$$\mathrm{pgcd}(a, b) = \prod_{p \in \mathrm{Pr}} p^{\min(v_p(a), v_p(b))}, \qquad \text{et} \qquad \mathrm{ppcm}(a, b) = \prod_{p \in \mathrm{Pr}} p^{\max(v_p(a), v_p(b))}. \tag{5a, b}$$

Ces formules aident à comprendre les propriétés des opérations pgcd et ppcm, mais ne donnent pas une manière très efficace de les calculer, car il faut un effort considérable pour trouver les $p \in \mathrm{Pr}$ qui donnent une contribution (autre que 1) dans ces produits, autrement dit pour factoriser a et b. Et pour expliquer l'existence de $\mathrm{pgcd}(a, b)$ et $\mathrm{ppcm}(a, b)$, on n'a pas besoin de la factorialité de $\mathbf{Z}$: elle découle directement de la principalité. En effet, $\mathrm{ppcm}(a, b)$ doit par définition être un élément qui engendre (comme idéal principal) l'intersection $a\mathbf{Z} \cap b\mathbf{Z}$, et $\mathrm{pgcd}(a, b)$ un élément qui engendre un idéal principal qui est maximal pour la condition de contenir $a\mathbf{Z}$ et $b\mathbf{Z}$, et donc $a\mathbf{Z} + b\mathbf{Z}$. Mais la principalité dit que $a\mathbf{Z} \cap b\mathbf{Z}$ et $a\mathbf{Z} + b\mathbf{Z}$ sont eux-mêmes principaux, et il suffit donc d'en prendre un générateur (positif).

Cet argument cache toujours l'aspect effectif de la procédure, qui s'avère être plus direct pour $\operatorname{pgcd}(a,b)$, car on peut modifier l'expression pour l'idéal $a\mathbf{Z}+b\mathbf{Z}$, la simplifiant jusqu'au point où un générateur devient évident (la description de l'idéal $a\mathbf{Z}\cap b\mathbf{Z}$ ne permet pas un tel procédé). Ce point sera atteint si l'idéal s'écrit comme $d\mathbf{Z}+0\mathbf{Z}$ (dont d est un générateur) ; tant que ce n'est pas le cas, la division euclidienne permet d'obtenir a partir du couple (a,b) un élément de $a\mathbf{Z}+b\mathbf{Z}$ qui est strictement plus petit en valeur absolue que b, à savoir le reste de la division de a par b. Ce n'est pas encore un générateur, mais l'idée est de continuer à trouver des éléments de plus en plus petit en valeur absolue. Ce qui rend cette approche particulièrement simple est qu'on n'a pas besoin de retenir plus que 2 éléments de l'idéal à la fois : si le reste r est égal à $a-bq$, alors non seulement $r\in a\mathbf{Z}+b\mathbf{Z}$ qui est donc égal à $a\mathbf{Z}+b\mathbf{Z}+r\mathbf{Z}$, mais on a aussi $a=bq+r\in b\mathbf{Z}+r\mathbf{Z}$ qui permet d'omettre $a\mathbf{Z}$ de l'expression, donnant $a\mathbf{Z}+b\mathbf{Z}=b\mathbf{Z}+r\mathbf{Z}$. Après ce changement, on peut continuer avec le couple (b,r) à la place de (a,b) : si $r\neq 0$, on peut rajouter le reste r' de la division de b par r, et omettre b : on aura toujours $a\mathbf{Z}+b\mathbf{Z}=r\mathbf{Z}+r'\mathbf{Z}$. Chaque itération fait décroître la valeur absolue du reste, donc fatalement on doit obtenir un reste 0 à un certain point. La simplification $a\mathbf{Z}+b\mathbf{Z}=d\mathbf{Z}+0\mathbf{Z}=d\mathbf{Z}$ s'appliquera alors, montrant que $\operatorname{pgcd}(a,b)=|d|$. Cette méthode de calcul est appelé l'*algorithme d'Euclide*. Quant à $\operatorname{ppcm}(a,b)$, il peut alors être obtenu comme $\operatorname{ppcm}(a,b)=ab/\operatorname{pgcd}(a,b)$, formule qui peut être déduit de (5) (car $\max(x,y)=x+y-\min(x,y)$), mais aussi par un simple raisonnement ne nécessitant pas la factorialité, comme on verra ci-dessous.

Dans la pratique on veut souvent plus d'information que la simple valeur $\operatorname{pgcd}(a,b)$: on veut aussi expliciter le fait $\operatorname{pgcd}(a,b)\in a\mathbf{Z}+b\mathbf{Z}$ en donnant $s,t\in\mathbf{Z}$ tels que $\operatorname{pgcd}(a,b)=as+bt$, égalité qui s'appelle *relation de Bezout*, et s,t des *coefficients de Bezout* pour a,b. Ces derniers ne sont pas uniques : supposons pour $a>0$ et $b\neq 0$ une telle paire (s_0,t_0) connue, alors on trouve toutes les paires (s,t) de coefficients de Bezout comme solutions de $as+bt=as_0+bt_0$, ce qui donne l'équation $a(s-s_0)=b(t_0-t)$ dont la solution avec la plus petite valeur $s>s_0$ est donnée par $s-s_0=\operatorname{ppcm}(a,b)/a$ et $t_0-t=\operatorname{ppcm}(a,b)/b$. On conclut que les solutions possibles pour le coefficient s forment la classe de s_0 modulo $\operatorname{ppcm}(a,b)/a=b/\operatorname{pgcd}(a,b)$, et celles pour t la classe de t_0 modulo $\operatorname{ppcm}(a,b)/b=a/\operatorname{pgcd}(a,b)$ (mais une fois l'un des coefficients est fixé, l'autre est bien évidemment aussi déterminé). Pour trouver une paire (s_0,t_0) de coefficients de Bezout, on peut simplement maintenir pour chaque élément x de l'idéal $a\mathbf{Z}+b\mathbf{Z}$ qu'on construit une paire de coefficients $s_x,t_x\in\mathbf{Z}$ telle que $x=as_x+bt_x$: au départ on prend $(s_a,t_a)=(1,0)$ et $(s_b,t_b)=(0,1)$, et chaque fois qu'un nouveau reste r est obtenu après division euclidienne de x par y, disons $r=x-qy$, on effectue la combinaison linéaire correspondante sur les paires : $s_r=s_x-qs_y$ et $t_r=t_x-qt_y$.

En faisant quelques exemples, on se rendra compte que si $a,b>0$, les signes de ces coefficients intermédiaires sont prévisibles, et que leurs valeurs absolues sont donc toujours croissantes. On peut aussi remarquer que s_x et t_x se déterminent mutuellement, d'où il suffit d'en calculer un. On peut ainsi déduire un algorithme que calcule $\operatorname{pgcd}(a,b)$ et ses coefficients de Bezout sans avoir besoin de nombres négatifs, et dont on montrera qu'il trouve les plus petits (en valeur absolue) coefficients de Bezout possibles. Pour les intéressés nous donnons tous les détails.

2.1.4. Algorithme. *(Extension de l'algorithme euclidien dans* $\mathbf{N}$*.) Paramètres:* $a,b\in\mathbf{N}$*. But : calculer* $d=\operatorname{pgcd}(a,b)$ *et le coefficient de Bezout* $t\in\mathbf{Z}$*, tel que* $d=sa+tb$ *avec* $s\in\mathbf{Z}$*. Variables* $r_0,r_1,t_0,t_1\in\mathbf{N}$*.*

0. Initialiser $r_0:=a$*,* $r_1:=b$*,* $t_0:=0$*,* $t_1:=1$*.*
1. Si $r_0=0$ *terminer en rendant* $(d,t)=(r_1,+t_1)$*.*
2. Trouver $q,r\in\mathbf{N}$ *avec* $r<r_0$ *tels que* $r_1=qr_0+r$ *par division euclidienne ; avec ces valeurs remplacer* $r_1:=r$ *et* $t_1:=t_1+qt_0$*.*
3. Si $r_1=0$ *terminer en rendant* $(d,t)=(r_0,-t_0)$*.*
4. Trouver $q,r\in\mathbf{N}$ *avec* $r<r_1$ *tels que* $r_0=qr_1+r$ *par division euclidienne ; avec ces valeurs remplacer* $r_0:=r$ *et* $t_0:=t_0+qt_1$*, puis continuer à l'étape 1.*

2.1.5. Proposition. *Pour tout* $a,b\in\mathbf{N}$*, l'algorithme 2.1.4 se termine, rendant* $(d,t)\in\mathbf{N}\times\mathbf{Z}$ *tels que* $d\mathbf{Z}=a\mathbf{Z}+b\mathbf{Z}$*, et* $d\in a\mathbf{Z}+bt$*. En plus, si* $a,b>0$ *et* $a\neq b$*, alors* $|t|\leq\frac{a}{2d}$*, ainsi que* $|s|\leq\frac{b}{2d}$ *pour l'autre coefficient de Bezout* $s=(d-bt)/a$ *tel que* $d=as+tb$*. Ces inégalités sont strictes dès lors que leur second membre est* >1*. Par conséquent* s *et* t *sont chacun le plus petit en valeur absolue (et strictement si l'inégalité correspondante est stricte) des coefficients de Bezout qui peuvent figurer à leur place.*

Remarquons d'abord que les cas exclus dans la seconde phrase sont inévitables : si a ou b est 0, l'inégalité pour le coefficient de Bezout de l'autre le forcerait d'être 0 ce qui est impossible (mais les valeur rendues $(s,t)=(0,1)$ respectivement $(s,t)=(1,0)$ sont bien les plus petites possibles) ; si $a=b$ on a des solutions $(s,t)=(1,0),(0,1)$ dont ni l'une ni l'autre peut prétendre d'être les plus petit pour les deux coefficients à la fois (et les deux inégalités énoncées sont incompatibles). D'après le fait observé ci-dessus que s est déterminé modulo b/d et t modulo a/d,

chaque inégalité fait bien du coefficient concerné le plus petit en valeur absolue (et strictement si elle est stricte) de toute sa classe de congruence.

Preuve. La démonstration repose sur le constat d'un nombre de propriétés invariantes de l'algorithme. On a déjà indiqué que les valeurs des variables restent dans $\mathbf{N}$; puis on a l'invariant $a\mathbf{Z} + b\mathbf{Z} = r_0\mathbf{Z} + r_1\mathbf{Z}$ sur lequel l'algorithme d'Euclide est basé ; finalement on a $r_0t_1 + r_1t_0 = a$, ainsi que les congruences $r_0 \equiv -bt_0$ et $r_1 \equiv bt_1$ modulo a, dont l'invariance est éclairée par le fait que les étapes 2 et 4 font une $\mathbf{Z}$-opération de colonnes sur la matrice

$$\begin{pmatrix} r_0 & r_1 \\ -t_0 & t_1 \end{pmatrix},$$

c'est-à-dire elles rajoutent un multiple entier d'une colonne à l'autre colonne (le déterminant de la matrice, qui est a, ne change pas). Ayant constaté ces invariances, on voit que $a\mathbf{Z} + b\mathbf{Z} = d\mathbf{Z}$ et $d \equiv bt \pmod a$ dans les deux cas de terminaison, quelle congruence est équivalente à $d \in a\mathbf{Z}+bt$. Pour les affirmations restantes supposons leurs hypothèses sur a, b vérifiées. Considérant la situation à la terminaison, soit $i \in \{0, 1\}$ tel que $d = r_i = \operatorname{pgcd}(a, b)$, autrement dit la terminaison est déclenché par $r_{1-i} = 0$, et $t = (-1)^{1-i}t_i$. Alors l'invariant $r_0t_1 + r_1t_0 = a$ donne $a/d = t_{1-i}$ (simplifier l'équation par $d = r_i$). Remarquons que pour toute division euclidienne dans l'algorithme sauf la toute première, le diviseur (le nombre par lequel on divise) est garanti d'être strictement plus petit que la dividende, car celui-là était auparavant obtenu comme reste après division par celle-ci. Par conséquence (et grâce aux hypothèses sur a, b) la dernière division, qui est exacte, produit un quotient $q \geq 2$. Cette division a donné, comme dernière affectation à t_{1-i}, le remplacement $t_{1-i} := t_{1-i} + qt_i$, et on a donc $2|t| \leq 2t_i \leq t_{1-i} = a/d$. Cette inégalité sera stricte sauf si la dernière division produit un quotient $q = 2$ *et* on avait $t_{1-i} = 0$ avant la dernière affectation, ce qui se produit seulement avec $i = 1$, et seulement si l'algorithme se termine au *second* passage à l'étape 1. Dans ce cas $a = 2r_1 = 2d$, donc $\frac{a}{2d} = 1$ (et en effet $t = t_1 = 1 = \frac{a}{2d}$).

Pour prouver l'inégalité restante $|s| \leq \frac{b}{2d}$, on pourrait déduire de $-\frac{a}{2d} < t \leq \frac{a}{2d}$ (qu'on a en fait démontré) que $-\frac{b}{2d} + \frac{d}{a} \leq (d - bt)/a = s < \frac{b}{2d} + \frac{d}{a}$, et argumenter qu'on peut se débarrasser du terme $\frac{d}{a} \leq 1$ à droite, quitte à rendre la seconde inégalité faible (seul le cas $d = a$ pose souci, mais on aura alors $t = 0$ et $s = 1$). Une approche peut-être plus transparente est d'employer l'argument de symétrie suivant. On pourrait tracer les valeurs de s correspondants aux t_i en rajoutant des variables $s_0, s_1 \in \mathbf{N}$ à l'algorithme, initialisées comme $s_0 := 1$, $s_1 := 0$ et modifiées par $s_1 := s_1 + qs_0$ respectivement $s_0 := s_0 + qs_1$ dans les étapes 2 et 4 ; dans ce cas on aurait les invariants additionnels $r_0 = as_0 - bt_0$ et $r_1 = -as_1 + bt_1$, et donc $s = (-1)^i s_i$ à la fin. Alors l'évolution des s_i pour (a, b) suit fidèlement celle des t_i pour (b, a), dans la mesure où, en alignant les deux calculs à leurs premières divisions produisant un quotient $q \neq 0$ (car un et un seul des deux commence avec un quotient nul, qui ne change donc pas les variables), les affectations aux variables sont identiques sous les correspondances $s_0 \leftrightarrow t_1$ et $s_1 \leftrightarrow t_0$. Par conséquent, si la calcul de $d = \operatorname{pgcd}(a, b)$ rend le coefficient de Bezout t, et $s = (d - bt)/a$, alors celui de $d = \operatorname{pgcd}(b, a)$ rend s comme coefficient de Bezout. Tout ce qu'on a montré pour t est donc valable *mutatis mutandis* pour s. □

Le calcul d'un coefficient de Bezout (le plus souvent on n'a pas besoin des deux à la fois) est utile pour résoudre des congruences linéaires, c'est-à-dire des relations $ax \equiv b \pmod n$ avec $a, b, n \in \mathbf{Z}$ donnés. En particulier, pour $b = 1$ c'est le problème de trouver un inverse de (la classe de) a dans $\mathbf{Z}/n\mathbf{Z}$. Un tel inverse ne peut exister si a et n ont un diviseur commun $d > 1$, car on a alors un morphisme d'anneaux $\mathbf{Z}/n\mathbf{Z} \to \mathbf{Z}/d\mathbf{Z}$ (la projection canonique $\mathbf{Z} \to \mathbf{Z}/d\mathbf{Z}$ passe au quotient $\mathbf{Z}/n\mathbf{Z}$, d'après la proposition 1.3.3) qui envoie la classe de a modulo n sur l'élément $0 \in \mathbf{Z}/d\mathbf{Z}$, et cette classe n'est donc pas inversible. Mais réciproquement, en l'absence d'un tel diviseur commun, c'est-à-dire quand $\operatorname{pgcd}(a, n) = 1$, la classe de a possède bien un inverse, car en écrivant une relation de Bezout $1 = as + nt$ et en réduisant modulo n, on voit que la classe de s est l'inverse de celle de a dans $\mathbf{Z}/n\mathbf{Z}$. Cela nous mène a la

2.1.6. Définition/Proposition. *Deux entiers $a, b \in \mathbf{Z}$ sont dits premiers entre eux si leurs seuls diviseurs communs sont les éléments inversibles $1, -1 \in \mathbf{Z}^\times$. Cette propriété est équivalente aux suivantes :*
(1) $\operatorname{pgcd}(a, b) = 1$,
(2) aucun nombre premier est diviseur commun de a et de b,
(3) $a\mathbf{Z} + b\mathbf{Z} = \mathbf{Z}$,
(4) l'image de b dans $\mathbf{Z}/a\mathbf{Z}$ est inversible,
(5) l'image de a dans $\mathbf{Z}/b\mathbf{Z}$ est inversible.
Si l'algorithme 2.1.4 retourne un couple $(1, t)$, alors la classe de t est l'inverse de celle de b dans $\mathbf{Z}/a\mathbf{Z}$. □

Considérons ensuite la congruence linéaire générale $ax \equiv b \pmod n$. Si $d = \operatorname{pgcd}(n, a)$ ne divise pas b, la réduction modulo d donne la relation impossible $0x = b \pmod d$, qui exclut toute solution la congruence initiale. Dans le cas contraire, tous les coefficients sont divisibles par d, et on pourra simplifier

la congruence par d pour obtenir la congruence équivalente $(a/d)x = b/d \pmod{n/d}$ (on laisse au lecteur le soin de vérifier l'équivalence de deux, et d'analyser la possibilité $d = 0$). Or $\operatorname{pgcd}(n/d, a/d) = 1$, car si k est diviseur commun de n/d et a/d, alors kd est diviseur commun de n et a ; on a donc réduit le problème (en posant $n' = n/d$, $a' = a/d$, $b' = b/a$) au cas où n et a sont premiers entre eux. Mais dans ce cas a est inversible modulo n, et en multipliant la congruence $ax \equiv b \pmod{n}$ par $a^{-1} \in (\mathbf{Z}/n\mathbf{Z})^\times$, on obtient la congruence, encore équivalente, $x \equiv ba^{-1} \pmod{n}$ qui se résout trivialement. En fait, si (d, t) sont calculés par l'algorithme 2.1.4 appliqué aux valeurs initiales (n, a), alors t représentante la classe de l'inverse de a' modulo n', car $d = ns + at$ implique $1 = n's + a't$ sans modification des coefficients s, t. En résumé, pour résoudre $ax \equiv b \pmod{n}$, on applique l'algorithme 2.1.4 à (n, a) pour trouver (d, t) ; une solution existe alors seulement si $d \mid b$ auquel cas la solution complète est $x \in (b/d)t + (n/d)\mathbf{Z}$.

Les relations de Bezout permettent aussi de résoudre des systèmes de congruences linéaires. Grâce à la réduction décrite ci-dessus, on peut supposer que les congruences individuelles sont réduites à leur plus simple forme $x \equiv b_i \pmod{n_i}$. Un système de telles congruences peut très bien être contradictoire (par exemple si $n_1 = n_2$), mais cette possibilité sera exclue quand les n_i sont premiers entre eux 2 à 2.

Ce problème est lié à la structure de l'anneau produit $(\mathbf{Z}/n_1\mathbf{Z}) \times \cdots \times (\mathbf{Z}/n_k\mathbf{Z})$, car chaque congruence fixe l'une des coordonnées b_i dans le produit cartésien, et on demande de trouver les $x \in \mathbf{Z}$ dont l'image est l'élément donné par ces coordonnées. Dire que le système est résoluble quels que soient $b_1, \ldots, b_k$ veut donc dire qui l'image de $\mathbf{Z}$ remplit tout le produit cartésien, comme c'est le cas dans le tableau suivant, pour $n_1 = 5$ et $n_2 = 13$; chaque case est remplie par le plus petit entier positif dont c'est l'image.

	0	1	2	3	4	5	6	7	8	9	10	11	12
0	0	40	15	55	30	5	45	20	60	35	10	50	25
1	26	1	41	16	56	31	6	46	21	61	26	11	51
2	52	27	2	42	17	57	32	7	47	22	62	27	12
3	13	54	28	3	43	18	58	33	8	48	23	63	28
4	39	14	55	29	4	44	19	59	34	9	49	24	64

Pour voir si une solution existe toujours, et pour trouver concrètement des solutions, la cas fondamental à comprendre est celui d'un système de deux congruences. Dans ce cas, le résultat est facile à obtenir.

2.1.7. Proposition. *Soit $n, m \in \mathbf{Z}$ premiers entre eux. Alors les conditions suivantes sont vérifiées :*
(1) l'unique morphisme $\mathbf{Z} \to (\mathbf{Z}/n\mathbf{Z}) \times (\mathbf{Z}/m\mathbf{Z})$ est surjectif,
(2) l'anneau $(\mathbf{Z}/n\mathbf{Z}) \times (\mathbf{Z}/m\mathbf{Z})$ est canoniquement isomorphe à $\mathbf{Z}/nm\mathbf{Z}$,
(3) pour toute paire de congruences $x \equiv a \pmod{n}$, $x \equiv b \pmod{m}$, il existe $c \in \mathbf{Z}$ tel qu'elle soit équivalente à la seule congruence $x \equiv c \pmod{nm}$.

Preuve. Le noyau du morphisme du point (1) est l'idéal des multiples commun de n et m, qui est engendré par $\operatorname{ppcm}(n, m) = nm/\operatorname{pgcd}(n, m) = nm$, car $\operatorname{pgcd}(n, m) = 1$ d'après l'hypothèse. Par conséquent le sous-anneau image du morphisme possède nm éléments, et est donc égal à $(\mathbf{Z}/n\mathbf{Z}) \times (\mathbf{Z}/m\mathbf{Z})$ tout entier. Cela établit les deux premiers points, et le dernier point est équivalent au second, car la paire de congruences spécifie un élément de $(\mathbf{Z}/n\mathbf{Z}) \times (\mathbf{Z}/m\mathbf{Z})$, pendant qu'une congruence $x \equiv c \pmod{nm}$ spécifie un élément de $\mathbf{Z}/nm\mathbf{Z}$. La surjectivité, et la détermination de c en fonction de a, b peuvent être rendues explicite à l'aide d'une relation de Bezout $1 = ns + mt$, car $(1, 0) \in (\mathbf{Z}/n\mathbf{Z}) \times (\mathbf{Z}/m\mathbf{Z})$ est alors l'image de mt, et $(0, 1) \in (\mathbf{Z}/n\mathbf{Z}) \times (\mathbf{Z}/m\mathbf{Z})$ celle de ns, et on pourra donc prendre $c = mta + nsb$. □

Dans la pratique on peut simplifier le calcul de c en utilisant $ns = 1 - mt$, ce qui donne le formule $c = b + mt(a - b)$. Par exemple, le nombre $c = 33$ dans le tableau ci-dessus sera trouvé pour $(a, b) = (3, 7)$ comme $7 + 26 \times (3 - 7) = 7 - 104 \equiv 33 \pmod{65}$ au lieu de $26 \times 3 + 40 \times 7 = 358 \equiv 33 \pmod{65}$.

[Compléments personnels de l'auteur, qui un jour a dû programmer la résolution de plus de 13 milliard systèmes de 4 congruences, tous pour les mêmes moduli $(n_1, \ldots, n_4) = (251, 253, 255, 256)$.] Dans le cas où n et m sont fixés avant, et c doit être calculé pour beaucoup de paires (a, b), on peut calculer mt une fois pour toutes, et la résolution de chaque système demandera alors une soustraction, une multiplication, une addition, et une réduction modulo nm (car dans la pratique il est important de rendre c le plus petit possible dans sa classe). Dans le cas où $\max(n, m)$ est très grand (et on verra que pour résoudre plusieurs congruences simultanées cela arrive facilement), et si on veut limiter la taille des nombres intermédiaires dans le calcul (par exemple parce que

l'ordinateur utilisé impose une borne), le produit $mt \times (a-b)$ peut poser problème, car mt est une valeur imposée modulo nm, et $|a-b|$ peut atteindre $\max(n,m)-1$, ce qui donne un produit beaucoup plus grand en valeur absolue que nm, pendant qu'on s'intéresse seulement à sa classe modulo nm. Il est alors utile de tabuler auparavant les n premiers multiples de mt modulo mn (c'est la première colonne dans le tableau ci-dessus), qu'on peut calculer avec seulement des additions et des soustractions. Le calcul à répéter pour chaque paire de congruences est alors le suivant : trouver le reste r de $a-b$ modulo n, chercher la valeur de $mt \times r$ dans la table de multiples, et le rajouter à b donnant c. Le calcul du reste est utile quand n est beaucoup plus petit que m, pour limiter la taille de la table de multiples de mt à stocker ; une alternative serait d'étendre la table, qui est périodique de période n.

Pour assurer l'existence d'une solution dans le cas de systèmes de plusieurs congruences, on pourra itérer ce qui précède, pourvu que chaque nouveau modulo n_j soit premier avec le produit $n_1 \cdots n_{j-1}$ des moduli précédents. Pour cela il faut et il suffit que $\operatorname{pgcd}(n_i, n_j) = 1$ pour $i < j$. On a en effet :

2.1.8. Théorème des restes chinois. *Soit $n_1, \ldots, n_k$ des entiers deux à deux premiers entre eux.*
(1) l'unique morphisme $\mathbf{Z} \to (\mathbf{Z}/n_1\mathbf{Z}) \times \cdots \times (\mathbf{Z}/n_k\mathbf{Z})$ est surjectif,
(2) l'anneau $(\mathbf{Z}/n_1\mathbf{Z}) \times \cdots \times (\mathbf{Z}/n_k\mathbf{Z})$ est canoniquement isomorphe à $\mathbf{Z}/(n_1 \cdots n_k)\mathbf{Z}$,
(3) pour tout système de congruences $x \equiv b_i \pmod{n_i}$ pour $i = 1, \ldots, k$, il existe $c \in \mathbf{Z}$ tel qu'il soit équivalent à la seule congruence $x \equiv c \pmod{n_1 \cdots n_k}$.

Preuve. Comme pour la proposition 2.1.7, les trois parties sont clairement équivalentes, il suffira de montrer (par exemple) le (2). C'est une récurrence immédiate basée sur le (2) de ladite proposition : par récurrence on a un isomorphisme $(\mathbf{Z}/n_1\mathbf{Z}) \times \cdots \times (\mathbf{Z}/n_{k-1}\mathbf{Z}) \to \mathbf{Z}/m\mathbf{Z}$ avec $m = n_1 \cdots n_{k-1}$, et la proposition donne un isomorphisme $(\mathbf{Z}/m\mathbf{Z}) \times (\mathbf{Z}/n_k\mathbf{Z}) \to \mathbf{Z}/mn_k\mathbf{Z}$, pourvu que $\operatorname{pgcd}(m, n_k) = 1$. Mais les diviseurs premiers de n_k ne divisent aucun des n_i avec $i < k$, donc ils ne divisent pas non plus le produit $m = n_1 \cdots n_{k-1}$ d'après le lemme d'Euclide 2.1.3, d'où m et n_k sont premiers entre eux. □

On remarque que la condition, assez forte, que les moduli soient premier entre eux *deux à deux* est aussi nécessaire : si n_i et n_j avaient un diviseur commun $d > 1$, alors leurs congruences impliqueraient toutes deux une congruence modulo d, et les deux peuvent être contradictoires. On fera attention à ne pas confondre cette condition avec celle, beaucoup plus faible, de ne pas avoir des diviseurs $d > 1$ communs à *tous* les n_i à la fois, qui s'écrit $\operatorname{pgcd}(n_1, n_2, \ldots, n_k) = 1$ ou de façon équivalente $n_1\mathbf{Z} + \cdots + n_k\mathbf{Z} = \mathbf{Z}$. On appelle cela parfois "être premiers entre eux dans leur ensemble", mais attention que cela devient moins contraignant plus l'ensemble est grand (contrairement à par exemple la notion d'indépendance linéaire). Ici $\operatorname{pgcd}(n_1, \ldots, n_k) = 1$ ne servirait pas à grande chose : le lecteur vérifiera qu'une "relation de Bezout" $n_1 s_1 + \cdots + n_k s_k = 1$ n'est d'aucune utilité pour résoudre des systèmes de congruences quand $k > 2$.

Pour le calcul effectif du nombre c à partir de $b_1, \ldots, b_k$, on pourra combiner chaque fois une paire de congruences modulo n et m par une congruence modulo nm. Dans la discussion ci-dessus, la situation est relativement favorable quand n est beaucoup plus petit que m, donc ce sera pratique d'intégrer chaque fois une seule congruence $x \equiv b_i \pmod{n_i}$ (et donc de *ne pas essayer* de combiner des groupes de congruences de tailles équilibrées), et de faire correspondre n au nouveau modulo n_i, et m à $n_1 \cdots n_{i-1}$. Dans cette situation, l'algorithme 2.1.4 a aussi l'avantage d'être rapide à l'exécution (car on commence à réduire m modulo n), et de rendre une valeur t assez petite, mais qui n'empêchera pas mt d'avoir une taille considérable.

Un exemple concret illustrera la méthode de calcul mieux que de longs discours. Considérons le système

$$\begin{aligned} x &\equiv 5 \pmod{64}, \\ x &\equiv 49 \pmod{63}, \\ x &\equiv 3 \pmod{61}, \\ x &\equiv 27 \pmod{59}, \\ x &\equiv 23 \pmod{53}. \end{aligned}$$

On applique d'abord l'algorithme 2.1.4 au couples $(63, 64)$, $(61, 64\times63)$, $(59, 64\times63\times61)$ et $(53, 64\times63\times61\times59)$, avec les résultats suivants.

a	b	d	t	bt
63	64	1	1	64
61	4032	1	−10	−40320
59	245952	1	−28	−6886656
53	14511168	1	−8	−116089344

Finalement on applique 4 fois la formule $c = b + (mt \times ((a-b) \bmod n)) \bmod nm$, donnant le tableau suivant (les colonnes b et m sont copiées des colonnes c et nm de la ligne précédente, la colonne mt de la colonne bt ci-dessus).

a	n	b	m	$(a-b) \bmod n$	mt	$\cdot \times \cdot \bmod nm$	$c = b + \cdot$	nm
49	63	5	64	44	64	2816	2821	4032
3	61	2821	4032	49	−40320	237888	240709	245952
27	59	240709	245952	38	−6886656	14019264	14259973	14511168
23	53	14259973	14511168	18	−116089344	217667520	231927493	769091904

On peut vérifier à chaque étape que la valeur de c obtenue possède les bons restes modulo ces moduli parmi 64, 63, 61, 59, 53 qui sont déjà pris en compte. Le système donné est donc équivalent à $x \equiv 231927493 \pmod{769091904}$.

L'application du théorème des restes chinois nécessite en général un peu de calcul avec des entiers de taille considérable, mais malgré cela, son utilité est surtout la possibilité de remplacer dans certaines situations de longs calculs avec de très grands entiers par des calculs dans des anneaux $\mathbf{Z}/n\mathbf{Z}$, où la taille des nombres est bornée. Le type de situation où cela est possible et intéressant est celui des computations dans $\mathbf{Z}$ qui sont entièrement compatibles avec la réduction modulaire (essentiellement les opérations des anneaux, avec éventuellement quelques divisions exactes si les facteurs premiers possibles des diviseurs sont prévisibles et circonscrits (pour qu'on puisse les éviter dans le choix des moduli) ; les comparaisons $x \leq y$ sont strictement interdites), et où on peut borner par estimation *a priori*, même grossière, la valeur absolue du résultat. Un exemple est le calcul du déterminant d'une très grande matrice à coefficients dans $\mathbf{Z}$. On pourra alors choisir une collection de moduli dont le produit est suffisamment grand pour que la connaissance du résultat modulo ce produit le détermine, réduire les données initiales par chacun des moduli, faire chaque fois le calcul demandé de façon modulaire, et finalement combiner les résultats modulaires par le procédé indiqué ci-dessus. Si on choisit pour les moduli uniquement des nombres premiers, on pourra même utiliser dans les calculs modulaires des techniques qui sont disponibles uniquement sur un corps, comme la méthode du pivot de Gauss dans le calcul des déterminants. Il est clair que cette méthode est d'autant plus intéressante quand on reste très longtemps dans le monde modulaire avant de "resurgir" dans $\mathbf{Z}$.

Terminons cette section avec un résultat généralisant le lemme d'Euclide, et attribué à Gauss.

2.1.9. Proposition. *Si $a, b \in \mathbf{Z}$ sont premiers entre eux et $a \mid bc$ pour un certain $c \in \mathbf{Z}$, alors $a \mid c$.*

Preuve. Le morphisme $\mathbf{Z} \to \mathbf{Z}/a\mathbf{Z}$ envoie b vers un élément inversible $\bar{b}$, et bc vers 0 ; multiplication par $\bar{b}^{-1}$ montre que l'image de c est aussi 0. Un autre argument est basé sur l'existence des pgcd : de $\operatorname{pgcd}(a,b) = 1$ on déduit $\operatorname{pgcd}(ac, bc) = c$ (car $c \mid ac, bc$ donne $c \mid \operatorname{pgcd}(ac, bc)$, et avec $d = \operatorname{pgcd}(ac, bc)/c$ on a $d \mid a, b$ et donc d inversible) ; or d'après l'hypothèse $a \mid ac, bc$, donc $a \mid \operatorname{pgcd}(ac, bc) = c$. □

2.2. *Divisibilité dans les anneaux commutatifs intègres ; anneaux factoriels.*

Dans cette section on va donner certaines notions générales sur la divisibilité. Elle a pour but de montrer qu'un certain nombre de résultats élémentaires peuvent être obtenus sans autre hypothèse que l'intégrité, et que la factorialité est presque équivalente à l'existence des pgcd ou des ppcm. Ceci dit, ce résultat ne servira rarement pour déduire la factorialité de ces existences, mais plutôt pour l'affirmation contraposée : quand la factorialité fait défaut, il ne faut pas espérer non plus d'avoir des pgcd ou des ppcm.

La relation $a \mid b$ pour "a divise b" peut aussi être lue comme "b est divisible par a", "b est multiple de a", ou encore "$b \in aR$" ou "$aR \supseteq bR$" (attention au sens de l'inclusion !). Cette relation est transitive, c'est-à-dire $a \mid b$ et $b \mid c$ entraînent $a \mid c$. On pourra aussi la simplifier par tout élément non nul : $ab \mid ac$ implique $b \mid c$ si $a \neq 0$ (et la réciproque est toujours vraie), et $ac/ab = c/b$. On écrira $d \mid x, y$ pour dire "$d \mid x$ et $d \mid y$" (d est diviseur commun de x et de y), ainsi que $x, y \mid m$ pour "$x \mid m$ et $y \mid m$" (m est multiple commun de x et de y), notations qu'on pourra même combiner : $d \mid x, y \mid m$.

Le fait que $a \mid b$ peut s'exprimer uniquement en termes d'idéaux principaux ($aR \supseteq bR$) indique que des éléments a, b tels que $aR = bR$ sont équivalents pour la relation de divisibilité : ils se divisent mutuellement, et a divise (respectivement est divisible par) c si et seulement si b possède la même propriété. La divisibilité peut donc être considérée, même si elle s'écrit un termes des éléments individuels, comme une relation d'ordre partiel définie sur l'ensemble des classes de la relation d'équivalence, dit d'association, définie par le fait d'engendrer le même idéal principal.

2.2.1. Définition. *Dans un anneau commutatif intègre R, deux éléments a, b sont associés, noté $a \sim b$, si $a \mid b$ et $b \mid a$, ou de façon équivalente si $aR = bR$, ou encore s'il existe $u \in R^\times$ tel que $au = b$.*

La dernière description, qui s'exprime aussi en disant que les classes de cette relation d'équivalence sont les orbites pour l'action du groupe $R^\times$ par multiplication sur R, a besoin d'une petite justification. Si $au = b$ avec $u \in R^\times$ on a aussi $a = bu^{-1}$ et donc $a \sim b$; réciproquement $a \sim b$ implique l'existence de $u, v \in R$ tel que $au = b$ et $bv = a$, donc $auv = a$, et comme R est intègre finalement $uv = 1$ et $u \in R^\times$.

La relation d'association se comporte bien par rapport à l'opération de multiplication, qui "passe au quotient" de l'équivalence, et définit une opération au niveau des classes d'équivalence (par contre ce n'est pas du tout le cas pour l'addition). En effet, si dans un produit $a_1 \cdots a_k$ on remplace chaque facteur par un facteur associé, cela introduit k facteurs inversibles dans le produit qui peuvent être regroupés et multipliés ensemble pour donner un seul facteur inversible, d'où le produit obtenu après le replacement sera associé au produit initial. Ainsi on obtient un monoïde $(R, \times)/\!\sim$, quotient du monoïde multiplicatif $(R, \times)$ (un monoïde est un "groupe sans inverses", c'est-à-dire un ensemble muni d'une opération associative qui possède un élément neutre). Les questions de divisibilité et de factorisation devraient logiquement être formulées au niveau de $(R, \times)/\!\sim$, mais pour éviter une certaine lourdeur dans le discours et la notation, on formulera plutôt dans $(R, \times)$; le prix à payer est un souci constant de "facteurs inversibles parasites".

2.2.2. Lemme. *Soit R un anneau commutatif intègre, et $x, y \in R \setminus \{0\}$. La correspondance $d \mapsto xy/d$ définit une bijection $f : \{\, d \in R : d \mid x, y \,\} \to \{\, m \in R : x, y \mid m \mid xy \,\}$ entre l'ensemble des diviseurs communs de x et y et l'ensemble de leurs multiples communs qui divisent xy, qui renverse la relation de divisibilité : $a \mid b \iff f(b) \mid f(a)$. Elle induit aussi une bijection entre leurs classes dans $(R, \times)/\!\sim$.*

Preuve. Si $d \mid x, y$, on a évidemment $d \mid xy$, et les égalités $(xy)/d = x(y/d) = y(x/d)$ (obtenues en simplifiant $xy = xy$ par d) montrent que xy/d est multiple commun de x et de y. Réciproquement si $x, y \mid m \mid xy$ on a $x = (xy/m)(m/y)$ (simplifier $xy = (xy/m)m$ par y) et $y = (xy/m)(m/x)$, donc $xy/m \mid x, y$. Si on prend $m = xy/d$ on retrouve $xy/m = d$ et si on prend $d = xy/m$ on retrouve $xy/d = m$, donc les applications $d \mapsto xy/d$ et $m \mapsto xy/m$ sont réciproques. Finalement si $a \mid b \mid xy$, on aura $(xy/b)(b/a) = xy/a$ et donc $xy/b \mid xy/a$, donc ces applications renversent la relation de divisibilité. □

2.2.3. Définition. *Soit R un anneau commutatif intègre, et $x, y \in R$.*

a. Un élément $d \in R$ est un pgcd *de x et y si $d \mid x, y$, et $d' \mid d$ pour tout d' tel que $d' \mid x, y$.*

b. Un élément $m \in R$ est un ppcm *de x et y si $x, y \mid m$, et $m \mid m'$ pour tout m' tel que $x, y \mid m'$.*

Quand x, y possèdent un pgcd*, respectivement un* ppcm*, les différents* pgcd *(*ppcm*) possibles forment une classe pour '$\sim$' ; on notera par* $\mathrm{pgcd}(x, y)$ *(resp.* $\mathrm{ppcm}(x, y)$*) soit cette classe dans $(R, \times)/\!\sim$, soit un représentant choisi de façon canonique, soit (si le contexte le permet) un représentant quelconque.*

Parmi les contextes qui permettent de noter par exemple $\mathrm{pgcd}(x, y)$ sans spécifier un représentant précis, on trouve notamment ceux où cette expression figure uniquement dans les relations de divisibilité, éventuellement en tant que facteur dans un produit. Dans le cas $R = \mathbf{Z}$ on a pu choisir des représentants canoniques en leur imposant la positivité, et dans le cas $R = K[X]$ de polynômes sur un corps commutatif on pourra choisir des représentants canonique en leur imposant d'être unitaire (ou nul). Dans les autres cas un peu d'attention aux formulations est nécessaire pour éviter l'ambiguïté.

2.2.4. Corollaire. *Si deux éléments non nuls x, y d'un anneau intègre admettent m comme un* ppcm*, alors x, y admettent aussi un* pgcd*, à savoir xy/m.*

Preuve. La définition de ppcm impose à m d'être diviseur de xy, et il divise tout autre multiple commun de x et y, en particulier tous ceux qui divisent xy. Alors d'après le lemme 2.2.2, xy/m est un diviseur commun de x et de y qui divise tout autre diviseur commun, autrement dit c'est un pgcd de x et de y . □

On voit donc que $\mathrm{pgcd}(x, y)\,\mathrm{ppcm}(x, y) \sim xy$ est vrai dès que les expressions à gauche ont un sens (même $x = 0$ ne pose pas de problème : y est un pgcd de 0 et de y, et 0 un ppcm). La réciproque du corollaire est fausse. En fait, on peut trouver dans tout anneau où la factorisation n'est pas unique des éléments x, y sans diviseurs communs non inversibles (dont 1 est donc un pgcd) et un multiple commun que xy ne divise pas ; ceci montre que xy, pourtant le seul candidat pour $\mathrm{ppcm}(x, y)$ d'après le corollaire, n'est pas un tel ppcm. Par exemple dans l'anneau non factoriel $\mathbf{Z}[\sqrt{5}\,\mathbf{i}]$, le fait $(1 + \sqrt{5}\,\mathbf{i})(1 - \sqrt{5}\,\mathbf{i}) = 6 = 2 \times 3$

établit cette situation pour les éléments $x = 1 + \sqrt{5}\,\mathbf{i}$, $y = 2$ et leur multiple commun 6, non divisible par $2 + 2\sqrt{5}\,\mathbf{i}$. Mais si des pgcd existent pour *tous* les couples x, y, alors des ppcm existent aussi.

2.2.5. Proposition. *Soit R un anneau commutatif intègre. Les conditions suivantes sont équivalentes :*
(i) tout couple d'éléments $x, y \in R$ possède un ppcm,
(ii) tout couple d'éléments $x, y \in R$ possède un pgcd.

Preuve. Si l'un au moins de x ou y est nul, l'autre est un pgcd des deux et 0 est un ppcm, donc on peut supposer $xy \neq 0$. On a déjà vu que (i)⇒(ii), donc supposons (ii), et soit d un pgcd de x et de y. Alors le lemme 2.2.2 dit que $x, y \mid xy/d \mid xy$ et que $xy/d \mid z$ pour tout autre z avec $x, y \mid z \mid xy$. Soit maintenant m un diviseur commun de x et de y, ne divisant pas forcément xy. Alors x et y sont chacun des diviseurs communs de xy/d et de m, et ces deux éléments possèdent un pgcd, disons q, dont x et y sont chacun des diviseurs. Alors $x, y \mid q \mid xy/d \mid xy$ donc $xy/d \mid q$ et du coup $xy/d \mid m$, ce qui montre que xy/d est un ppcm de x et de y (et q, qui lui est associé, l'est aussi). □

2.2.6. Définition. *Soit R un anneau commutatif intègre. Un élément $p \in R' = R \setminus (\{0\} \cup R^\times)$ est dit*
a. irréductible si p n'est pas produit de deux éléments de R' (donc $p = ab$ implique $a \in R^\times$ ou $b \in R^\times$),
b. premier s'il engendre un idéal premier pR de R, c'est-à-dire si $p \mid ab$ implique $p \mid a$ ou $p \mid b$.

L'ensemble R' dans la définition est celui des éléments non nuls et non inversibles ; si $c \in R'$ n'est pas irréductible, il est appelé composé ou réductible (il n'y a pas de terme pour la négation de premier). Ces qualificatifs ne sont jamais attribués à 0 ou aux éléments inversibles ; on remarque que si on ne les avait pas exclus explicitement, les inversibles auraient rejoint les rangs des irréductibles, et 0 les rang des éléments premiers (car l'idéal $0R = \{0\}$ est premier dans un anneau intègre). Comme on a vu, les notions de irréductible et premier sont confondues dans $\mathbf{Z}$, et on verra qu'elles le sont encore dans les anneaux factoriels, mais elles ne le sont pas en général, comme le montre l'exemple $p = 2$ dans $\mathbf{Z}[\sqrt{5}]$ (qui est irréductible, mais pas premier à cause de $(1+\sqrt{5})(1-\sqrt{5}) = -4$). Une implication est toujours valable :

2.2.7. Proposition. *Dans un anneau commutatif intègre, tout élément premier est irréductible.*

Preuve. Soit p un élément premier de R, et supposons $p = ab$. Alors a et b divisent tous deux p, et comme p est premier il divise à son tour l'un d'eux, disons $p \mid a$. Par conséquent on a $p \sim a$, et $b = p/a \in R^\times$. □

2.2.8. Proposition. *Soit R un anneau commutatif intègre qui vérifie les conditions de la proposition 2.2.5. Alors tout élément irréductible est premier.*

Preuve. Soit p un élément irréductible de R, et supposons que $p \mid ab$. Alors comme ab est divisible par a et p, il est aussi divisible par $\mathrm{ppcm}(a, p)$. Si p ne divise pas a, alors p et a n'ont aucun diviseur non-inversible commun, donc en appliquant le lemme 2.2.2 on voit que ap est un $\mathrm{ppcm}(a, p)$, ce qui donne $ap \mid ab$, et $p \mid b$ après simplification par $a \neq 0$. On conclut que p est un élément premier de R. □

On peut maintenant presque conclure que la factorisation unique est équivalente aux conditions de la proposition 2.2.5, c'est-à-dire à l'existence soit des pgcd soit des ppcm. La seule difficulté est qu'on ne s'est pas encore soucié de l'existence d'éléments irréductibles et plus généralement des factorisations des éléments quelconques en éléments irréductibles (on ne parle pas de factorisation en éléments premiers, et pour cause : si la notion n'est pas confondue avec celle des éléments irréductibles, c'est-à-dire s'il existe des éléments irréductibles non premiers, alors ceux-ci ne seront certainement pas factorisables en éléments premiers). L'existence des factorisations en irréductibles peut sembler évidente, car tant qu'un élément est réductible on pourra l'écrire comme produit, et continuer avec les facteurs si nécessaire. Mais bien qu'il soit ainsi dans tout les anneaux qui nous intéressent, on ne peut pas prouver sans hypothèse supplémentaire sur R que le processus se termine obligatoirement.

2.2.9. Définition. *Un anneau commutatif intègre R sera dit "avec factorisations" si tout élément non nul $a \in R$ permet au moins une écriture comme produit d'un élément inversible et d'un nombre fini d'éléments irréductibles (pas forcément distincts). On appellera un tel anneau factoriel si en plus deux telles écritures pour un même élément a sont toujours équivalentes dans le sens suivant : elles ont le même nombre de facteurs, et on peut permuter les facteurs irréductibles du second produit de telle façon que chaque facteur dans le premier produit est associé au facteur correspondant du second produit.*

Pour un anneau factoriel, la factorisation se décrit le plus simplement au niveau de $(R, \times)/\sim$.

2.2.10. Théorème. *Soit R un anneau commutatif intègre avec factorisations. Alors sont équivalents :*
(i) R est factoriel,
(ii) tout élément irréductible de R est premier,
(iii) tout couple d'éléments $x, y \in R$ possède un pgcd,
(iv) tout couple d'éléments $x, y \in R$ possède un ppcm,
(v) l'intersection de deux idéaux principaux est toujours principal.

Preuve. On a déjà vue que (iii) et (iv) sont équivalents et impliquent (ii), et par définition un ppcm de x, y est la même chose qu'un générateur de l'idéal $(xR) \cap (yR)$, d'où (iv) et (v) ne sont que deux manières de dire la même chose. Il reste donc à montrer les implications (ii) $\Rightarrow$ (i) $\Rightarrow$ (iii). La démonstration de (ii) $\Rightarrow$ (i) est essentiellement la même qu'on a vue pour $\mathbf{Z}$ à l'aide du lemme d'Euclide, mais en prenant en compte la relation d'être associé. Soient $up_1 \cdots p_k = vq_1 \cdots q_l$ deux factorisations de la même valeur, avec $u, v \in R^\times$ et $p_1, \ldots, p_k, q_1, \ldots, q_l$ irréductibles ; on applique récurrence sur k. Si $k = 0$, on a $u = vq_1 \cdots q_l \in R^\times$, ce qui n'est possible qu'avec $l = 0$ et $u = v$. Sinon réduction modulo p_1 donne $0 \in R/p_1R$ à gauche, et comme R/pR est intègre grâce à (ii), au moins un des facteurs q_i à droite devient 0 dans la réduction. Quitte à permuter les facteurs q_i, on peut donc supposer que $q_1 \in p_1R$. Comme p_1 et q_1 sont irréductibles, ceci implique $p_1 \sim q_1$, et on pourra simplifier par p_1 en remplaçant à droite vq_1 par vq_1/p_1 ; l'identification des autres facteurs et en particulier $k = l$ découlent de l'hypothèse de récurrence. Considérons finalement l'implication (i) $\Rightarrow$ (iii). Comme x est un $\mathrm{pgcd}(x, 0)$ pour tout $x \in R$ on peut supposer $x, y \neq 0$, et pour ces éléments un pgcd est donné par la formule dans (5), avec la modification que Pr désigne un ensemble de représentants des classes pour '$\sim$' d'éléments irréductibles dans R, et $v_p(a)$ est toujours donné par $v_p(a) = \max\{\, i \in \mathbf{N} : p^i \mid a \,\}$. □

Attention : contrairement à l'intersection, l'idéal somme de deux idéaux principaux dans un anneau factoriel n'est pas toujours principal, même si c'est évidemment vrai dans les anneaux où *tous* les idéaux sont principaux, comme c'est le cas dans $\mathbf{Z}$ (propriété 2.1.2) et dans $K[X]$ (corollaire 1.5.14) (et qu'on appelle des anneaux principaux). Par exemple, dans $K[X, Y]$, dont on verra plus tard que c'est un anneau factoriel, les éléments X et Y n'ont aucun facteur non constant commun, donc 1 est un $\mathrm{pgcd}(X, Y)$, mais l'idéal engendré par X et Y n'est pas principal, et ne contient pas $\mathrm{pgcd}(X, Y)$. La seule relation qui tient en général entre les idéaux $aR + bR$ et $\mathrm{pgcd}(a, b)R$, quand ce dernier existe, est que par définition $\mathrm{pgcd}(a, b)R$ est le plus petit idéal *principal* qui contient $aR + bR$.

Dans un anneau factoriel R ont peut penser de chaque élément non nul comme "cachant" un unique produit d'éléments irréductibles (et un facteur inversible pour le distinguer de ces associés), mais dans la pratique il peut être très difficile (voire impossible, cela dépend de l'anneau) d'obtenir explicitement une telle factorisation. Par exemple, déjà le problème de factoriser $P \in K[X]$ en polynômes irréductibles demande d'abord de trouver ses racines (qui donnent des facteurs irréductibles de la forme $X - a$), dont on sait que c'est difficile en général (tout dépend de ce qu'on veut dire par "trouver" ; pour $K = \mathbf{R}$ ou $K = \mathbf{C}$ des méthodes d'approximation des racines sont assez simples, mais pas satisfaisant pour toutes les applications). Pour $K = \mathbf{Q}$ ou $K = \mathbf{Z}/p\mathbf{Z}$, des méthodes algorithmiques complètes de factorisation dans $K[X]$ existent, et sont disponibles dans des systèmes de calcul formel. Dans un anneau de polynômes à plusieurs variables comme $K[X, Y, Z]$, le problème de factorisation est encore plus difficile.

2.2.11. Proposition. *Soit R un anneau factoriel, $a, b, c \in R$ tel que a, b sont premiers entre eux (c'est-à-dire* 1 *est un* $\mathrm{pgcd}(a, b)$*) et $a \mid bc$, alors $a \mid c$.*

Preuve. Voir la seconde démonstration de la proposition 2.1.9, qui n'utilise que l'existence des pgcd. □

2.3. *Anneaux euclidiens, anneaux principaux.*

On a vu que les propriétés arithmétiques de $\mathbf{Z}$ sont très largement une conséquence de la propriété 2.1.2, l'existence d'une division avec reste par tout diviseur $b \neq 0$, pour laquelle les restes sont toujours plus petit (en valeur absolue) que b. Or d'après la proposition 1.5.12, les anneaux $K[X]$ vérifient une propriété similaire, avec pour seule différence les remplacement de la valeur absolue par le degré des polynômes

(ce qui ajoute $-\infty$ à l'ensemble des valeurs possibles, mais cela ne change pas l'impossibilité d'une descente indéfinie). D'autres anneaux peuvent encore être rajouté, chacun avec son propre fonction mesurant la taille des éléments ; par exemple on pourra le montrer pour $\mathbf{Z}[\mathbf{i}]$ ou $\mathbf{Z}[\sqrt{2}\,\mathbf{i}]$ avec la fonction $z \mapsto |z|^2 = z\overline{z} \in \mathbf{N}$ comme "valeur absolue". Cela nous mène à la définition générale suivante.

2.3.1. Définition. *Un anneau euclidien est un anneau commutatif intègre R pour lequel il existe une fonction $v : R \setminus \{0\} \to \mathbf{N}$, dite stathme euclidien, telle que, pour tout $b \in R \setminus \{0\}$, chaque classe dans l'anneau quotient R/bR possède un élément r tel que ou bien $r = 0$, ou bien $v(r) < v(b)$.*

En termes d'éléments cette propriété s'exprime ainsi : pour tout $a, b \in R$ avec $b \neq 0$ il existe $q, r \in R$ tels que $a = bq + r$ et $r = 0$ ou $v(r) < v(b)$. On voit donc d'après les résultats cités que $\mathbf{Z}$ est un anneau euclidien pour le stathme $v(n) = |n|$, et $K[X]$ avec K un corps commutatif est un anneau euclidien pour le stathme $v(P) = \deg_X(P)$. La définition d'anneau euclidien exige l'existence d'un stathme, mais ne dit pas que R est *muni* d'un stathme, ce qui nous permet d'échanger le stathme pour un autre si cela nous convient. Par exemple, en rajoutant 1 à toutes les valeurs du stathme on en trouve un autre pour lequel la valeur 0 n'est pas utilisé ; on pourrait ensuite compléter le stathme à une fonction définie sur R tout entier, en affectant la valeur 0 à l'élément $0 \in R$ (ce qui laisse intacte la propriété fondamentale), de sorte qu'on puisse omettre les exceptions pour l'élément 0 dans la définition (sauf que $b = 0$ reste exclu). Mais ce changement n'est pas très commode dans le cas de $K[X]$, ce qui explique lesdites exceptions.

Au lieu de servir réellement aux changements de stathme (ceux qu'on trouve le plus facilement sont en général les meilleurs, même si c'est intéressant de savoir que sur $\mathbf{Z}$ on peut aussi utiliser $v(x) = \lfloor \log_2 |x| \rfloor$ comme stathme, au lieu de la valeur absolue), cette liberté sert surtout à pourvoir supposer des propriétés qui ne sont pas incluses dans la définition (qui n'exige que ce qui est essentiel), si on peut toujours les obtenir par un "bon choix" de stathme. Notamment, la définition n'exige pas de relation particulière entre $v(a)$ et $v(b)$ quand $a \mid b$, pourtant dans les exemples connus c'est toujours le cas. Mais on a :

2.3.2. Proposition. *Soit R un anneau euclidien. Il existe un stathme v pour R qui, en plus de la propriété exigée dans le définition, vérifie $v(a) \leq v(b)$ pour $a, b \in R \setminus \{0\}$ tels que $a \mid b$, avec égalité si et seulement si $a \sim b$.*

Preuve. Soit v_0 un stathme quelconque pour R, et pour toute classe $C = a + bR$ modulo $b \neq 0$ ne contenant pas 0 (ce qu'on écrira $C \in (R/bR) \setminus \{0\}$) posons $m(C) = \min_{x \in C}(v_0(x))$. La définition du stathme dit précisément que $m(C) < v_0(b)$ pour toute telle classe, et donc $\max_{C \in R/bR \setminus \{0\}}(m(C)) < v_0(b)$ quand $b \notin R^\times$ (pour que le maximum ne porte pas sur $\emptyset$). Posons $v(u) = 0$ pour $u \in R^\times$, et

$$v(b) = 1 + \max_{C \in (R/bR) \setminus \{0\}}(m(C))$$

pour tout autre élément $b \neq 0$. Alors il découle de ce qu'on vient d'observer que $v(b) \leq v_0(b)$ pour tout $b \neq 0$; on peut donc voir que v est aussi un stathme pour R, en prenant r dans chaque classe C de R/bR autre que bR (où évidemment on prend $r = 0$) tel qu'il minimise $v_0(r)$ sur C, et en observant $v(r) \leq v_0(r) = m(C) < v(b)$. Si on a $a \mid b \neq 0$, alors le maximum dans la définition de $v(a)$ porte sur un sous-ensemble des valeurs dans la définition de $v(b)$, car si $x \notin aR$ vérifie $v_0(x) = m(x + aR)$ il vérifie aussi $v_0(x) = m(x + bR)$ (car $x + aR \supseteq x + bR$) ; conséquent $v(a) \leq v(b)$. Finalement, si en plus $a \not\sim b$, donc $0 \notin a + bR \subset aR$, il existe $r \in a + bR$ avec $v(r) < v(b)$, mais $a \mid r$ donc $v(a) \leq v(r) < v(b)$. □

Un façon alternative de construire un (autre) stathme v avec cette propriété à partir de v_0 est de prendre $v(a) = \min_{x \in aR} v_0(x)$; il est alors directement clair que $a \mid b \neq 0$ implique $v(a) \leq v(b)$, mais il est un peu plus difficile de montrer que v est encore un stathme (exercice). On pourra en plus modifier le stathme si nécessaire pour qu'il n'y ait pas de "trous" dans son image : $v(R \setminus \{0\})$ est ou bien $\mathbf{N}$, ou bien un intervalle initial $[0, n]$ de $\mathbf{N}$. Supposant cela fait, le stathme prend la valeur 0 précisément sur $R^\times$. Un corps commutatif K est trivialement un anneau euclidien avec v nul sur $K^\times = K \setminus \{0\}$. Pour tout autre cas il existe $b \neq 0$ avec $v(b) = 1$, nécessairement irréductible, et tous les éléments de l'anneau R/bR (qui est un corps comme on le verra) ont au moins un représentant parmi les éléments de $\{0\} \cup R^\times$, d'après la définition d'un stathme; c'est une contrainte forte qui permet parfois de démontrer qu'un anneau donné *n'est pas euclidien.*

La propriété la plus importante des anneaux euclidiens est d'être principaux, ce qu'on définit ainsi.

2.3.3. Définition. *Un anneau commutatif intègre R est principal si ses seuls idéaux sont aR pour $a \in R$.*

2.3.4. Proposition. *Tout anneau euclidien est principal.*

Preuve. Soit R un anneau euclidien avec un stathme v, et (l'idéal $\{0\}$ étant principal) $I \neq \{0\}$ un idéal. Alors on aura $I = bR$ pour tout $b \in I \setminus \{0\}$ qui minimise $v(b)$ sur cet ensemble, car pour tout $a \in I$ il existe $r \in a + bR \subseteq I$ tel que $v(r) < v(b)$, donc $r = 0$ et par conséquent $a \in bR$. □

La réciproque de cette proposition est fausse, mais il n'est pas facile de donner beaucoup d'exemples qui l'illustrent. Il y a quelques anneaux d'entiers quadratiques, c'est-à-dire de la forme $\mathbf{Z}[\xi]$ où ξ est racine d'un polynôme P unitaire de degré 2 et irréductible dans $\mathbf{Z}[X]$, dont on sait qu'ils sont de ce type, notamment pour $\xi = \frac{1+\sqrt{19}\,\mathbf{i}}{2}$ qui est racine de $P = X^2 - X + 5$.

2.3.5. Proposition. *Soit R un anneau principal et $a, b \in R$. Alors pour $d \in R$ on a équivalence entre*
(i) d est un pgcd *de a et b, et*
(ii) $d \mid a, b$ et $d \in aR + bR$.
En plus, pour tout $a, b \in R$ il existe $d \in R$ qui vérifie ces conditions.

Preuve. Par définition, un pgcd(a, b) est un générateur d'un idéal principal qui contient aR et bR et qui est maximal parmi de tels idéaux. Mais dans un anneau principal $aR + bR$ est déjà un idéal principal, et condition (i) est équivalent à être l'un de ses générateurs, ce qui montre (i) ⇒ (ii) ainsi que le dernier point. Pour montrer (ii) ⇒ (i) il suffit d'observer que si d vérifie la condition (ii) et $d' \mid a, b$, alors d' divise tout élément de $aR + bR$ et en particulier d, d'où d est un pgcd(a, b). □

L'existence des pgcd et des relations de Bezout s'étend donc à tous les anneaux principaux. Les anneaux euclidiens gardent néanmoins un avantage, du moins si la propriété euclidienne de l'anneau est effective (c'est-à-dire on a un algorithme pour trouver un reste r dans la définition 2.3.1, et donc le quotient associé), dans la mesure où l'algorithme 2.1.4 s'adapte sans aucune modification essentielle à ces anneaux, et permet de trouver algorithmiquement des coefficients de Bezout. Ceci dit, ce calcul n'est pas facile dans $K[X]$ même pour $K = \mathbf{Q}$, car les coefficients rationnels dans les restes et dans les coefficients de Bezout se compliquent très rapidement, même pour des calculs de pgcd apparemment très modestes.

Considérons ensuite la factorialité, et pour commencer l'existence de factorisations. La proposition suivante est presque triviale. En plus on la démontrera ensuite avec l'hypothèse plus faible d'un anneau principal. Mais c'est parce que la preuve est plus simple dans le cas euclidien qu'on la présente séparément. On observe d'abord (pour les deux démonstrations qui suivent) que si $n = xy$ et x et y possèdent des factorisations (pas forcément uniques) on peut les combiner en une factorisation de n.

2.3.6. Proposition. *Tout anneau euclidien est un anneau avec factorisations.*

Preuve. Soit R un anneau euclidien avec un stathme v vérifiant la propriété supplémentaire de la proposition 2.3.2. Alors une décomposition $0 \neq a = xy$ avec $x, y \notin R^\times$ implique $v(x), v(y) < v(a)$. Cela permet une preuve par récurrence immédiate sur $v(n)$ que tout $n \neq 0$ admet une factorisation. Si $n \in R^\times$ ou si n est irréductible on a une factorisation évidente à un facteur. Sinon on choisit une décomposition $n = xy$ où par récurrence x et y possèdent des factorisations, et c'est donc aussi le cas de n. □

2.3.7. Proposition. *Tout anneau principal est un anneau avec factorisations.*

Preuve. On raisonne par l'absurde, en supposant que $a \in R \setminus \{0\}$ ne possède aucune factorisation. On construit une suite infinie $(a_i)_{i \in \mathbf{N}}$ d'éléments n'ayant aucune factorisation, en posant $a_0 = a$ et en continuant de façon récurrente ainsi : comme a_i ne possède aucune factorisation il n'est ni inversible ni irréductible, donc il existe une écriture $a_i = xy$ avec $x, y \notin R^\times$; si x possède une factorisation, alors y n'en possède pas (car cela donnerait une factorisation de a_i, qui n'en a pas) et on pose $a_{i+1} = y$, et sinon on pose $a_{i+1} = x$. Le fait que chaque a_{i+1} divise strictement a_i implique qu'on a une suite strictement croissante d'idéaux $a_0R \subset a_1R \subset a_2R \subset \cdots$, et leur réunion $I = \bigcup_{i \in \mathbf{N}} a_iR$ est encore un idéal (pour les propriétés de fermeture requises, $x, y \in I$ implique l'existence d'un $i \in \mathbf{N}$ avec $x, y \in a_iR$, et donc $x + y \in a_iR \subseteq I$ et $rx \in a_iR \subseteq I$ pour tout $r \in R$). Comme R est un

anneaux principal, il existe b tel que $I = bR$, ce qui nécessite $b \in I$ et donc l'existence d'un $i \in \mathbf{N}$ avec $b \in a_iR$, mais alors $a_iR \supseteq bR = I \supseteq a_{i+1}R$, contredisant l'inclusion stricte $a_iR \subset a_{i+1}R$. □

On remarque que cette démonstration utilise l'axiome du choix (forme faible, dit de "choix dépendant"), a savoir pour choisir les décompositions des a_i (dont chacune dépend des choix précédents). Ceci montre l'aspect non constructif de la démonstration (même si on disposait d'une procédure fournissant pour chaque idéal un générateur, on ne saurait pas utiliser la démonstration pour construire une factorisation d'un élément quelconque), et justifie la démonstration séparée pour le cas euclidien. En revanche, cette démonstration reste valable avec l'hypothèse plus faible que chaque idéal de R s'écrive comme $b_1R + \cdots + b_nR$, c'est-à-dire avec un nombre *fini* de générateurs (il suffit de choisir a_iR contenant tous les b_j). Cette remarque est pertinente dans la mesure où cette condition (qui caractérise les anneaux *noethériens*, une classe importante mais dont on ne parlera plus dans ce cours) est plus robuste que celle d'être principal, par exemple elle est préservée dans le passage de R à $R[X]$.

2.3.8. Théorème. *Tout anneau principal (et en particulier tout anneau euclidien) est factoriel.*

Preuve. Compte tenu de la proposition 2.3.7, c'est une conséquence immédiate du théorème 2.2.10, via la condition (v). On peut aussi donner un argument plus direct que celui qui démontrait le théorème cité, en établissant sa condition (ii) (le "lemme d'Euclide", qui donne directement la factorialité). Si $p \in R$ est irréductible et divise ab sans diviser a, alors $pR+aR = R$ (c'est un idéal principal dont le générateur divise strictement p) c'est-à-dire on a une relation de Bezout $ps + at = 1$; puis $0 \equiv abt \equiv b \pmod p$ et $p \mid b$. □

2.3.9. Proposition. *Dans un anneau principal R, tout idéal premier autre que $\{0\}$ est un idéal maximal.*

Preuve. Soit pR l'idéal premier, avec donc p premier, le cas $p = 0$ étant exclu. Alors p est irréductible d'après la proposition 2.2.7 : pR est maximal parmi les idéaux propres principaux, donc maximal. □

Par conséquent, on n'a pour un quotient R/aR d'un anneau principal avec $a \neq 0$ deux possibilités : si a est premier (donc irréductible) c'est un corps, sinon c'est un anneau non intègre. Ceci est d'une importance fondamentale dans le cas $R = K[X]$: pour un polynôme non nul $P \in K[X]$, le quotient $K[X]/(P)$ est un corps si P est irréductible, et dans ce cas l'image de X dans le quotient est une racine de P qui (à l'exception du cas $\deg_X(P) = 1$ qui est sans intérêt) n'en possède pas dans K ; dans le cas contraire c'est un anneau avec diviseurs de zéro. Ainsi, si les facteurs irréductibles dans la factorisation un polynôme P dans $K[X]$ ne sont pas tous de degré 1, on pourra rajouter une racine de P à K par une "extension du corps", en formant $K[X]/(Q)$ pour un facteur irréductible Q de P avec $\deg_X(Q) > 1$.

Le reste de cette section sera dédié à une application de cette théorie en arithmétique, qui nous permettra de caractériser l'ensemble des valeurs qui peuvent être obtenues comme la somme de deux entiers. Cette application est basée sur l'anneau $\mathbf{Z}[\mathbf{i}]$ des entiers de Gauss, dont on va montrer d'abord que c'est un anneau euclidien, avec stathme $\mathbf{Z}[\mathbf{i}] \to \mathbf{N}$ donné par l'application $N : (a+b\,\mathbf{i}) \mapsto a^2+b^2$ pour $a, b \in \mathbf{Z}$, appelée la norme pour $\mathbf{Z}[\mathbf{i}]$. La norme $N(a + b\,\mathbf{i})$ est le carré du module $|a + b\,\mathbf{i}|$ de $a + b\,\mathbf{i}$ en tant que nombre complexe, d'où on voit tout de suite sa multiplicativité : $N(xy) = N(x)N(y)$ pour tout $x, y \in \mathbf{Z}[\mathbf{i}]$. L'idée fondamentale pour montrer que c'est un stathme est que pour $x, y \in \mathbf{Z}[\mathbf{i}]$ avec $y \neq 0$, le quotient exact $\frac{x}{y}$ dans $\mathbf{C}$ peut être approximé par un entier de Gauss $q \in \mathbf{Z}[\mathbf{i}]$ (non unique) de telle manière qu'on ait $\left|\frac{x}{y} - q\right| < 1$ et donc $|x - yq| < |q|$. Cela peut être obtenu en arrondissant les parties réelle et imaginaire de $\frac{x}{y}$ vers l'entier le plus proche. Pour éviter tout calcul rationnel, on utilisera la fonction rnd : $\mathbf{Z} \times (\mathbf{Z} \setminus \{0\}) \to \mathbf{Z}$ définie par $\mathrm{rnd}(a, b) = (2a+b)$ **div** $2b$, ou 'a **div** b' désigne le quotient de la division entière de a par b, c'est-à-dire l'entier q tel que $0 \leq a - bq < |b|$. Pour $q = \mathrm{rnd}(a, b)$ on déduit de $0 \leq 2a + b - 2bq < 2b$ que $-\frac{b}{2} < bq - a \leq \frac{b}{2}$, donc q est l'unique entier tel que $\frac{a}{b} - \frac{1}{2} < q \leq \frac{a}{b} + \frac{1}{2}$.

2.3.10. Proposition. *L'anneau $\mathbf{Z}[\mathbf{i}]$ est un anneau euclidien, dont $N : (a+b\,\mathbf{i}) \mapsto a^2+b^2$ est un stathme.*

Preuve. Soit $a + b\,\mathbf{i}, c + d\,\mathbf{i} \in \mathbf{Z}[\mathbf{i}]$ avec $a, b, c, d \in \mathbf{Z}$ et $c + d\,\mathbf{i} \neq 0$. On pose $n = N(c + d\,\mathbf{i}) = c^2 + d^2 > 0$, et puis $\gamma = \mathrm{rnd}(ad + bc, n) + \mathrm{rnd}(bd - ac, n)\mathbf{i} \in \mathbf{Z}[\mathbf{i}]$ et $\rho = a + b\,\mathbf{i} - \gamma(c + d\,\mathbf{i})$. On a visiblement $\rho \in a + b\,\mathbf{i} + (c + d\,\mathbf{i})\mathbf{Z}[\mathbf{i}]$, et on montrera que $N(\rho) < n = N(c + d\,\mathbf{i})$. Si on pose $\gamma = \gamma_1 + \gamma_2\mathbf{i}$ avec $\gamma_1, \gamma_2 \in \mathbf{Z}$ on a $|n\gamma_1 - (ad + bc)| \leq \frac{n}{2}$ et $|n\gamma_2 - (bd - ac)| \leq \frac{n}{2}$ d'après la spécification de la fonction 'rnd'. En multipliant l'équation $\rho = a + b\,\mathbf{i} - \gamma(c + d\,\mathbf{i})$ par $c - d\,\mathbf{i}$ on trouve $(c - d\,\mathbf{i})\rho = (ad+bc)+(bd-ac)\mathbf{i}-n\gamma = (ad+bc-n\gamma_1)+(bd-ac-n\gamma_2)\mathbf{i}$. En appliquant la norme, qui est multiplicative,

on trouve $nN(\rho) = (ad+bc-n\gamma_1)^2 + (bd-ac-n\gamma_2)^2 \leq \frac{n^2}{4} + \frac{n^2}{4} = \frac{n^2}{2} < n^2$ d'après les inégalités qu'on vient d'évoquer. On a donc $N(\rho) < n$ comme voulu, prouvant que N est un stathme euclidien. □

On peut donc conclure que $\mathbf{Z}[\mathbf{i}]$ est un anneau euclidien, donc principal et factoriel, et comme la description de la division euclidienne est explicite, on possède un algorithme pour calculer des pgcd et des coefficients de Bezout correspondants. Le fait d'avoir l'application multiplicative N de l'anneau factoriel $\mathbf{Z}[\mathbf{i}]$ vers un autre anneau factoriel $\mathbf{Z}$ est très utile, comme le montre l'étude suivante des éléments irréductibles de $\mathbf{Z}[\mathbf{i}]$, dits "premiers gaussiens". D'abord, les éléments inversibles de $\mathbf{Z}[\mathbf{i}]$ sont forcément de norme 1, et en effet les quatre éléments 1, $\mathbf{i}$, -1, $-\mathbf{i}$ de norme 1 sont tous inversibles. Les éléments irréductibles peuvent ne pas être dans $\mathbf{Z}$, comme les plus petits d'entre eux en norme, $1+\mathbf{i}$ et ses associés ; ils peuvent aussi être dans $\mathbf{Z}$ comme c'est le cas de 3 (mais $2 = (1+\mathbf{i})(1-\mathbf{i})$ n'est pas un premier gaussien).

Le fait $(a+b\,\mathbf{i})(a-b\,\mathbf{i}) = a^2+b^2$ montre que $N(z)$, vu comme élément de $\mathbf{Z}[\mathbf{i}]$ est un multiple de z. Par conséquent, si π est un premier gaussien, la factorisation de $N(\pi)$ dans $\mathbf{Z}$ ne peut comporter qu'un seul facteur premier, et celui-ci à la puissance 2 au plus : π est un élément premier de $\mathbf{Z}[\mathbf{i}]$ (car $\mathbf{Z}[\mathbf{i}]$ est factoriel), donc $\pi \mid N(\pi)$ implique que π divise l'un des facteurs dans la factorisation, disons p, mais $\pi \mid p$ dans $\mathbf{Z}[\mathbf{i}]$ implique $N(\pi) \mid N(p) = p^2$ dans $\mathbf{Z}$, donc $N(\pi) \in \{p, p^2\}$. En plus si $N(\pi) = p^2 = N(p)$, on voit que π et p sont associés, donc cela n'arrive que pour $\pi \in \{p, p\,\mathbf{i}, -p, -p\,\mathbf{i}\}$ où p est un nombre premier qui reste irréductible dans $\mathbf{Z}[\mathbf{i}]$. De l'autre côté, si $N(\pi)$ est un nombre premier, cela suffit pour montrer que π est irréductible, par la multiplicativité de N. Dans ce cas $p = N(\pi)$ est un nombre premier qui devient réductible dans $\mathbf{Z}[\mathbf{i}]$: sa factorisation dans $\mathbf{Z}[\mathbf{i}]$ comporte comme facteurs irréductibles π et son conjugué $\overline{\pi}$ (ou leurs associés), qui sont non associés entre eux sauf si $p = 2$. Pour connaître les irréductibles de $\mathbf{Z}[\mathbf{i}]$, tout revient donc à savoir quels sont les nombres premiers p qui deviennent réductibles dans $\mathbf{Z}[\mathbf{i}]$, ou de façon équivalente qui sont dans l'image de la fonction N, c'est-à-dire qui s'écrivent comme somme de deux carrés parfaits (et en plus on aimerait savoir pour ces p quels sont ces deux carrés).

On a déjà vu que 2 se factorise en un produit de deux premiers gaussiens conjugués, ce qu'on peut aussi écrire comme un inversible et le carré d'un premier gaussien : $2 = -\mathbf{i}(1+\mathbf{i})^2$. Pour les nombres premiers p impairs, une écriture en somme de deux carrés parfaits utilisera évidemment un carré pair et un carré impair, dont les classes modulo 4 sont toujours celles de 0 et 1 ; un condition évidente pour l'existence d'une telle écriture est donc $p \equiv 1 \pmod 4$. Pour les petits nombres premiers de cette forme on constate qu'ils s'écrivent tous en somme de deux carrés : $5 = 2^2+1^2$, $13 = 3^2+2^2$, $17 = 4^2+1^2$, $29 = 5^2+2^2$, $37 = 6^2+1^2$, $41 = 5^2+4^2$, $53 = 7^2+2^2$, $61 = 6^2+5^2$, $73 = 8^2+3^2$, $89 = 8^2+5^2$, $97 = 9^2+4^2$, ...

2.3.11. Lemme. *Soit p un nombre premier. Les conditions suivantes sont équivalentes :*
(i) l'équation $x^2+1=0$ pour $x \in \mathbf{Z}/p\mathbf{Z}$ possède (au moins) une solution ;
(ii) l'élément $p \in \mathbf{Z}[\mathbf{i}]$ est réductible : $p = (a+b\,\mathbf{i})(a-b\,\mathbf{i}) = a^2+b^2$ avec $a, b \in \mathbf{Z}$;
(iii) l'idéal de $\mathbf{Z}[X]$ engendré par X^2+1 et p n'est pas premier ;
(iv) ou bien $p = 2$, ou bien $p \equiv 1 \pmod 4$.

Preuve. La condition (i) veut dire que le polynôme $X^2+1 \in (\mathbf{Z}/p\mathbf{Z})[X]$ possède une racine dans $\mathbf{Z}/p\mathbf{Z}$, ce qui est équivalent à dire (parce que $\deg_X(X^2+1) = 2$) qu'il n'est pas irréductible, ou encore qu'il engendre un idéal I qui n'est pas premier (théorème 2.2.10(ii)). Pour le morphisme surjectif $\mathbf{Z}[X] \to (\mathbf{Z}/p\mathbf{Z})[X]$ dont le noyau est engendré par p, le préimage de I est l'idéal de (iii), et l'un est premier si et seulement si l'autre l'est, car les anneaux quotients sont isomorphes (proposition 1.3.3) ; on a établi (i) $\iff$ (iii). Pour la condition (ii), l'argument est similaire : dire que p possède une factorisation non triviale (qui est forcément du type indiqué, car $N(p) = p^2$ doit être le produit dans $\mathbf{Z}$ des normes de ces facteurs) équivaut à dire qu'il engendre un idéal J qui n'est pas premier, et l'idéal de (iii) est le préimage de J pour le morphisme surjectif $\mathbf{Z}[X] \to \mathbf{Z}[\mathbf{i}]$ qui envoie $X \mapsto \mathbf{i}$ et dont X^2+1 engendre le noyau; cela établit (ii) $\iff$ (iii). Finalement l'équivalence (i) $\iff$ (iv) découle du corollaire 1.5.11. □

Ce lemme résout le problème de caractériser les premiers gaussiens : ce sont les éléments $z \in \mathbf{Z}[\mathbf{i}]$ tels que, ou bien $N(z)$ soit un nombre premier (qui ne sera pas congruent à 3 modulo 4), ou bien z soit lui-même associé à un nombre premier congruent à 3 modulo 4. On a aussi vu que dans le premier cas l'ensemble des premiers gaussiens avec la même norme $N(z)$ est constitué de deux classes d'association

conjuguées (donc de 8 éléments), sauf pour $N(z) = 2$ où c'est une seule classe (4 éléments) qui est sa propre conjuguée. Mais la preuve du lemme suggère aussi une méthode pour trouver concrètement les premiers gaussiens avec pour norme un nombre premier p donné, du moins si l'on dispose d'une solution explicite pour le (i) (mais c'est facile dans la pratique, comme il est indiqué après le corollaire 1.5.11). Si $r \in \mathbf{Z}$ est tel que $p \mid r^2 + 1$ dans $\mathbf{Z}$, alors on a $p \mid (r + \mathbf{i})(r - \mathbf{i})$ dans $\mathbf{Z}[\mathbf{i}]$, pendant que p ne divise aucun des facteurs (à cause de leurs parties imaginaires), mettant en évidence le fait que p n'est pas un élément premier dans $\mathbf{Z}[\mathbf{i}]$. Mais les facteurs irréductibles $z, \overline{z}$ dans une factorisation de $p = z\overline{z}$ dans $\mathbf{Z}[\mathbf{i}]$ sont forcément des éléments premiers de $\mathbf{Z}[\mathbf{i}]$, et divisent donc chacun l'un des facteurs $r + \mathbf{i}, r - \mathbf{i}$ (le cas $p = 2$ mis à part, z et $\overline{z}$ ne sont pas associés et ne peuvent pas tous deux diviser le même facteur, car celui-ci n'est pas divisible par $z\overline{z} = p$). Par conséquent, on peut trouver l'un de $z, \overline{z}$ comme un $\mathrm{pgcd}(p, r + \mathbf{i})$, qui peut être effectivement trouvé en appliquant l'algorithme d'Euclide dans $\mathbf{Z}[\mathbf{i}]$. Réciproquement, étant donné $z = a + b\,\mathbf{i} \in \mathbf{Z}[\mathbf{i}]$ avec $N(z) = p$ premier, la déduction d'un $r \in \mathbf{Z}$ tel que $p \mid r^2 + 1$ est moins intéressante, mais encore plus simple : un représentant r de $ab^{-1} \in \mathbf{Z}/p\mathbf{Z}$ convient (vérification facile).

2.3.12. Théorème. *Soit $n \in \mathbf{N}_{>0}$, et $n = p_1^{m_1} \cdots p_l^{m_l}$ une factorisation ($l \geq 0$, et p_i premier, $m_i > 0$, pour tout i). Une condition nécessaire et suffisante pour l'existence de $a, b \in \mathbf{Z}$ avec $n = a^2 + b^2$ est que m_i soit pair pour tout i tel que $p_i \equiv 3 \pmod 4$. Le nombre de telles paires (a, b) est alors*

$$4 \prod_{p_i \equiv 1 \,(\mathrm{mod}\ 4)} (m_i + 1).$$

Preuve. On interprète l'existence de a, b comme l'existence d'un entier gaussien z avec $N(z) = n$; or $\mathbf{Z}[\mathbf{i}]$ est factoriel et la norme multiplicative. On peut donc considérer une factorisation de z, et appliquer le fait trouvé ci-dessus que les normes des premiers gaussiens sont précisément les nombres premiers $p \not\equiv 3 \pmod 4$, ainsi que p^2 pour les nombres premiers $p \equiv 3 \pmod 4$; les produits qu'on peut former avec ces normes sont les nombres décrits dans le théorème. Il reste la formule énumérative, pour laquelle on observe qu'on peut compter le nombre de classes d'association dans $\mathbf{Z}[\mathbf{i}]$ d'éléments de norme z, et le multiplier par le nombre 4 d'éléments inversibles (et donc d'éléments dans chaque classe). Une telle classe est déterminée par le choix, pour chaque i, de m_i classes d'association de premiers gaussiens de norme p_i. Si $p \not\equiv 1 \pmod 4$, il n'a y qu'une telle classe, et donc pas de choix, mais pour $p \equiv 1 \pmod 4$ il y a deux telles classes (conjuguées). Comme l'ordre des facteurs n'a pas d'importance, le choix est déterminé par le nombre k de fois qu'on choisit l'une des deux classes, qui laisse l'autre classe pour les $m_i - k$ facteurs restants ; cela donne $m_i + 1$ possibilités différentes pour ce i ; d'où la formule du théorème. □

2.4. *Corps des fractions, hérédité de la factorialité.*

Dans cette section on montrera d'abord comment on peut construire "autour" de chaque anneau intègre R un corps $\mathrm{Frac}(R)$ le contenant, appelé le corps des fractions de R, dans lequel chaque élément s'exprime (de façon non unique bien sûr) comme quotient d'éléments de R, à l'instar de la construction de $\mathbf{Q}$ à partir de $\mathbf{Z}$. Ensuite on montrera le résultat, dû à Gauss pour le cas $R = \mathbf{Z}$ qui est aussi difficile que le cas général, que si R est factoriel alors $R[X]$ est aussi factoriel ; ce résultat étend la portée des anneaux factoriels aux cas comme $\mathbf{Z}[X]$ et $K[X, Y, Z]$, c'est-à-dire loin au delà du cas des seuls anneaux principaux.

2.4.1. Théorème. *Soit R un anneau commutatif intègre. Il existe un corps commutatif F, appelé corps des fractions $\mathrm{Frac}(R)$ de R, muni d'un morphisme d'anneaux injectif $\iota : R \to F$, tel que pour tout $x \in F$ il existe $a \in R$ et $b \in R \setminus \{0\}$ tel que $x = \iota(a)\iota(b)^{-1}$. Ce corps est unique à isomorphisme canonique près.*

On note que dans l'énoncé $\iota(b) \neq 0$ par l'injectivité de ι, et que $\iota(b)^{-1}$ est donc bien défini car F est un corps. Pour démontrer ce théorème, on commence à déduire des propriétés plus précises que le corps doit avoir. Tout élément de F s'écrit sous la forme $\iota(a)\iota(b)^{-1}$, quelle expression on notera $\frac{a}{b}$. Comme ι est un morphisme d'anneaux on a $\iota(ac)\iota(bc)^{-1} = \iota(a)\iota(c)\iota(b)^{-1}\iota(c)^{-1} = \iota(a)\iota(b)^{-1}$ pour tout $c \in R \setminus \{0\}$, autrement dit $\frac{ac}{bc} = \frac{a}{b}$. Pour $a, c \in R$ et $b, d \in R \setminus \{0\}$ on a donc $\frac{a}{b} = \frac{c}{d}$ si et seulement si $\frac{ad}{bd} = \frac{cb}{bd}$, et comme multiplication par $\iota(bd)$ est bijective et ι injectif, cela est équivalent à $ad = bc$ dans R, ce qui fournit un moyen de tester l'égalité dans F par une condition dans R.

Les formules pour l'addition et la multiplication dans F sont faciles à déduire, la première étant assez proche del a formule pour l'égailté qu'on vient d'établit. En mettant les fractions sur un dénominateur commun (qui reste non nul puisque R est un anneau intègre), on trouve

$$\frac{a}{b}+\frac{c}{d}=\frac{ad+bc}{bd} \qquad \text{et} \qquad \frac{a}{b}\times\frac{c}{d}=\frac{ac}{bd}. \tag{6}$$

Ces deux expressions sont compatibles avec la relation donnant l'égalité de fractions : si $\frac{a}{b}=\frac{a'}{b'}$ et $\frac{c}{d}=\frac{c'}{d'}$, c'est-à-dire si $ab'=ba'$ et $cd'=dc'$, alors $(ad+bc)b'd'=ab'dd'+bb'cd'=ba'dd'+bb'dc'=bd(a'd'+b'c')$, ainsi que $acb'd'=a'c'db$ directement. Avec ces préparations on est prêt à aborder la preuve du théorème.

Preuve. En tant qu'ensemble, on prend pour F l'ensemble des classes dans $R\times(R\setminus\{0\})$ pour la relation $(a,b)\sim(c,d)$ définie par $ad=bc$, qui est une relation d'équivalence car si $(a,b)\sim(c,d)\sim(e,f)$ on a $adf=bcf=bde$ qui après simplification par l'élément d donne $af=be$ comme voulu (on a utilisé que R est commutatif et intègre, donc $d\neq 0$ est régulier). On note $\frac{a}{b}$ la classe de (a,b), on définit les opérations '$+$' et '$\times$' : $F\to F$ par l'équation (6), dont on vient de voir qu'elle est compatible avec la relation '$\sim$', et on définit $\iota : R\to F$ par $\iota(a)=\frac{a}{1}$. Il est clair que ι est injectif ($\frac{a}{1}=\frac{b}{1}$ implique $a=b$) et vérifie $\iota(a+b)=\iota(a)+\iota(b)$ et $\iota(ab)=\iota(a)\iota(b)$, donc en posant $0_F=\iota(0)$ et $1_F=\iota(1)$ la partie $\iota(R)$ de F devient un anneau isomorphe (par ι) à R. Observons qu'on peut simplifier les fractions $\frac{ac}{bc}=\frac{a}{b}$ grâce à la relation '$\sim$', et que la règle d'addition devient $\frac{a}{b}+\frac{c}{b}=\frac{a+c}{b}$ quand les dénominateurs coïncident ; en plus on peut mettre toute addition dans cette forme par un choix convenable des représentants pour '$\sim$'. La vérification des axiomes d'un anneau commutatif de la définition 1.1.1 sur F tout entier se fait sans difficulté ; donnons à titre d'exemple les détails pour la distributivité. On a

$$\frac{a}{b}\times\left(\frac{c}{d}+\frac{e}{d}\right)=\frac{a}{b}\times\left(\frac{c+e}{d}\right)=\frac{a(c+e)}{bd}=\frac{ac+ae}{bd}=\frac{ac}{bd}+\frac{ae}{bd}=\frac{a}{b}\times\frac{c}{d}+\frac{a}{b}\times\frac{e}{d}$$

pour $a,c,e\in R$ et $b,d\in R\setminus\{0\}$, et d'après la remarque faite, ce cas des "dénominateurs égaux" dans l'addition couvre le cas général. Il reste à vérifier que F est un corps : $\frac{a}{b}\neq 0_F=\frac{0}{1}$ veut dire $a\neq 0$, et dans ce cas $\frac{a}{b}\times\frac{b}{a}=\frac{ab}{ba}=1_F$. L'unicité de F à isomorphisme près découle des considérations préalables, qui montraient que les éléments de F doivent correspondre aux classes pour '$\sim$', et que les équations (6) sont obligatoires ; ce sera aussi une instance d'un résultat plus général et plus formel ci-dessous. □

2.4.2. Corollaire. *Tout anneau commutatif intègre R admet un plongement dans (c'est-à-dire un morphisme injectif de R vers) un corps commutatif, à savoir le corps des fractions de R.*

2.4.3. Proposition. *Soit $f : R\to K$ est un morphisme d'anneaux injectif d'un anneau commutatif intègre R vers un corps commutatif K. Alors il existe un unique morphisme de corps commutatifs $\tilde{f}:\mathrm{Frac}(R)\to K$ qui prolonge f, c'est-à-dire tel que $f=\tilde{f}\circ\iota$.*

Preuve. Comme f est injectif, on a $f(b)\in K\setminus\{0\}=K^\times$ pour tout $b\in R\setminus\{0\}$. Pour $\frac{a}{b}\in\mathrm{Frac}(R)$ on doit avoir $\tilde{f}(\frac{a}{b})=\tilde{f}(\iota(a)\times\iota(b)^{-1})=\tilde{f}(\iota(a))\times\tilde{f}(\iota(b))^{-1}=f(a)\times f(b)^{-1}$, ce qui montre que l'on n'a qu'une seule possibilité pour $\tilde{f}$. Or cette équation définit bien une application $\mathrm{Frac}(R)\to F$ car elle est compatible avec l'égalité des fractions : si $ad=bc$ on a $f(a)f(d)=f(b)f(c)$ et donc $f(a)\times f(b)^{-1}=f(c)\times f(d)^{-1}$. Finalement une vérification directe montre que ce $\tilde{f}$ est bien un morphisme de corps, par exemple $\tilde{f}(\frac{a}{b}+\frac{c}{b})=\tilde{f}(\frac{a+c}{b})=f(a+c)f(b)^{-1}=(f(a)+f(c))f(b)^{-1}=f(a)f(b)^{-1}+f(c)f(b)^{-1}=\tilde{f}(\frac{a}{b})+\tilde{f}(\frac{c}{b})$. □

Cette proposition met en évidence le morphisme canonique du théorème 2.4.1 : si K est un corps commutatif et $f : R\to K$ un morphisme d'anneaux injectif avec la propriété du théorème, alors la proposition fournit un morphisme de corps $\tilde{f}:\mathrm{Frac}(R)\to K$ tel que $f=\tilde{f}\circ\iota$, et qui est surjectif car $f(a)f(b)^{-1}=\tilde{f}(\frac{a}{b})$; il s'agit donc d'un isomorphisme de corps. Une autre conséquence de la proposition est que tout morphisme injectif d'anneaux commutatifs intègres $g : R\to S$ se prolonge de façon unique en un morphisme de corps $\tilde{g}:\mathrm{Frac}(R)\to\mathrm{Frac}(S)$ (appliquer la proposition à $\iota_S\circ g : R\to\mathrm{Frac}(S)$).

Mis à part l'archétype $\mathbf{Q}=\mathrm{Frac}(\mathbf{Z})$ des corps des fractions, le cas le plus important de la formation du corps $\mathrm{Frac}(R)$ est celui où R est un anneau de polynômes sur un corps commutatif K, pour lequel on emploie la notation abrégée $K(X_1,\dots,X_n)$ pour $\mathrm{Frac}(K[X_1,\dots,X_n])$, et dont les éléments s'appellent des

fractions rationnelles en $X_1, \ldots, X_n$ sur K (terme un peu pléonastique, on se demande ce que pouvait être une "fraction irrationnelle"). D'après la définition du corps des fractions, une fraction rationnelle s'écrit donc de façon non unique comme une fraction formée de deux polynômes (avec pour seule condition que le dénominateur ne soit pas le polynôme nul), et la multiplication ou simplification du numérateur et du dénominateur par un même facteur non nul ne change pas la fraction rationnelle désignée. Contrairement aux polynômes, il n'y a en général pas de morphisme de substitution défini sur $K(X_1, \ldots, X_n)$.

La construction du corps des fractions appliquée aux anneaux commutatifs intègres non isomorphes peut très bien avoir pour résultat des corps isomorphes, autrement dit le corps $\mathrm{Frac}(R)$ "ne se souvient pas" de l'anneau R ayant servi pour sa construction. Par exemple pour n'importe quel sous-anneau R de $\mathbf{Q}$ (et il y en a beaucoup) on voit facilement que $\mathrm{Frac}(R) \cong \mathbf{Q}$ canoniquement (le droit de mettre certains nombres rationnels au numérateur et au dénominateur ne change pas le nombre de classes de fractions). En particulier on a toujours $\mathrm{Frac}(\mathrm{Frac}(R)) \cong \mathrm{Frac}(R)$, ce qui est un cas particulier de $\mathrm{Frac}(K) \cong K$, valable quand K est (déjà) un corps commutatif. On a aussi $\mathrm{Frac}(R[X_1, \ldots, X_n]) \cong \mathrm{Frac}(R)(X_1, \ldots, X_n)$ pour tout anneau commutatif intègre R, ce qui montre qu'on ne perd pas de généralité en ne considérant les fractions rationnelles que sur un corps commutatif.

Sous des hypothèses supplémentaires assez faibles sur R, il existe des formes irréductibles de toutes les fractions dans $\mathrm{Frac}(R)$, c'est-à-dire des formes où numérateur et dénominateur n'ont aucun diviseur commun non inversible (il suffit qu'il n'existe pas de chaînes infinies de diviseurs stricts : on pourra alors simplifier par des diviseurs non inversibles communs du numérateur et du dénominateur jusqu'à ce qu'il n'en ait plus). Si R est un anneau factoriel, comme c'est le cas pour $R = \mathbf{Z}$ et pour $R = K[X_1, \ldots, X_n]$ (on le sait pour $\mathbf{Z}$ et $K[X]$ qui sont principaux, on le verra pour les autres), la forme irréductible est même unique à multiplication près du numérateur et du dénominateur par un même facteur inversible, et elle peut être obtenue à partir d'une fraction quelconque en simplifiant numérateur et dénominateur par un pgcd des deux. Dans le cas des nombres rationnels, on peut même choisir une forme irréductible privilégiée en exigeant un dénominateur positif, et pour les fractions rationnelles on pourra de façon similaire exiger un dénominateur unitaire. Mais rappelons que la considération des formes irréductibles n'entre point dans la construction du corps de fractions, qui elle ne suppose que la commutativité et l'intégrité de l'anneau de base, et qui n'est nullement plus compliquée que son cas de base, la construction de nombres rationnels. En retournant cette observation, R. Godement remarque dans son "Cours d'Algèbre" (1962) :

> *Le lecteur évitera de croire qu'on pourrait simplifier ces raisonnements dans le cas « élémentaire » où il s'agit de construire les nombres rationnels à partir des nombres entiers. Un nombre rationnel peut s'écrire d'une infinité de façons sous le forme d'une fraction, et on ne peut pas définir la somme (par exemple) de deux nombres rationnels en se bornant à poser [(6)] ; pour que cette formule définisse la somme de deux* nombres rationnels *on doit montrer que si l'on remplace les fractions a/b et c/d par des fractions équivalentes [...]. Le fait qu'on ne se donne pas la peine, dans l'enseignement élémentaire, de faire ces démonstrations ôte tout espèce de valeur mathématique aux définitions (sic) ainsi obtenues de la somme et du produit de deux nombres rationnels, et constitue une escroquerie majeure, destinée à masquer à des enfants innocents et sans défense la difficulté réelle du problème.*

On va maintenant aborder la démonstration du fait que si R est un anneau factoriel, l'anneau de polynômes $R[X]$ est aussi factoriel. Ce résultat se base sur la construction des corps de fractions, et en particulier sur le plongement de $R[X]$ dans $\mathrm{Frac}(R)[X]$, ce dernier étant principal et donc factoriel dans tous les cas. Évidemment cela ne rendra pas $R[X]$ factoriel sans l'hypothèse que R le soit (considérer les polynômes constants), mais indique que le point essentiel sera de comprendre le passage de R à $\mathrm{Frac}\, R$ au niveau des polynômes, et qui "se passe bien" dans le cas où R est un anneau factoriel ; on pensera d'abord au cas $R = \mathbf{Z}$. Commençons par une proposition facile qui montre que le fait d'étendre l'anneau des coefficients de R à $\mathrm{Frac}(R)$ ne fait que diminuer le nombre de classes d'association des polynômes.

2.4.4. Proposition. *Soit R un anneau commutatif intègre. Pour $P \in \mathrm{Frac}(R)[X]$ il existe $P' \in R[X]$ associé à P dans* $\mathrm{Frac}(R)[X]$. *Deux éléments associés de $R[X]$ sont aussi associés dans* $\mathrm{Frac}(R)[X]$.

Preuve. Le dernier point est évident, car un élément inversible de $R[X]$ sera aussi inversible dans $\mathrm{Frac}(R)[X]$. Puisque tout élément non nul de R est inversible dans $\mathrm{Frac}(R)$, toute multiplication de $P \in \mathrm{Frac}(R)[X]$ par un tel élément donnera un élément associé à P dans $\mathrm{Frac}(R)[X]$, et pour le premier point il suffira donc de trouver un tel élément qui fera rentrer tous les coefficients de P dans R,

c'est-à-dire qui transforme ces coefficients en fractions dont le dénominateur divise le numérateur. On n'est pas obligé de chercher un facteur "économique", donc on pourra prendre pour chaque coefficient non nul de P une fraction le représentant, et prendre comme facteur le produit de tous les dénominateurs de ces fractions ; la multiplication par cet élément non nul de R fera certainement l'affaire. □

L'idée de base pour factoriser un polynôme dans $R[X]$ est de le factoriser d'abord dans $\mathrm{Frac}(R)[X]$, ce qui est en principe possible puisque l'anneau est factoriel (on ne parle pas ici des questions d'effectivité de la factorisation dans $K[X]$, qui contrairement au calcul du pgcd ne peuvent pas être traitées uniformément pour tous les corps K), puis de faire rentrer dans $R[X]$ les facteurs P_i de cette factorisation, quitte à rajouter un facteur "constant" $\alpha \in \mathrm{Frac}(R)$ à la factorisation, de s'organiser pour que α appartienne à R, et de le factoriser séparément dans R. Il est clair que cette dernière étape va exiger que R soit factoriel, et il y a deux autres soucis dans cette approche dont on verra qu'on peut les surmonter sous la même hypothèse. Le premier souci est évidemment qu'on puisse obtenir que $\alpha \in R$, et le second souci est que les facteurs irréductibles P_i dans $\mathrm{Frac}(R)[X]$ restent irréductibles dans $R[X]$. La seule façon qu'un tel P_i puisse être réductible dans $R[X]$ est qu'il soit divisible par un élément inversible dans $\mathrm{Frac}(R)[X]$ qui ne le soit pas dans $R[X]$, c'est-à-dire un polynôme constant (par rapport à X) mais non inversible dans R. Ce second souci est donc lié au premier, car un tel facteur constant dépend de la manière pour faire rentrer P_i dans $R[X]$ par le choix d'un élément associé P_i' ; au lieu d'introduire un diviseur constant dans P_i', on pourra l'incorporer par multiplication dans α, ce qui ne fera qu'améliorer les chances du dernier d'appartenir à R. On est donc amené à considérer les choix les plus économiques possible d'un représentant dans $R[X]$ d'une classe donnée d'éléments associés dans $\mathrm{Frac}(R)[X]$.

2.4.5. Définition. *Un polynôme $P \in R[X]$ est dit primitif si ses seuls diviseurs dans R sont les $u \in R^\times$.*

Dans le cas où R est factoriel, on pourra extraire le plus grand (dans le sens de la divisibilité) diviseur constant de tout polynôme non nul $P \in R[X]$ en calculant le pgcd d de tous ces coefficients. Comme au moins un de ces coefficients n'est pas nul, on aura $d \neq 0$, et P/d sera un polynôme primitif.

2.4.6. Définition/Proposition. *Si R est un anneau factoriel et $P \in R[X]$, le contenu $c_X(P)$ de P (par rapport à X) est le* pgcd *de tous les coefficients de P (comme le* pgcd*, $c_X(P)$ est en fait une classe d'association d'éléments de R). On a une décomposition $P = c_x(P)P'$ où P' est un polynôme primitif.*

Cette dernière affirmation (qui suppose évidemment le choix d'une valeur pour $c_X(P)$ dans sa classe), découle du fait que si $d \in R$ était un diviseur non inversible de (tous les coefficients de) P', alors $dc_X(P)$ serait diviseur commun de tous les coefficients de P sans diviser $c_X(P)$, en contradiction avec la définition d'un pgcd. Par un raisonnement similaire on trouve la règle suivante.

2.4.7. Fait. *Si R est un anneau factoriel et $P \in R[X]$ est primitif, alors $c_X(aP) = a$ pour tout $a \in R$.*

2.4.8. Corollaire. *Soit $P \in R[X]$ primitif avec R factoriel, et $\alpha \in \mathrm{Frac}(R)$. Si $\alpha P \in R[X]$ alors $\alpha \in R$.*

Preuve. Écrivons $\alpha = \frac{a}{b}$ avec $a, b \in \mathbf{R}$. Alors $\alpha P \in R[X]$ s'écrit sous la forme $\frac{aP}{b} \in R[X]$, qui montre que b divise tous les coefficients de aP, et donc $c_X(aP) = a$, autrement dit $\frac{a}{b} \in R$. □

On peut maintenant affiner la proposition 2.4.4 pour le cas où R est un anneau factoriel :

2.4.9. Corollaire. *Soit R un anneau factoriel. Pour $P \in \mathrm{Frac}(R)[X]$ il existe $P' \in R[X]$ associé à P dans $\mathrm{Frac}(R)[X]$ et primitif dans $R[X]$; en plus P' est unique à association dans $R[X]$ près.*

Preuve. Seulement l'unicité demande encore une justification. Si $P'' = \alpha P'$ avec $\alpha \in \mathrm{Frac}(R)^\times$ est un autre polynôme primitif dans $R[X]$, alors le corollaire 2.4.8 montre $\alpha, \alpha^{-1} \in R$, et donc $\alpha \in R^\times$. □

Si P est un polynôme irréductible dans $\mathrm{Frac}(R)[X]$, il est clair qu'on n'obtiendra un polynôme irréductible dans $R[X]$ qui soit associé à P dans $\mathrm{Frac}(R)[X]$ que si l'on choisit un P' comme dans le corollaire, et il est également facile de voir qu'un produit PQ dans $R[X]$ ne peut être primitif que si les facteurs P et Q le sont. L'étape cruciale dans notre raisonnement sera d'obtenir des énoncés réciproques à ces constats, que voici.

2.4.10. Lemme de Gauss. *Soit R un anneau factoriel.*
(1) Le produit PQ de deux polynômes primitifs $P, Q \in R[X]$ est primitif dans $R[X]$.
(2) Un polynôme $P \in R[X] \setminus R$ qui est irréductible dans $R[X]$ est primitif et irréductible dans $\mathrm{Frac}(R)[X]$.

Preuve. Pour (1), soient $P, Q \in R[X]$ primitifs et supposons qu'une constante $d \in R \setminus R^\times$ divise le produit PQ. Comme R est factoriel on peut trouver (en factorisant d dans R) au moins un diviseur *irréductible* p de d. Alors d'après le théorème 2.2.10, p est aussi premier, ce qui veut dire que l'anneau quotient R/pR est intègre. D'après le corollaire 1.4.3 $(R/pR)[X]$ est aussi intègre, et par le choix de p on a $\pi(PQ) = 0$ pour le morphisme surjectif $\pi : R[X] \to (R/pR)[X]$ qui opère par la projection canonique $R \to R/pR$ sur les coefficients ; par conséquent on a $\pi(P) = 0$ ou $\pi(Q) = 0$. Mais cela veut dire que l'un de P, Q est divisible par p, ce qui contredit le fait qu'il sont tous les deux primitifs.

Ensuite pour (2), considérons $P \in R[X]$ qui est non constant et irréductible dans $R[X]$. Cela implique que P est primitif (sinon on aurait une décomposition $P = d(P/d)$ en facteurs non inversibles dans $R[X]$) ; supposons pour une contradiction que l'on ait $P = ST$ avec $S, T \in \mathrm{Frac}(R)[X]$ non constants. On choisit d'après le corollaire 2.4.9 des polynômes primitifs S', T' dans $R[X]$ qui sont associés à S respectivement à T dans $\mathrm{Frac}(R)[X]$, et on aura $P = \alpha S'T'$ pour un certain $\alpha \in \mathrm{Frac}(R)^\times$. Or $S'T'$ est primitif d'après le point (1), et l'unicité dans le corollaire 2.4.9 donne $\alpha \in R^\times$. Mais la décomposition $P = \alpha S'T'$ se passe alors dans $R[X]$, avec S', T' non constants donc non inversibles, contredisant l'irréductibilité de P. □

2.4.11. Théorème. *Si R est un anneau factoriel, alors $R[X]$ est un anneau factoriel aussi.*

Preuve. Il est facile à montrer que $R[X]$ est un anneau avec factorisations : tout $P \in R[X] \setminus \{0\}$ s'écrit $P = c_X(P)P'$ avec P' primitif ; $c_X(P)$ se factorise dans R par hypothèse, et P' ne peut se décomposer (si on écarte des facteurs dans $R^\times$) qu'en produit de polynômes primitifs de degrés plus bas, donc l'itération de tels décompositions se termine forcément avec des facteurs irréductibles (et toujours primitifs). Pour montrer l'unicité (à l'ordre et à association dans $R[X]$ près) de cette factorisation, on commence par constater que les éléments irréductibles de $R[X]$ sont de deux types : ceux qui sont dans R (et qui sont inversibles dans $\mathrm{Frac}(R)[X]$) et les autres qui sont primitifs. Deux continuations sont possibles.

En considérant une factorisation quelconque de P, le lemme de Gauss montre que le produit des facteurs du second type est primitif, et il est donc un représentant primitif P' de la classe d'association dans $\mathrm{Frac}(R)[X]$ de P comme dans le corollaire 2.4.9. Le produit de facteurs du premier type est (un représentant de la classe) $c_X(P)$, et il est déterminé par P à association dans $R[X]$ près, tout comme P'. Par conséquent il suffit de montrer l'unicité de la factorisation séparément pour $c_X(P)$ et pour P'. Dans le premier cas l'unicité relève de la factorialité de R. Dans le second cas le lemme de Gauss montre que les facteurs de la factorisation dans $R[X]$ sont encore irréductibles dans $\mathrm{Frac}(R)[X]$, et y constituent donc une factorisation de P'. Mais cette dernière est unique à l'ordre et à association de ces facteurs dans $\mathrm{Frac}(R)[X]$ près, et le représentant primitif de chaque classe d'association dans $\mathrm{Frac}(R)[X]$ est unique à association dans $R[X]$ près (corollaire 2.4.9), ce qui établit l'unicité de la factorisation dans $R[X]$.

L'autre continuation établit la condition (ii) du théorème 2.2.10. Si $p \in R$ est un élément irréductible de $R[X]$ du premier type, l'idéal principal $pR[X]$ est le noyau de la surjection $R[X] \to (R/pR)[X]$ dont on a déjà vu que l'image est intègre, donc p est premier dans $R[X]$. Un élément irréductible Q du second type est irréductible dans $\mathrm{Frac}(R)[X]$ d'après le lemme de Gauss, et donc premier car $\mathrm{Frac}(R)[X]$ est factoriel, autrement dit $\mathrm{Frac}(R)[X]/(Q)$ est intègre. Alors son sous-anneau $\theta(R[X])$, image du morphisme composé $\theta : R[X] \to \mathrm{Frac}(R)[X] \to \mathrm{Frac}(R)[X]/(Q)$ est aussi intègre, et on a $\ker(\theta) = Q\,\mathrm{Frac}(R)[X] \cap R[X] = QR[X]$, la seconde égalité parce que tout élément de $Q\,\mathrm{Frac}(R)[X]$ s'écrit $Q\alpha S$ avec $\alpha \in \mathrm{Frac}(R)$ et $S \in R[X]$ primitif, et si aussi $Q\alpha S \in R[X]$, alors $\alpha \in R$ d'après le corollaire 2.4.8, car QS est primitif. On a montré que $QR[X]$ est un idéal premier de $R[X]$, donc que Q est premier dans $R[X]$ comme voulu. □

La preuve du théorème obtient la factorialité de $R[X]$ à l'aide de celle de $\mathrm{Frac}(R)[X]$, un anneau qui possède la propriété plus forte d'être principal. Mais cela ne veut pas dire que dans la pratique la factorisation dans $\mathrm{Frac}(R)[X]$ est plus simple que celle dans $R[X]$. C'est plutôt le contraire : on utilise la forme contraposée du lemme de Gauss qui implique que un polynôme dans $\mathrm{Frac}(R)[X]$ est réductible (si et) seulement si le représentant de sa classe d'association qui est primitif dans $R[X]$ est réductible ;

l'arithmétique beaucoup plus contraignante de R permettra souvent soit de trouver une décomposition du dernier, soit de prouver qu'il n'en existe pas. On peut montrer que le problème de factorisation dans $\mathbf{Q}[X]$ se résolut par ce type de méthodes de façon algorithmique (mais dont la description est trop compliquée pour traiter dans ce cours). Nous clorons ce chapitre avec quelques considérations utiles pour trouver des factorisations dans $\mathbf{Q}[X]$, et surtout pour vérifier qu'une décomposition donnée en est une. Si l'on ne parle pas de $\mathbf{R}[X]$ ou de $\mathbf{C}[X]$, c'est parce que pour ces corps la factorisation n'est pas accessible par des méthodes exactes, et elle se résume donc par des méthodes d'approximations de racines complexes. Le seul type de questions dans ce domaine qui relèvent du calcul exact est la détermination du nombre précis de racines réelles d'un polynôme à coefficients rationnels (qu'on peut supposer irréductible dans $\mathbf{Q}[X]$).

Si on a un polynôme primitif dans $\mathbf{Z}[X]$ qu'on veut factoriser, une première chose à chercher sont des facteurs éventuels de la forme $aX + b$, qui correspondent aux racines rationnelles $-\frac{b}{a}$ du polynôme. Le nombre de candidats pour de tels facteurs est fini, d'après le résultat élémentaire suivant.

2.4.12. Proposition. *Si un polynôme P dans $R[X]$ est divisible par un polynôme $aX + b$ de degré 1, alors a est un diviseur du coefficient dominant de P, et b est un diviseur du coefficient constant de P.* □

En utilisant cette condition, il ne faut évidemment pas oublier que les diviseurs d'un entier peuvent être positifs ou négatifs, et qu'il faut donc tester des racines éventuelles avec les deux signes. Si cette méthode suffit pour factoriser les polynômes jusqu'au degré 3, les polynômes de plus haut degré nécessitent d'autres considérations. L'outil principal est la réduction modulo p qui définit un morphisme d'anneaux $\pi : \mathbf{Z}[X] \to (\mathbf{Z}/p\mathbf{Z})[X]$ pour tout nombre premier p (et même pour tout entier p, mais le caractère factoriel de $(\mathbf{Z}/p\mathbf{Z})[X]$ quand p est premier est un atout important). Par conséquent, si $P = ST$ est une décomposition dans $\mathbf{Z}[X]$, alors $\pi(P) = \pi(S)\pi(T)$ en est une dans $(\mathbf{Z}/p\mathbf{Z})[X]$ (la réciproque est fausse : une décomposition de $\pi(P)$ peut très bien ne pas provenir d'une décomposition de P). Ce fait est surtout utile pour sa contraposée, qui dit que sans décomposition de $\pi(P)$ il ne peut pas y avoir une de P non plus, mais il faut faire attention aux facteurs inversibles dans $(\mathbf{Z}/p\mathbf{Z})[X]$ (qui existent toujours) : un facteur $\pi(S)$ peut être de degré 0, soit parce que déjà $\deg_X(S) = 0$, soit parce que la réduction modulo p annule son coefficient dominant. Une conclusion peut être tiré si ces deux possibilités sont écartées :

2.4.13. Proposition. *Si $P = \mathbf{Z}[X]$ est primitif, et p est un nombre premier ne divisant pas le coefficient dominant de P et tel que l'image $\pi(P)$ dans $(\mathbf{Z}/p\mathbf{Z})[X]$ soit irréductible, alors P est irréductible dans $\mathbf{Z}[X]$.*

Preuve. Les facteurs d'une décomposition éventuelle de P, primitif, seront de degré > 0. Le coefficient dominant de P étant le produit de ceux des facteurs, ces coefficients ne peuvent être divisibles par p; la réduction modulo p donne donc une décomposition non triviale de $\pi(P)$, contredisant l'hypothèse. □

On voit que savoir factoriser dans $(\mathbf{Z}/p\mathbf{Z})[X]$ peut s'avérer utile pour la factorisation dans $\mathbf{Z}[X]$ et dans $\mathbf{Q}[X]$. Le nombre de polynômes irréductibles dans $(\mathbf{Z}/p\mathbf{Z})[X]$ d'un degré donné est fini, donc on pourra en principe trouver ces irréductibles et les factorisations des réductibles par une méthode similaire au crible d'Ératosthène. Il faut cependant éviter de croire que cette méthode soit suffisamment efficace pour être utile pour des calculs à la main, sauf pour des très petites valeurs de p tels que $2, 3$. Le cas le plus simple où cette méthode serait utile est pour décider la décomposition éventuelle de polynômes de degré 4 en deux facteurs quadratiques (sinon un test de racines suffit). Or il y a $\frac{p(p-1)}{2}$ polynômes unitaires irréductibles de degré 2 dans $(\mathbf{Z}/p\mathbf{Z})[X]$ (soit p^2 polynômes unitaires, moins $\frac{p(p+1)}{2}$ différents produits de deux facteurs unitaires de degré 1), donc il faudrait autant de divisions polynomiales dans $(\mathbf{Z}/p\mathbf{Z})[X]$ pour tester la réductibilité d'un polynôme de degré 4 donné. Pour trouver tous les polynômes de degré 4 ainsi décomposables il faudrait calculer $\frac{p^4-2p^3+3p^2-2p}{8}$ produits polynomiaux.

La factorisation dans $(\mathbf{Z}/p\mathbf{Z})[X]$ n'est donc pas vraiment faisable sans l'aide (et surtout la capacité d'éviter des erreurs) d'un ordinateur. Mais avec cette aide, on peut faire beaucoup mieux que d'essayer différentes décompositions comme le fait le crible d'Ératosthène. Voici l'esquisse d'une méthode due à Elwyn Berlekamp, qui montre l'utilité de considérations concernant la structure algébrique abstraite de certains anneaux, même lorsque certains aspects de cette structure ne sont pas explicitement connus. Étant donné un polynôme $P \in (\mathbf{Z}/p\mathbf{Z})[X]$ à factoriser, l'attention se focalise sur l'anneau quotient $A = (\mathbf{Z}/p\mathbf{Z})[X]/(P)$. On peut calculer dans A grâce à la division euclidienne par P pour réduire les représentants, et on sait que A est un corps si et seulement si P est irréductible (théorème 2.2.10(ii) et proposition 2.3.9). Plus généralement si la factorisation de P comporte $n \geq 1$ facteurs irréductibles distincts $P_1, \ldots, P_n$ (et donc premiers entre eux deux à deux), alors A sera le produit direct des n corps $K_i = (\mathbf{Z}/p\mathbf{Z})[X]/(P_i)$, pour $i = 1, \ldots, n$, et donc un anneau non intègre si $n > 1$. (Le cas restant où la factorisation de P contient des facteurs répétés est très rare, et peut être détecté par le calcul de $\mathrm{pgcd}(P, P')$

où P' est la dérivée formelle de P par rapport à X, car tout facteur répété divisera ce pgcd ; si celui-ci n'est pas 1, il donne une décomposition non triviale dont on peut ensuite se contenter de factoriser les deux parties. On supposera désormais ce cas écarté.) L'image de $Q \in (\mathbf{Z}/p\mathbf{Z})[X]$ dans A est un diviseur de zéro si l'un au moins de ces images dans les facteurs K_i est nulle, mais elles ne le sont pas toutes ; c'est précisément dans ce cas que $\operatorname{pgcd}(P,Q)$ donne un diviseur non trivial de P, à savoir le produit des P_i pour lequel l'image est nulle.

Chaque facteur K_i de A contient un sous-corps $\mathbf{Z}/p\mathbf{Z}$, et le produit $\Pi \subseteq A$ de ces n sous-corps est *plus grand* que le sous-corps $\mathbf{Z}/p\mathbf{Z}$ de A si $n > 1$, c'est-à-dire si P est réductible. Même si l'on ne connaît pas explicitement la décomposition de A en facteurs K_i (car cela revient a connaître la factorisation de P), on peut reconnaître les éléments de Π comme les solutions de l'équation $x^p = x$, quelle équation s'évalue dans chaque facteur K_i séparément, et dont tout $a \in \mathbf{Z}/p\mathbf{Z}$ est racine (c'est le petit théorème de Fermat, qui découle de la proposition 1.2.10 en écrivant $a = 1 + \cdots + 1$) ; dans le corps K_i, il ne peut pas y avoir plus que ces p racines. Or dans A, qui est entre autres un espace vectoriel sur $\mathbf{Z}/p\mathbf{Z}$, l'application $F : x \mapsto x^p$ est (malgré l'apparence) une application *linéaire* $A \to A$ (toujours grâce à la proposition 1.2.10), dont on établit facilement la matrice par rapport à la base formée des images dans A des monômes X^i pour $0 \leq i < \deg_X(P)$ (et l'exponentiation dans A est relativement peu coûteuse à calculer). L'ensemble Π des points fixes de F peut donc être trouvé par des méthodes de l'algèbre linéaire (notamment le pivot de Gauss), comme le noyau de l'application $F - \mathrm{id}_A$. Si ce noyau est de dimension 1, c'est-à-dire s'il est réduit au sous-corps $\mathbf{Z}/p\mathbf{Z}$ de A dont on sait qu'il est contenu dans Π, on pourra conclure que $n = 1$, et donc que P est irréductible. Sinon on sait que P est réductible, et on aura des éléments $\pi \in \Pi \setminus \mathbf{Z}/p\mathbf{Z} \subseteq A$. Un tel π n'est pas toujours un diviseur de zéro dans A, mais on sait que ses coordonnées (inconnues) dans les K_i sont chacune dans $\mathbf{Z}/p\mathbf{Z} \subseteq K_i$, et elles ne sont pas toutes égales (car $\pi \notin \mathbf{Z}/p\mathbf{Z} \subseteq A$). Parmi les p éléments de A de la forme $\pi - a$ pour $a \in \mathbf{Z}/p\mathbf{Z}$, on trouvera donc au moins deux fois un diviseur de zéro (quand a est égal à l'une des coordonnées de π), ce qu'on peut détecter par le calcul dans $\mathbf{Z}/p\mathbf{Z}[X]$ de $\operatorname{pgcd}(P,Q)$ pour un représentant Q de $\pi - a$, et qui donne un diviseur non trivial de P. Quand p est grand, cette dernière étape reste coûteuse, mais on ne détaillera pas ici les méthodes connues pour l'accélérer.

La réduction modulo p d'un polynôme (primitif) $P \in \mathbf{Z}[X]$ peut parfois démontrer que P est irréductible même si sa réduction modulo p ne l'est pas. Le cas le plus célèbre est donné par le

2.4.14. Critère de Schönemann-Eisenstein. *Soit $P \in \mathbf{Z}[X]$ un polynôme primitif et p un nombre premier ne divisant pas son coefficient dominant, mais divisant tous les autres coefficients de P, et tel que p^2 ne divise pas le coefficient constant de P. Alors P est irréductible dans $\mathbf{Z}[X]$.*

Preuve. Supposons pour une contradiction que P possède une décomposition non triviale $P = ST$ dans $\mathbf{Z}[X]$. Alors $S, T \in \mathbf{Z}[X]$ sont de degrés > 0, et leurs coefficients dominants, diviseurs de celui de P, ne sont pas divisibles par p. Alors la réduction modulo p donne $\overline{P} = \overline{S}\,\overline{T}$ dans $(\mathbf{Z}/p\mathbf{Z})[X]$, et on a $\deg_X(\overline{S}) = \deg_X(S) > 0$ et $\deg_X(\overline{T}) = \deg_X(T) > 0$. Mais d'après les hypothèses on a $\overline{P} = aX^d$ avec $a \in \mathbf{Z}/p\mathbf{Z}$ et $d = \deg_X(P)$, et ses diviseurs $\overline{S}$ et $\overline{T}$ ne peuvent qu'être réduits à un seul terme eux aussi, car $(\mathbf{Z}/p\mathbf{Z})[X]$ est factoriel. Alors les coefficients constants de $\overline{S}$ et $\overline{T}$ sont nuls, et ceux de S et T donc divisibles par p, contredisant l'hypothèse que p^2 ne divise pas le coefficient constant de $P = ST$. □

L'avantage de ce critère est que les conditions sont très faciles à vérifier, beaucoup plus faciles que de vérifier qu'un polynôme dans $(\mathbf{Z}/p\mathbf{Z})[X]$ est irréductible, comme il est nécessaire pour l'application de la proposition 2.4.13. Par contre le critère ne couvre qu'une toute petite partie des polynômes primitifs irréductibles de $\mathbf{Z}[X]$ (la proposition 2.4.13 ne couvre pas tous les cas non plus, c'est-à-dire il existe des polynômes irréductibles dans $\mathbf{Z}[X]$ qui deviennent réductibles modulo p pour *tout* nombre premier p ; ceci dit, cette proposition a une plus forte chance d'être applicable). Mais il existe certaines transformations du polynôme ne changeant pas sa nature réductible ou non, qui peuvent rendre le critère applicable. Une première telle transformation est d'appliquer un isomorphisme de $\mathbf{Z}[X]$ donné par une substitution $X := X + a$ avec $a \in \mathbf{Z}$. Une autre est de renverser l'ordre des coefficients, grâce au fait suivant.

2.4.15. Proposition. *Soit R un anneau intègre, et $S = \{\, P \in R[X] : P[X := 0] \neq 0 \,\}$ l'ensemble des polynômes à terme constant non nul. Alors l'application $\rho : S \to S$, qui est définie par la relation $\rho(\sum_{i=0}^{n} c_i X^i) = \sum_{i=0}^{n} c_{n-i} X^i$ quand $c_n \neq 0$, est une involution multiplicative : $\rho(PQ) = \rho(P)\rho(Q)$.*

Preuve. C'est une conséquence directe de la formule $\sum_{i+j=k} p_i q_j$ pour le coefficient de X^k dans le produit PQ de deux polynômes $P = \sum_i p_i X^i$ et $Q = \sum_j q_j X^j$ (l'intégrité de R est nécessaire pour contrôler le degré de PQ par la proposition 1.4.2). Un argument un peu plus structurel peut être donné en utilisant l'anneau de polynômes de Laurent $R[X, X^{-1}]$, et le fait que des morphismes de substitution

existent aussi pour cet anneau, à condition que l'image de X soit inversible ; en particulier il existe un automorphisme θ de $R[X,X^{-1}]$ qui fixe les éléments de R et qui envoie $X \mapsto X^{-1}$. Il découle de la définition de ρ que $\rho(P) = X^{\deg_X(P)}\theta(P)$ pour tout $P \in S$, où on considère $R[X] \subseteq R[X,X^{-1}]$. Alors on a $\rho(PQ) = X^{\deg_X(PQ)}\theta(PQ) = X^{\deg_X(P)+\deg_X(Q)}\theta(P)\theta(Q) = X^{\deg_X(P)}\theta(P)X^{\deg_X(Q)}\theta(Q) = \rho(P)\rho(Q)$. □

La première méthode de transformation a une application proéminente dans le résultat suivant. En fait il s'agit de la toute première application du critère, donnée en 1846 par Theordor Schönemann qui avait formulé le critère ainsi : "un polynôme $(X-a)^n + pF$ est irréductible modulo p^2 si F modulo p n'est pas divisible par $X-a$"†, formulation qui prévoit déjà d'évaluer en a (avec $a=1$) plutôt qu'en 0.

2.4.16. Corollaire. *Soit p un nombre premier. Alors le polynôme $\sum_{i=0}^{p-1} X^i$ est irréductible dans $\mathbf{Z}[X]$.*

Preuve. Soit $P = X^{p-1} + X^{p-2} + \cdots + X + 1 = (X^p-1)/(X-1)$ ce polynôme. On a

$$P[X := X+1] = (X^p-1)[X := X+1]/(X-1)[X := X+1] = ((X+1)^p-1)/X = \sum_{i=1}^{p} \binom{p}{i} X^{i-1},$$

dont le terme dominant est $\binom{p}{p}X^{p-1} = X^{p-1}$, le terme constant est $\binom{p}{1}X^0 = p$, et les autres termes sont divisibles par p (voir la proposition 1.2.10). Le critère de Schönemann-Eisenstein pour p s'applique donc au polynôme $P[X := X+1]$, impliquant qu'il est irréductible dans $\mathbf{Z}[X]$, mais alors P l'est aussi. □

Ce résultat, qui avait été obtenu originalement par Gauss par des méthodes beaucoup plus compliquées, était tellement célèbre, que quand le jeune Gotthold Eisenstein formule son critère en 1850, quelques années après Schönemann, il l'applique lui aussi tout de suite au polynôme $X^{p-1} + \cdots + X + 1$, et cela pendant qu'il ignorait visiblement le résultat de Schönemann (il affirme ne connaître aucune autre preuve précédente, que celle de Gauss et une preuve de Kronecker de 1845 ; Schönemann se plaint ensuite de cette ignorance, à juste titre d'autant plus que Eisenstein fait référence à l'article de Schönemann pour d'autres raisons). Il formule en fait son critère non seulement pour les polynômes à coefficients entiers, mais aussi pour ceux à coefficients dans les entiers de Gauss, ainsi (un peu condensé) : "Quand un polynôme unitaire F dont les autres coefficients sont des entiers (réels ou complexes), tous divisibles par un nombre premier (réel respectivement complexe) p, et dont le coefficient constant n'est pas divisible par p^2, alors il est impossible d'écrire F comme produit de deux polynômes non constants à coefficients entiers (réels respectivement complexes)". Après une démonstration détaillée de ce résultat, il lâche malheureusement son attention en annonçant (sans preuve) une généralisation grossièrement fausse, affirmant qu'il suffirait en fait pour l'irréductibilité qu'un seul parmi les coefficients non dominants divisibles par p, pas forcément le dernier, ne soit pas divisible par p^2. Ceci montre qu'il n'a même pas pensé aux exemples pourtant pas difficiles à imaginer comme $X(X+p) = X^2 + pX$, ou $(X+p)^2 = X^2 + 2pX + p^2$ avec $p \neq 2$. Ce passage de la littérature* montre que même les plus grands mathématiciens ne sont pas à l'abri des gaffes énormes, en écrit.

Pour finir notre discussion de questions arithmétiques, nous tirerons une conclusion inattendue du lemme de Gauss 2.4.10. Si R est un anneau factoriel et $P \in R[X]$ est *unitaire*, alors P est certainement primitif (mais on évitera de croire la réciproque, une chose qui n'est que trop tentant pour ceux qui sont habitués à considérer des polynômes sur un corps). Alors, d'après ledit lemme, toute racine éventuelle de P dans $\mathrm{Frac}(R)$ est aussi racine d'un diviseur de P dans $R[X]$ de degré 1, mais celui-ci doit être (à un facteur dans $R^\times$ près) unitaire, c'est-à-dire de la forme $X-a$, dont $a \in R$ est visiblement la seule racine.

2.4.17. Corollaire. *Si R est un anneau factoriel et $P \in R[X]$ est unitaire, alors toute racine de P dans $\mathrm{Frac}(R)$ est déjà dans R.* □

Il s'avère que la condition d'être une racine d'un polynôme unitaire dans $R[X]$ est une propriété importante, et on appelle une telle valeur un *entier algébrique* sur R. On peut montrer que l'ensemble des entiers algébriques sur R est fermé pour les opérations '+' et '×', et l'ensemble de tels entiers algébriques dans un sur-anneau S forme donc toujours un sous-anneau de S (qui contient au moins R). Si on fait cela pour le corps $S = \mathrm{Frac}(R)$, le sous-anneau obtenu est appelé la *clôture intégrale* de R, et dans le cas

† La condition que F modulo p ne soit pas divisible par $X-a$ exige que la valeur $pF[X := a]$ ne soit pas divisible par p^2, ce qui correspond à notre condition pour le coefficient constant. On remarquera l'absence d'une condition sur le terme dominant, notamment on n'exige pas que $\deg_X(F) \leq n$; en effet, l'exemple $X^2 + p(X^3+1) \equiv (X^2+p)(pX+1) \pmod{p^2}$ montre que le critère comme on l'a cité est *faux*.

* Journal für die reine und angewandte Mathematik (dit "Crelle's Journal"), **39** (1850), p. 167.

où on retrouve l'anneau R, on dit que R est *intégralement clos*. Le corollaire se résume donc en disant qu'un anneau factoriel est nécessairement intégralement clos. On s'arrêtera ici à cette terminologie.

Mais considérons maintenant un polynôme unitaire bien connu, $P = X^2 - X - 1$, dont les racines dans $\mathbf{R}$ sont le nombre d'or $\frac{1+\sqrt{5}}{2}$, et $\frac{1-\sqrt{5}}{2}$. Ce ne sont bien sûr pas des nombres rationnels, donc il n'y a rien qui contredit le corollaire pour $R = \mathbf{Z}$, mais ces nombres sont visiblement dans le corps $\mathbf{Q}[\sqrt{5}] \cong \mathbf{Q}[X]/(X^2 - 5)$ sans être dans l'anneau $\mathbf{Z}[\sqrt{5}] \cong \mathbf{Z}[X]/(X^2 - 5)$ dont celui-là est le corps des fractions. Ce qui se passe bien évidemment est que $R = \mathbf{Z}[\sqrt{5}]$ n'est pas un anneau factoriel, comme on l'avait déjà constaté, donc le corollaire ne s'applique pas dans ce cas. En effet, P fournit un exemple d'un polynôme qui est primitif et irréductible sur R, mais qui est réductible sur $\mathrm{Frac}(R)$, mettant en évidence qu'on ne saura pas simplement se passer de l'hypothèse "R factoriel" dans le lemme de Gauss (même si on pourra éventuellement imaginer de la remplacer par une hypothèse plus faible sur R). Si on forme dans $R[X]$ le produit des polynômes primitifs, mais non unitaires, dont les racines sont respectivement $\frac{1+\sqrt{5}}{2}$ et $\frac{1-\sqrt{5}}{2}$, on trouve $(2X - 1 - \sqrt{5})(2X - 1 + \sqrt{5}) = 4X^2 - 4X - 4$. ce qui montre aussi un produit de polynômes primitifs qui n'est pas primitif (cf. 2.4.10(1)), ce qui est attribuable à la non-unicité de la factorisation dans R du coefficient constant -4.

Mais cet exemple n'est pas isolé : la formule pour les racines d'un polynôme quadratique unitaire, s'il contient un discriminant Δ qui n'est pas un carré, donne *toujours* des éléments $\frac{-b\pm\sqrt{\Delta}}{2}$ du corps $\mathbf{Q}[\sqrt{\Delta}]$, qui ne sont pas dans l'anneau $\mathbf{Z}[\sqrt{\Delta}]$ dont c'est le corps des fractions (si $\Delta < 0$, on lira $\sqrt{\Delta}$ comme $\sqrt{|\Delta|}\,\mathbf{i}$) : si on avait $\frac{-b+\sqrt{\Delta}}{2} = k + l\sqrt{\Delta}$ avec $k, l \in \mathbf{Z}$ alors $-b + \sqrt{\Delta} = 2k + 2l\sqrt{\Delta}$, ce qui est impossible. Avant de conclure trop hâtivement que $\mathbf{Z}[\sqrt{n}]$ ne peut jamais être factoriel, voyons ce qui se passe pour le polynôme $X^2 + 1$: son discriminant est -4, et ces racines $\frac{\pm\sqrt{-4}}{2} = \pm\mathbf{i}$ ne sont effectivement pas dans $\mathbf{Z}[\sqrt{-4}] = \mathbf{Z}[2\mathbf{i}]$, quel anneau n'est donc pas factoriel, mais cela n'empêche pas à $\mathbf{Z}[\mathbf{i}]$ d'être factoriel (comme on le sait être). On voit donc que -1 ne peut pas être lui-même le discriminant d'un polynôme quadratique unitaire dans $\mathbf{Z}[X]$, et la raison est simple : un tel discriminant $b^2 - 4c$ est forcément un carré modulo 4, c'est-à-dire 0 où 1, et ce n'est pas le cas de $-1 \equiv 3$. En général, si $d \equiv 2, 3 \pmod 4$, la racine $\sqrt{d}$ ne peut entrer dans l'expression d'une racine d'un polynôme quadratique unitaire dans $\mathbf{Z}[X]$ que sous la forme $\frac{\sqrt{4d}}{2}$, et en fait on peut vérifier que l'anneau $\mathbf{Z}[\sqrt{d}]$ est intégralement clos dans ce cas.

2.4.18. Conclusion. *Si $n \in \mathbf{Z}$ n'est pas un carré, alors $\mathbf{Z}[\sqrt{n}]$ n'est intégralement clos que si la classe de n modulo 4 est celle de 2 ou de 3. Dans le cas contraire l'anneau $\mathbf{Z}[\sqrt{n}]$ n'est pas factoriel non plus.*

Il ne faut surtout pas penser que quand $\mathbf{Z}[\sqrt{n}]$ est intégralement clos, il soit toujours factoriel (penser à $n = -5$), ni que dans le cas où $\mathbf{Z}[\sqrt{n}]$ n'est pas intégralement clos, sa clôture intégrale soit toujours factoriel ; c'est le cas pour $n = -3, -4, -7, -11, -19, +5, +13$, et bien d'autres valeurs, mais pas toujours, notamment pas pour $n = -15, -23, +65, +229, \ldots$ (l'exactitude de ces affirmations n'est pas du tout facile à vérifier, mais si les informations trouvées sur Internet sont fiables, le nombre 229 est bien le plus petit nombre *premier* (avec obligatoirement $n \equiv 1 \pmod 4$) dans cette seconde catégorie, ce qui est assez remarquable). On voit que l'étude algébrique des anneaux $\mathbf{Z}[\sqrt{n}]$ et leurs clôtures intégrales, aussi simple que soit leur définition, mène à des questions assez subtiles, qui relèvent de la théorie de nombres.

§3. Polynômes d'un endomorphisme, réduction de matrices d'un endomorphisme.

Dans cette dernière section on discutera quelques applications de la connaissance de la structure de l'anneau $K[X]$, où K est un corps commutatif, à l'étude d'un espace vectoriel E de dimension finie n sur K muni, d'un endomorphisme ϕ. Cela se fera notamment grâce à la notion d'un polynôme de l'endomorphisme ϕ. On ne refera pas toute la théorie des valeurs propres, de diagonalisation, et d'espaces caractéristiques, mais on commence avec un rappel des principaux définitions et résultats.

3.1. *Rappels sur les valeurs propres et sur la diagonalisation.*

Un vecteur *non nul* $v \in E$ est appelé vecteur propre pour ϕ si v et $\phi(v)$ sont linéairement dépendants. Cela veut dire qu'il existe $\lambda \in K$ tel que $\phi(v) = \lambda v$, ce qui s'exprime également comme $v \in \mathrm{Ker}(\phi - \lambda\,\mathrm{id}_E)$. Le scalaire λ est appelé valeur propre de ϕ pour le vecteur propre v, et v est appelé un vecteur propre de ϕ pour la valeur propre λ. Tous les $\lambda \in K$ qui sont valeur propre de ϕ pour au moins un vecteur non nul v sont appelés des valeurs propres de ϕ. La condition que λ soit valeur propre de ϕ est équivalente à $\mathrm{Ker}(\phi - \lambda\,\mathrm{id}_E) \neq \{0\}$. Une famille de vecteurs propres est libre dès que chaque sous-famille de vecteurs propres pour une *même* valeur propre est libre; en particulier un k-uplet de vecteurs propres chacun pour une valeur propre différente, est toujours linéairement indépendant (et on aura nécessairement $k \leq n$). La matrice de ϕ dans une base $\mathcal{B}$ de E est diagonale si et seulement si tous les vecteurs de $\mathcal{B}$ sont des vecteurs propres (pas nécessairement pour des valeurs propres différentes), et on appelle donc ϕ diagonalisable si E possède une base de valeurs propres. Dans ce cas ϕ ne peut pas avoir d'autres valeurs propres que les coefficients diagonaux de la matrice, et chaque valeur propre λ est répétée $\dim(\mathrm{Ker}(\phi - \lambda\,\mathrm{id}_E))$ fois comme coefficient diagonal ; par conséquence si ϕ est diagonalisable, sa forme diagonale est unique à permutation des coefficients diagonaux près.

Si $A \in \mathcal{M}_n(K)$ est la matrice de ϕ dans une base de E, on désigne par $XI_n - A$ la matrice dans $\mathcal{M}_n(K[X])$ dont la coefficient à la position i, j est $X - a_{i,i}$ si $i = j$ et $-a_{i,j}$ sinon. Le polynôme caractéristique χ_A est le déterminant de $XI_n - A$, calculé dans l'anneau $K[X]$; c'est un polynôme unitaire en X de degré n. Ce polynôme ne dépend pas de la base utilisée pour exprimer la matrice A, et s'appelle donc aussi le polynôme caractéristique χ_ϕ de ϕ. Pour tout $\lambda \in K$ on a $\chi_A[X := \lambda] = \det(\lambda I_n - A)$ (car le calcul du déterminant peut être fait de façon équivalente avant ou après la substitution de λ pour X), et le dernier déterminant est nul si et seulement si λ est une valeur propre de ϕ ; par conséquent les valeurs propres de ϕ sont précisément les racines de χ_A. Une condition nécessaire (mais pas suffisante) pour que ϕ soit diagonalisable est que χ_ϕ soit scindé dans $K[X]$, c'est-à-dire qu'il s'écrive comme produit de facteurs de la forme $X - a$ (avec $a \in K$): si $D = \mathrm{diag}(\lambda_1, \ldots, \lambda_n)$ est une matrice diagonale de ϕ (dans une base de vecteurs propres) alors $\chi_\phi = \chi_D = (X - \lambda_1) \ldots (X - \lambda_n)$. Une condition suffisante (mais pas nécessaire) pour la diagonalisabilité est que χ_ϕ soit scindé et à racines *simples* (c'est-à-dire les facteurs unitaires de degré 1 sont tous distincts), car dans ce cas tout n-uplet de vecteurs contenant un vecteur propre pour chacune des n valeurs propres forme une base de vecteurs propres.

Un sous-espace V de E est dit ϕ-stable si $\phi(V) \subseteq V$; c'est précisément dans ce cas que la restriction de ϕ à V définit un endomorphisme de V (il induit alors aussi un endomorphisme du quotient E/V). Les sous-espaces propres de ϕ, et leurs sommes, sont des sous-espaces ϕ-stables, mais ils ne sont pas les seuls. Si V est ϕ-stable de dimension d, et on choisit une base de E dont les d premiers vecteurs forment une base de V, alors la matrice de ϕ dans cette base aura un bloc $(n - d) \times d$ de coefficients nuls dans les lignes $> d$ et des colonnes $\leq d$. Le bloc $d \times d$ en haut à gauche décrit la restriction $\phi|_V$ de ϕ à V, et le bloc $(n-d) \times (n-d)$ en bas à droite l'endomorphisme $\phi_{/V}$ de E/V induit par ϕ ; on a $\chi_\phi = \chi_{\phi|_V} \cdot \chi_{\phi_{/V}}$.

Si χ_A n'est pas scindé sur K, il le sera néanmoins sur un corps plus grand. Pour $K = \mathbf{R}$ il suffit de considérer χ_A comme élément de $\mathbf{C}[X]$ où tous les polynômes (unitaires) sont scindés (car $\mathbf{C}$ est algébriquement clos). Plus généralement, tant que χ_A possède au moins un facteur irréductible P de degré plus grand que 1, on peut étendre K au corps $K[X]/(P)$, dans lequel χ_A possède au moins une racine de plus que dans K, et le répéter jusqu'à ce que χ_A soit scindé. Si ce changement de corps est satisfaisant ou non dépend du contexte : pour une matrice donnée il est facile de considérer ses coefficients comme s'ils était choisis dans un corps plus grand, mais un endomorphisme d'un espace vectoriel sur K ne s'interprète pas facilement comme correspondant *naturellement* à un endomorphisme d'un espace vectoriel sur un plus grand corps.

Mais si χ_A est scindé avec des racines multiples, il peut y avoir une obstruction à la diagonalisation qui ne se laisse pas résoudre ainsi. Si on considère le cas extrême où $\chi_A = (X-\lambda)^n$ (on verra qu'on peut toujours décomposer l'espace en somme directe d'un tel façon que sur chaque partie le polynôme caractéristique n'a qu'un seul facteur irréductible, avec éventuellement une multiplicité, donc ce cas est assez représentatif), alors A ne sera diagonalisable que dans l'*unique* cas $A = \lambda I_n$, pendant que *beaucoup* d'autres cas existent, par exemple toute matrice triangulaire avec coefficients diagonaux tous égaux à λ.

Si $\chi_A = (X-\lambda)^n$, alors $\phi - \lambda\,\mathrm{id}_E$ sera *nilpotent*. Pour le voir, constatons d'abord que le polynôme caractéristique de la transposée $\phi^\top$ sera $\chi_{A^\top} = (X-\lambda)^n$ aussi. Le fait que λ est valeur propre de $\phi^\top$ (en fait la seule) veut dire qu'il existe un forme linéaire non nulle $\nu \in E^*$ tel que $\nu \circ \phi = \lambda\nu$, ce qui implique $\mathrm{Ker}(\nu) \subseteq \mathrm{Ker}(\lambda\nu) = \mathrm{Ker}(\nu\circ\phi)$ et donc $\phi(\mathrm{Ker}(\nu)) \subseteq \phi(\mathrm{Ker}(\nu\circ\phi)) \subseteq \mathrm{Ker}(\nu)$: l'hyperplan vectoriel $H = \mathrm{Ker}(\nu)$ est ϕ-stable. On a $(X-\lambda)^n = \chi_\phi = \chi_{\phi|_H}\cdot\chi_{\phi_{/H}}$ donc $\chi_{\phi|_H} = (X-\lambda)^{n-1}$ et $\chi_{\phi_{/H}} = X-\lambda$; comme $(\phi-\lambda\,\mathrm{id}_E)_{/H} = 0$ on a $\mathrm{Im}(\phi-\lambda\,\mathrm{id}_E)\subseteq H$, et par récurrence $(\phi-\lambda\,\mathrm{id}_E)|_H$ est nilpotent, donc $\phi-\lambda\,\mathrm{id}_E$ est nilpotent. (Par le même raisonnement on montre plus généralement que si χ_ϕ est scindé sur K, alors ϕ est *trigonalisable* : il a une matrice triangulaire supérieur dans une certaine base ; on peut obtenir ce résultat aussi sans utiliser la transposée ni des formes linéaires, en choisissant un sous-espace supplémentaire à un espace propre.) Donc même si dans ce cas l'espace propre $\mathrm{Ker}(\phi-\lambda\,\mathrm{id}_E)$ n'est pas souvent E tout entier, on a toujours $E = \mathrm{Ker}((\phi-\lambda\,\mathrm{id}_E)^n)$. Cela motive la définition suivante.

Si λ est une valeur propre de ϕ, avec multiplicité m comme racine de χ_ϕ, alors on définit l'espace caractéristique pour λ de ϕ comme $E_\lambda = \mathrm{Ker}((\phi-\lambda\,\mathrm{id}_E)^m)$. C'est un sous-espace ϕ-stable tel que λ est l'unique valeur propre de la restriction $\phi|_{E_\lambda}$, et λ *n'est pas* valeur propre de $\phi_{/E_\lambda}$. On a donc $\chi_{\phi|_{E_\lambda}} = (X-\lambda)^m$, et en particulier $\dim(E_\lambda) = m$. Les espaces caractéristiques pour des valeurs propres distinctes sont en somme directe, comme on le montre ainsi. Pour $\mu\neq\lambda$, la restriction à E_λ de $\phi-\mu\,\mathrm{id}_E$ est inversible : dans le cas contraire son noyau contiendrait un vecteur propre $v\in E_\lambda$ pour μ, pour lequel on aurait $(\phi-\lambda\,\mathrm{id}_E)^m(v) = (\mu-\lambda)^m v \neq 0$, en contradiction avec la définition de E_λ. Si l'un des vecteurs non nuls v d'un espace caractéristique E_μ s'exprimait comme combinaison linéaire de vecteurs non nuls d'autres espaces caractéristiques $E_{\lambda_1},\ldots,E_{\lambda_k}$, qu'on peut supposer en somme directe par récurrence, alors en appliquant $(\phi-\mu\,\mathrm{id}_E)^m$ (avec $m=\dim(E_\mu)$) à cette expression pour v, on voit d'un côté que v est annulé, et d'autre côté que les vecteurs dans les espaces E_{λ_i} sont transformés en d'autres vecteurs *non nuls* des mêmes espace, obtenant une relation de dépendance linéaire qui contredit l'hypothèse de la somme directe des E_{λ_i} ; en conclusion, la somme reste directe en rajoutant E_μ. Par conséquent, si on a une décomposition $\chi_\phi = \prod_{i=1}^d (X-\lambda_i)^{m_i}$ où on prend les λ_i *distincts*, alors on a $E = \bigoplus_{i=1}^d E_{\lambda_i}$.

3.2. *Polynômes d'un endomorphisme d'un espace vectoriel, le polynôme minimal.*

La pertinence de la théorie de l'anneau $K[X]$ dans l'étude des endomorphismes d'un espace vectoriel de dimension finie, mise à part son caractère factoriel qui est utilisé implicitement en considérant la décomposition du polynôme caractéristique, est surtout contenue dans la notion d'un polynôme d'un endomorphisme, c'est-à-dire le résultat de substituer un endomorphisme ϕ pour X dans un polynôme. Contrairement à l'indéterminée X, les puissances de ϕ sont définies par *composition*, une opération qui n'est pas commutative en général, et la substitution n'est donc pas anodine. Mais en considérant les différents polynômes d'un même endomorphisme, on obtient une partie *commutative* de l'anneau non commutatif des endomorphismes, une situation qui mérite une formulation précise.

3.2.1. Proposition. *Soit ϕ un endomorphisme d'un espace vectoriel E de dimension finie n sur un corps commutatif K. Alors il existe un morphisme d'anneaux $f_\phi : K[X] \to \mathrm{End}(E)$ non injectif défini par $f_\phi(\sum_{i=0}^d c_i X^i) = \sum_{i=0}^d c_i\phi^i$ (où comme d'habitude $\phi^0 = \mathrm{id}_E$). L'image $f_\phi(K[X])$ est un sous-anneau commutatif $K[\phi]$ de $\mathrm{End}(E)$ dont les éléments s'appellent des polynômes de l'endomorphisme ϕ.*

Preuve. C'est une application directe du théorème 1.5.1, avec $f : K\to\mathrm{End}(E)$ le morphisme $\lambda\mapsto\lambda\,\mathrm{id}_E$ qui associe à un scalaire l'homothétie correspondante, et $s=\phi$ qui commute avec toutes ces homothéties. Le caractère non injectif de f_ϕ découle de $\dim_K(\mathrm{End}(E)) = n^2 < \infty$ pendant que $\dim_K(K[X]) = \infty$ (car f_ϕ est certainement K-linéaire). La commutativité de $K[\phi]$ résulte de $f_\phi(K[X]) \cong K[X]/\mathrm{Ker}(f_\phi)$. □

Le nom f_ϕ est de circonstance ; c'est essentiellement un morphisme de substitution, et on écrira $P[X:=\phi]$ pour $f_\phi(P)$ (dans la littérature on trouvera le plus souvent $P(\phi)$), mais on fera attention que

$c[X := \phi] = c\,\mathrm{id}_E$ pour une constante $c \in K$: la "substitution" transforme les scalaires en homothéties. Le fait que f_ϕ est un morphisme d'anneaux s'exprime par les relations

$$(P+Q)[X := \phi] = P[X := \phi] + Q[X := \phi] \qquad \text{et} \qquad (PQ)[X := \phi] = P[X := \phi] \circ Q[X := \phi]. \tag{7}$$

Quand on fait agir ces endomorphismes sur des vecteurs, la notation devient assez lourde : $P[X := \phi](v)$ (la notation traditionnelle $P(\phi)(v)$ est plus courte mais moins lisible, car il s'agit de deux types différents de "application"). Des trois acteurs P, ϕ, v dans cette expression, ϕ est le moins variable, en on propose donc une notation qui le met moins en évidence : on écrira $P \cdot_\phi v$ pour $P[X := \phi](v)$ (le polynôme P agit sur le vecteur v "selon" l'endomorphisme ϕ). Ainsi la règle de base pour la composition devient

$$(PQ) \cdot_\phi v = P \cdot_\phi (Q \cdot_\phi v), \tag{8}$$

et on adoptera de règles de priorité qui permettent de l'écrire sans parenthèses $PQ \cdot_\phi v = P \cdot_\phi Q \cdot_\phi v$.

3.2.2. Définition. *Le polynôme minimal μ_ϕ de $\phi \in \mathrm{End}(E)$ est le générateur unitaire de l'idéal $\mathrm{Ker}(f_\phi)$ de $K[X]$ dans la proposition précédente.*

Comme f_ϕ n'est pas injectif, $\mathrm{Ker}(f_\phi)$ n'est pas l'idéal nul de $K[X]$, et possède donc bien un générateur unitaire, nécessairement unique. Par définition $P[X := \phi] = 0 \in \mathrm{End}(E)$ si et seulement si $\mu_\phi \mid P$ dans $K[X]$, et $P[X := \phi] = 0$ veut dire que $P \cdot_\phi v = 0$ pour tout $v \in E$. Si $P \cdot_\phi v = 0$ on dira que le polynôme P annule le vecteur v (pour ϕ), et si $P[X := \phi] = 0$ on dira que le polynôme P annule ϕ.

Si $\mu_\phi = c_0 + c_1 X + \cdots + c_{d-1}X^{d-1} + X^d$ alors $\phi^d = -c_0\phi^0 - c_1\phi - \cdots - c_{d-1}\phi^{d-1}$, et par minimalité les endomorphismes $\phi^0 = \mathrm{id}_e, \phi, \ldots, \phi^{d-1}$ sont linéairement indépendants dans le K-espace vectoriel $\mathrm{End}(E)$. Cela reste valable avec à la place de ϕ la matrice A de ϕ dans une base choisie de E, ce qui donne une manière effective (mais un peu fastidieuse) de calculer μ_ϕ : on calcule les puissances successives de A à commencer par $A^0 = I_n$, on vérifie pour chacune si elle est linéairement indépendante des puissances précédentes, et dès qu'on trouve une relation de dépendance, cela donne le polynôme minimal de ϕ.

Si on fixe un vecteur v, on vérifie facilement que les polynômes P qui annulent v pour ϕ forment un idéal de $K[X]$, et cet idéal contient toujours μ_ϕ. On appellera polynôme minimal de (ϕ, v), noté $\mu_{\phi,v}$, le générateur unitaire de cet idéal ; c'est un diviseur de μ_ϕ (qui assez souvent est égal à μ_ϕ). On aimerait voir cet idéal comme le noyau d'un morphisme d'anneaux. Pour le faire, on fait d'abord le constat suivant.

3.2.3. Lemme. *Si P annule v pour ϕ, il annule aussi $Q \cdot_\phi v$ pour ϕ, pour tout $Q \in K[X]$.*

Preuve. On a $P \cdot_\phi v = 0$, donc $P \cdot_\phi (Q \cdot_\phi v) = PQ \cdot_\phi v = QP \cdot_\phi v = Q \cdot_\phi (P \cdot_\phi v) = Q \cdot_\phi 0 = 0$. □

Définissons donc $E_v \subseteq E$ par $E_v = K[\phi] \cdot v = \{\, Q \cdot_\phi v : Q \in K[X] \,\}$; c'est un sous-espace ϕ-stable (par construction), et tel que $P[X := \phi|_{E_v}] = 0 \in \mathrm{End}(E_v)$ dès que $P \cdot_\phi v = 0$ (c'est ce que dit le lemme). (On appelle E_v le $K[X]$-module cyclique engendré par v pour ϕ ; il est analogue au sous-groupe cyclique engendré par un élément d'un group abélien.) Autrement dit, l'idéal des polynômes qui annulent v pour ϕ est le noyau du morphisme $K[X] \to \mathrm{End}(E_v)$ défini par $P \mapsto P[X := \phi|_{E_v}]$. Trouver son générateur unitaire, le polynôme minimal $\mu_{\phi,v}$ de (ϕ, v), est analogue à trouver μ_ϕ, mais plus simple : on calcule les vecteurs $X^i \cdot_\phi v = \phi^i(v)$ pour les puissances successives à partir de $i = 0$, et on vérifie pour chacun s'il est linéairement indépendant des vecteurs précédents; dès qu'on trouve une relation de dépendance, cela donne le polynôme $\mu_{\phi,v}$ cherché. La famille $\big(v, \phi(v), \ldots, \phi^{d-1}(v)\big)$ avec $d = \deg_X(\mu_{\phi,v})$ forme une base de E_v (la famille est libre d'après les vérifications d'indépendance linéaires effectuées, et l'espace qu'elle engendre ϕ-stable car il contient $\phi^d(v)$, donc c'est E_v). On remarque, pour utilisation ultérieure, que ceci montre

$$\dim_K(K[\phi] \cdot v) = \deg_X(\mu_{\phi,v}) \qquad \text{pour tout vecteur } v \in E \text{ et tout } \phi \in \mathrm{End}(E). \tag{9}$$

Ce calcul est une étape dans la méthode la plus pratique de calculer μ_ϕ : on sait que $\mu_{\phi,v}$ est diviseur de μ_ϕ, et qu'il annule E_v. Si $d = \dim(E)$ (ce qui arrive souvent si on commence avec un vecteur v au hasard) on aura trouvé $\mu_\phi = \mu_{\phi,v}$, et dans le cas contraire il suffit de recommencer avec un vecteur $w \notin E_v$ et de prendre $\mathrm{ppcm}(\mu_{\phi,v}, \mu_{\phi,w})$, puis si toujours $E_v + E_w \neq E$ de prendre $x \notin E_v + E_w$, et ainsi

de suite. On peut prendre ces vecteurs parmi une base de E choisie d'avance, ce qui revient a tester l'indépendance linéaire des puissances de la matrice A de ϕ dans cette base à l'aide de *certaines* de ses colonnes (dans le pire des cas il faut utiliser tous les vecteurs de la base, c'est-à-dire tester l'indépendance pour toutes les colonnes, mais cela n'arrive qui si la base choisie est une base de vecteurs propres, et donc A une matrice diagonale ; du coup ce "pire des cas" est un cas très simple !).

3.2.4. Théorème. *Les valeurs propres de ϕ sont précisément les racines du polynôme minimal μ_ϕ.*

Preuve. Pour un vecteur propre v de ϕ avec valeur propre λ on a $P \cdot_\phi v = P[X := \lambda]v$ pour tout $P \in K[X]$. En particulier on a $\mu_\phi[X := \lambda]v = \mu_\phi \cdot_\phi v = 0$, et comme $v \neq 0$ on conclut que λ est racine de μ_ϕ. Réciproquement si $\dim(E) > 0$ (de sorte que $\mu_\phi \neq 0$) et λ est racine de μ_ϕ, on peut décomposer $\mu_\phi = (X - \lambda)Q$ dans $K[X]$, et on a $0 = \mu_\phi[X := \phi] = (\phi - \lambda \mathrm{id}_E) \circ Q[X := \phi]$ dans $\mathrm{End}(E)$. Clairement Q n'est pas divisible par μ_ϕ, donc $Q[X := \phi] \neq 0 \in \mathrm{End}(0)$. Il existe alors un vecteur non nul w dans $\mathrm{Im}(Q[X := \phi])$, disons $w = Q \cdot_\phi v$, pour lequel on trouve $0 = (X - \lambda \mathrm{id}_E) \cdot_\phi Q \cdot_\phi v = (X - \lambda \mathrm{id}_E) \cdot_\phi w = \phi(w) - \lambda w$, donc w est un vecteur propre pour λ. □

On a déjà vu dans la preuve du lemme 3.2.3 l'importance de la commutativité de $K[\phi]$. Cette commutativité servira régulièrement dans la site, entre autres pour appliquer le résultat général suivant.

3.2.5. Proposition. *Si $\phi, \psi \in \mathrm{End}(E)$ commutent, alors $\mathrm{Ker}(\psi)$ et $\mathrm{Im}(\psi)$ sont ϕ-stables.*

Preuve. Pour $v \in \mathrm{Ker}(\psi)$ on a $\psi(\phi(v)) = \phi(\psi(v)) = \phi(0) = 0$ donc $\phi(v) \in \mathrm{Ker}(\psi)$, qui est donc ϕ-stable. Pour $v \in \mathrm{Im}(\psi)$, disons $v = \psi(w)$, on a $\phi(v) = \phi(\psi(w)) = \psi(\phi(v)) \in \mathrm{Im}(\psi)$, et $\mathrm{Im}(\psi)$ est ϕ-stable. □

Pour compléter notre compréhension du polynôme minimal, étudions le lien entre sa décomposition en facteurs et l'espace E. Contrairement au polynôme caractéristique, μ_ϕ ne se "gonfle" pas automatiquement avec la dimension de E ; par exemple le polynôme minimale d'une homothétie $\lambda \mathrm{id}_E$ est toujours $X - \lambda$, quelle que soit la dimension de E. Le lemme suivant interprète une décomposition de μ_ϕ.

3.2.6. Lemme. *Soit $\mu_\phi = PQ$ une décomposition du polynôme minimal dans $K[X]$. Alors la restriction de ϕ au sous-espace ϕ-stable $E' = \mathrm{Im}(P[X := \phi])$ de E a pour polynôme minimal $\mu_{\phi|_{E'}} = Q$.*

Preuve. La ϕ-stabilité de E' découle de la proposition précédente et la commutativité de $K[\phi]$. Soit $w \in E'$ un élément quelconque, qui s'écrit donc $w = P \cdot_\phi v$; alors $Q \cdot_\phi w = Q \cdot_\phi P \cdot_\phi v = \mu_\phi \cdot_\phi v = 0$. Donc $Q[X := \phi|_{E'}]$ est l'endomorphisme nul de E'. Or si on avait $Q'[X := \phi|_{E'}] = 0$ pour un polynôme non nul Q' avec $\deg_X(Q') < \deg_X(Q)$, on aurait $Q'P[X := \phi] = Q'[X := \phi|_{E'}] \circ P[X := \phi] = 0$ pendant que $\deg_X(Q'P) < \deg_X(\mu_\phi)$, contredisant la minimalité de μ_ϕ ; par conséquent Q est le polynôme non nul de degré minimal qui annule $\phi|_{E'}$, c'est-à-dire il est son polynôme minimal. □

On peut maintenant donner un complément au théorème 3.2.4 qui décrit précisément la multiplicité des racines de μ_ϕ. En fait on décrira en même temps ce qu'il se passe pour des facteurs irréductibles de μ_ϕ, qu'ils soient de la forme $X - \lambda$ ou non. On remarque d'abord que pour tout endomorphisme ψ on a l'inclusion $\mathrm{Ker}(\psi^m) \supseteq \mathrm{Ker}(\psi^{m-1})$; la proposition suivante s'occupe de la question si elle est stricte.

3.2.7. Proposition. *Soit $\phi \in \mathrm{End}(E)$, $P \in K[X]$ irréductible ; on pose $\psi = P[X := \phi]$. Alors pour un entier $m > 0$, le polynôme P^m divise μ_ϕ si et seulement si $\mathrm{Ker}(\psi^m) \neq \mathrm{Ker}(\psi^{m-1})$.*

Preuve. Par récurrence sur m. Le cas $m = 1$ est le théorème 3.2.4 si $P = X - \lambda$; pour P général la démonstration et pareille : si $\mu_\phi = PQ$ alors $\mathrm{Im}(Q[X := \phi])$ est un sous-espace non nul annulé par ϕ, donc $\mathrm{Ker}(\psi) \neq \{0\} = \mathrm{Ker}(\psi^0)$, et réciproquement si $v \in \mathrm{Ker}(\psi)$ est non nul, alors $\mu_{\phi,v}$ est un diviseur unitaire non trivial de P, donc associé à P, et il divise μ_ϕ. Supposons ensuite $m > 1$, et posons $E' = \mathrm{Im}\,\psi$. On supposera que P divise μ_ϕ, car sinon ψ serait inversible (comme on vient de voir) et donc tout ψ^i aussi, et les deux conditions seraient fausses ; le lemme 3.2.6 affirme donc $\mu_\phi = P \times \mu_{\phi|_{E'}}$. S'il existe un vecteur $v \in \mathrm{Ker}(\psi^m) \setminus \mathrm{Ker}(\psi^{m-1})$, alors $\psi(v)$ appartient à E' et à $\mathrm{Ker}(\psi^{m-1}) \setminus \mathrm{Ker}(\psi^{m-2})$, et on a donc $\mathrm{Ker}((\psi|_{E'})^{m-1}) \neq \mathrm{Ker}((\psi|_{E'})^{m-2})$. Par hypothèse de récurrence P^{m-1} divise donc $\mu_{\phi|_{E'}}$, et P^m divise μ_ϕ. Réciproquement si P^m divise μ_ϕ, alors P^{m-1} divise $\mu_{\phi|_{E'}}$, et donc l'hypothèse de récurrence donne l'existence d'un vecteur $w \in \mathrm{Ker}((\psi|_{E'})^{m-1}) \setminus \mathrm{Ker}((\psi|_{E'})^{m-2})$; en particulier $w \in E'$ donc il existe $v \in E$ avec $\psi(v) = w$, et il est immédiat que $v \in \mathrm{Ker}(\psi^m) \setminus \mathrm{Ker}(\psi^{m-1})$. □

La multiplicité m d'une valeur propre λ comme racine de μ_ϕ est donc en particulier égale au plus petit exposant tel que $\mathrm{Ker}((\phi-\lambda\,\mathrm{id}_E)^m) = \mathrm{Ker}((\phi-\lambda\,\mathrm{id}_E)^{m+1})$. On aura aussi $\mathrm{Ker}((\phi-\lambda\,\mathrm{id}_E)^m) = \mathrm{Ker}((\phi-\lambda\,\mathrm{id}_E)^k)$ pour tout $k > m$, car si on avait $v \in \mathrm{Ker}((\phi-\lambda\,\mathrm{id}_E)^k \setminus \mathrm{Ker}((\phi-\lambda\,\mathrm{id}_E)^{k-1}$, on aurait $\phi^{k-1-m}(v) \in \mathrm{Ker}((\phi-\lambda\,\mathrm{id}_E)^{m+1} \setminus \mathrm{Ker}((\phi-\lambda\,\mathrm{id}_E)^m$, ce qui est impossible.

3.2.8. Corollaire. *$E_\lambda = \mathrm{Ker}((\phi-\lambda\,\mathrm{id}_E)^m)$ où m est la multiplicité de la racine λ de μ_ϕ, et $\dim(E_\lambda) \geq m$.*

Preuve. On avait déjà mentionné que λ n'est pas valeur propre de $\phi_{/E_\lambda}$, donc si $d = \dim(E_\lambda)$, de sorte que par définition $E_\lambda = \mathrm{Ker}((\phi-\lambda\,\mathrm{id}_E)^d)$, on a aussi $E_\lambda = \mathrm{Ker}((\phi-\lambda\,\mathrm{id}_E)^{d+1})$ (un vecteur que qui serait dans le second membre sans être dans le premier donnerait un vecteur propre pour λ de $\phi_{/E_\lambda}$). □

3.2.9. Théorème de Cayley-Hamilton. *Soit $\phi \in \mathrm{End}(E)$ où E est un K-espace vectoriel de dimension finie. Le polynôme minimal μ_ϕ divise le polynôme caractéristique χ_ϕ, donc $\chi_\phi[X := \phi] = 0 \in \mathrm{End}(E)$.*

Preuve. Si μ_λ est scindé dans $K[X]$, c'est le corollaire, qui dit que la multiplicité d'une racine dans μ_ϕ n'excède pas sa multiplicité dans χ_ϕ. Pour réduire à ce cas, il suffit de montrer qu'on peut rendre μ_ϕ scindé par une extension convenable du corps K ; cela ne change pas le sens de la conclusion si elle est mise sous la forme $\chi_\phi[X := A] = 0 \in \mathrm{Mat}_n(K)$, où A est la matrice de ϕ sur une base quelconque. Or on a vu qu'on peut agrandir le nombre de racines d'un polynôme par une extension de K qui rajoute une racine à l'un de ces facteurs irréductibles, tant qu'il y en a de degré > 1 ; on se ramène ainsi au cas où μ_ϕ est scindé. □

L'extension du corps ne change pas non plus le sens de la conclusion du théorème sous la forme $\mu_\phi \mid \chi_\phi$, mais cela est un peu moins facile : elle ne change pas le polynôme μ_ϕ car celui-ci est déterminé par des relations de dépendance linéaire entre les puissances de A, qui sont insensible à l'extension du corps ; elle ne change pas non plus la divisibilité $\mu_\phi \mid \chi_\phi$, car cela veut dire que le reste d'une division euclidienne est nul, et grâce à son unicité, ce reste ne peut pas changer en étendant le corps de base.

Le théorème de Cayley-Hamilton peut également être démontré par d'autres moyens, notamment sous la forme $\chi_A[X := A] = 0 \in \mathrm{Mat}_n(R)$ qui a un sens, et reste vrai, pour une matrice carré A à coefficients dans un anneau commutatif R quelconque ; on y reviendra.

3.3. *Théorème de décomposition des noyaux.*

Les considérations sur le polynôme minimal peuvent être complétées par un résultat très général sur la décomposition de l'espace qui peut être effectuée de façon canonique selon une décomposition du polynôme minimal, lorsque cette dernière est en facteurs qui sont premiers entre eux deux à deux.

3.3.1. Théorème de décomposition des noyaux. *Soit $P = P_1 \cdots P_l$ une décomposition de $P \in K[X]$ tels que les facteurs P_i sont premiers entre eux deux à deux, et ϕ un endomorphisme d'un K-espace vectoriel (non nécessairement de dimension finie). Alors le sous-espace $V = \mathrm{Ker}(P[X := \phi])$ de E est la somme directe des sous-espaces $V_i = \mathrm{Ker}(P_i[X := \phi])$ pour $i = 1, \ldots, l$.*

Preuve. Le résultat est trivial pour $l = 0, 1$, et les autres cas peuvent être obtenus par récurrence sur l dès qu'on établit le cas $l = 2$, car chaque P_i sera premier avec un produit des *autres* facteurs P_j ; on supposera donc désormais $l = 2$. Comme $K[X]$ est un anneau principal, il existe $Q_1, Q_2 \in K[X]$ tels que $P_1Q_1 + P_2Q_2 = 1$. Les espaces V, V_1, V_2 sont ϕ-stables d'après la proposition 3.2.5, et V contient les deux autres car $P_i \cdot_\phi v = 0$ implique $P \cdot_\phi v = 0$. On définit $\psi_1, \psi_2 \in \mathrm{End}(V)$ par $\psi_i = P_iQ_i[X := \phi|_V]$ pour $i = 1, 2$, de sorte que $\psi_1 + \psi_2 = \mathrm{id}_V$. On a $\mathrm{Im}(\psi_1) \subseteq V_2$ car pour $v \in V$ on a $P_2 \cdot_\phi \psi_1(v) = P_2P_1Q_1 \cdot_\phi v = Q_1 \cdot_\phi (P \cdot_\phi v) = Q_1 \cdot_\phi (0) = 0$ (cet argument dépend du fait que la substitution définissant ψ_1 utilise la restriction $\phi|_V$ de ϕ), et on a $\mathrm{Ker}(\psi_1) \supseteq V_1$ car pour $v_1 \in V_1 \subseteq V$ on a $\psi_1(v_1) = Q_1P_1 \cdot_\phi v_1 = Q_1 \cdot_\phi (0) = 0$. De façon similaire on a $\mathrm{Im}(\psi_2) \subseteq V_1$ et $\mathrm{Ker}(\psi_2) \supseteq V_2$. Maintenant pour prouver que $V_1 + V_2 \supseteq V$, il suffit d'appliquer $\psi_1 + \psi_2 = \mathrm{id}_V$ à $v \in V$ pour obtenir $v = \psi_1(v) + \psi_2(v) \in V_2 + V_1$; l'inclusion $V_1 + V_2 \subseteq V$ étant évident on a $V_1 + V_2 = V$. Pour obtenir que cette somme est directe, on procède de la même façon pour $x \in V_1 \cap V_2$, donnant $x = \psi_1(x) + \psi_2(x) = 0$ car $x \in \mathrm{Ker}(\psi_1) \cap \mathrm{Ker}(\psi_2)$. □

On remarque que $\psi_2 : V \to V_1$ et $\psi_1 : V \to V_2$ sont les projections selon la somme directe $V = V_1 \oplus V_2$, car ψ_i s'annule sur V_i, et leur somme étant l'identité, il fixe les vecteurs de l'autre facteur. Le fait que

ces projections sont réalisées par des éléments de $K[\phi]$ est important dans la mesure où cela implique que tout sous-espace ϕ-stable de V contient ses propres projections sur V_1 et sur V_2, ce qui n'est pas vrai en général pour une somme directe de sous-espaces ϕ-stables.

Ce théorème donne la décomposition *canonique* de E en somme directe de sous-espaces ϕ-stables suivante : si $\mu_\phi = \prod_{i=1}^{l} P_i^{m_i}$ où les $P_i \in K[X]$ sont irréductibles et non associés deux à deux, alors

$$E = \bigoplus_{i=1}^{l} \mathrm{Ker}(P_i^{m_i}[X := \phi]).$$

Dans le cas où μ_ϕ est scindé, et χ_ϕ donc aussi, on peut prendre les P_i de la forme $X - \lambda_i$, et on retrouve la décomposition en sous-espaces caractéristiques, avec l'exposant de chaque P_i choisi minimal pour obtenir ce sous-espace tout entier. Si μ_ϕ n'est pas scindé, la décomposition comprend aussi des facteurs sans vecteurs propres. La qualification "canonique" dans cette décomposition signifie qu'elle ne dépend d'autre chose que de l'endomorphisme ϕ, et en se servant de cette décomposition on ne perdra rien de la symétrie éventuelle de la situation. Des décompositions plus fines en sous-espaces ϕ-stables sont souvent possibles (par exemple, si l'un des facteurs est un espace propre de dimension > 1, on pourra la décomposer en somme d'espaces de dimension 1), mais elles dépendront de certains choix, et par conséquent plusieurs décompositions plus ou moins équivalentes seront possibles dans ces cas.

En fait si l'on considère les facteurs $\mathrm{Ker}(P_i^{m_i}[X := \phi])$ de cette décomposition, on peut distinguer dedans encore deux types particuliers de sous-espaces ϕ-stables. On a les sous-espaces intermédiaires $\mathrm{Ker}(P_i^{j}[X := \phi])$ pour $0 < j < m_i$ dont on s'est servi dans la proposition 3.2.7, et qui sont canoniques, mais qui ne sont pas en somme directe (et ne figurent dans *aucune* décomposition en somme directe de sous-espaces ϕ-stables). D'un autre côté on a les sous-modules cycliques $E_v = K[\phi] \cdot v$ engendrés par un vecteur particulier v ; ils ne sont pas canoniques, mais certains de tels modules peuvent figurer dans une décomposition en somme directe de sous-espaces ϕ-stables. On verra que E peut toujours être décomposé comme somme directe de sous-modules cycliques, ce qui est un résultat théorique important, parce qu'il permet une classification des espaces munis d'un endomorphisme. Mais dans la pratique il est aussi important de pouvoir reconnaître la structure d'un tel espace sans avoir recours à une telle décomposition, et c'est les dimensions des sous-espaces $\mathrm{Ker}(P_i^{j}[X := \phi])$ qui permettront cela.

On remarquera la ressemblance du théorème de décomposition des noyaux au théorème chinois, dans ses hypothèses et dans la forme de sa conclusion. En fait, on peut établir un rapport direct entre les deux, mais cela nécessite la notion d'un module sur un anneau commutatif (analogue à un espace vectoriel sur un corps) qu'on n'a pas abordé dans ce cours, et la considération d'un tel module un peu particulier. Le théorème chinois se formule et est valable pour tout anneau principal à la place de $\mathbf{Z}$, et sa version pour $K[X]$ affirme que pour $P_1, \ldots, P_l \in K[X]$ premiers entre eux deux à deux on a $K[X]/(P_1 \cdots P_l) \cong K[X]/(P_1) \times \cdots \times K[X]/(P_l)$. Pour le voir comme un cas particulier du théorème de décomposition des noyaux, il faut considérer le quotient $T = K(X)/K[X]$ des fractions rationnelles en X par les polynômes en X, une structure qui *n'est pas un anneau*, mais qui est un K-espace vectoriel dans lequel la multiplication par des polynômes est bien définie (contrairement à la division), autrement dit c'est un $K[X]$-module. Pour comprendre ses propriétés, on peut le comparer au groupe abélien $\mathbf{Q}/\mathbf{Z}$ des "nombres rationnels modulo 1", dans lequel tout élément est de torsion (son multiple par un certain $n \in \mathbf{Z}$ est nul), et tout $n \in \mathbf{Z}$ annule (par multiplication) précisément un sous-groupe cyclique d'ordre n. Dans T on prend l'endomorphisme ϕ de multiplication par X, alors pour tout $Q \in K[X]$ l'endomorphisme $Q[X := \phi]$ de T est celui de multiplication par Q, et le sous-espace $\mathrm{Ker}(Q[X := \phi])$ de T est égal à l'ensemble d'éléments représentés par des fraction rationnelles de la forme $\frac{P}{Q}$ avec $P \in K[X]$; comme seulement le reste de P après division par Q importe pour l'élément représenté par $\frac{P}{Q}$, on a $\mathrm{Ker}(Q[X := \phi]) \cong K[X]/(Q)$. Alors le théorème de décomposition des noyaux appliqué à T muni de ϕ donne la conclusion $K[X]/(P_1 \cdots P_l) \cong \prod_{i=1}^{l} K[X]/(P_i)$ du théorème chinois pour $K[X]$, mais sous la forme d'un isomorphisme de $K[X]$-modules plutôt que des anneaux (comme les $K[X]$-modules sont des quotients de $K[X]$, ils en héritent une structure d'anneau), et ce qui est nouveau, avec l'isomorphisme réalisé comme une somme directe *interne* de sous-modules du $K[X]$-module T.

3.4. *Décomposition en sous-modules cycliques, forme normale de Jordan.*

Pour comprendre la structure d'un K-espace E de dimension finie muni d'un endomorphisme ϕ, il nous reste à analyser le cas où le polynôme minimal est une puissance P^m d'un polynôme irréductible P. Malgré la simplification qu'apporte la décomposition des noyaux, ce cas reste assez compliqué dans sa classification, même si le nombre de cas non isomorphes est fini. Notre outil de base est une décomposition non canonique en somme directe de module cycliques. On a vu dans la proposition 3.2.7 qu'il existe un vecteur v qui n'est pas annulé par P^{m-1}, donc tel que $\mu_{\phi,v} = P^m$, et ce vecteur engendre donc un module cyclique E_v dont le polynôme minimal (de la restriction de ϕ) est le même que celui de l'espace E tout entier. Mais ce module n'est pas forcément égal à E, ce qui permet le polynôme caractéristique d'être que puissance plus élevée de P que P^m. Autrement dit, en ce qui concerne le polynôme minimal un module cyclique peut en cacher un autre (ou plusieurs), dont le polynôme minimal divise celui du premier.

Pour avancer par récurrence sur la dimension, il est nécessaire de prouver que E_v est un facteur direct dans une décomposition ϕ-stable, c'est-à-dire qu'il possède un espace supplémentaire dans E et aussi ϕ-stable (sinon on ne saura pas considérer la restriction à celui-ci). Comme on l'a fait pour la trigonalisation, nous utiliserons l'endomorphisme transposé de ϕ dans l'espace dual E^*.

3.4.1. Lemme. *Soit $\phi \in \mathrm{End}(E)$ tel que $\mu_\phi = P^m$ avec $P \in K[X]$ irréductible et $m > 0$, et $v \in E$ tel que $P^{m-1} \cdot_\phi v \neq 0$. Alors il existe un sous-espace ϕ-stable E' supplémentaire de l'espace $E_v = K[\phi] \cdot v$.*

Preuve. Montrons d'abord que pour tout polynôme $Q \in K[X]$ non divisible par P^m, il existe $R \in K[X]$ tel que $QR \cdot_\phi v = P^{m-1} \cdot_\phi v$. On écrit $Q = P^i Q'$ avec Q' premier avec P ; d'après les hypothèses on aura $i < m$ et $Q' \neq 0$. Alors Q' est inversible modulo P, c'est-à-dire il existe $S \in K[X]$ tel que $Q'S \equiv 1 \pmod P$. Il en résulte que $P^{m-1-i}QS = P^{m-1}Q'S \equiv P^{m-1} \pmod{P^m}$, et on pourra prendre $R = P^{m-1-i}S$ pour avoir $QR \cdot_\phi v = P^{m-1} \cdot_\phi v$. Soit maintenant $\nu \in E^*$ tel que $\nu(P^{m-1} \cdot_\phi v) \neq 0$. Alors pour tout vecteur non nul $w \in E_v$, disons $w = Q \cdot_\phi v$, il existe $R \in K[X]$ tel que $\nu(QR \cdot_\phi v) = 1$, c'est-à-dire $\nu \circ (R[X := \phi])(w) = 1$ ou encore $(R \cdot_{\phi^\top} \nu)(w) = 1$. Comme le polynôme minimal de $\phi^\top$ est le même que celui de ϕ, à savoir P^m, et $P^{m-1} \cdot_{\phi^\top} \nu \neq 0 \in E^*$ (car cette forme linéaire vaut 1 sur v), les $m \deg_X(P)$ formes linéaires $(\phi^\top)^i(\nu)$ pour $0 \leq i < m \deg_X(P)$ forment une K-base de $E^*_\nu = K[\phi^\top] \cdot \nu$, et l'intersection E' de leurs noyaux, qui est le sous-espace de E où toutes les formes de E^*_ν s'annulent, est de codimension $m \deg_X(P) = \dim(E_v)$. Or on a vu qu'aucun vecteur non-nul de E_v se trouve dans E', donc E' est un sous-espace supplémentaire de E_v, et sa description en termes du sous-espace E^*_ν de E^*, qui est $\phi^\top$-stable, montre que E' est ϕ-stable. □

3.4.2. Théorème. *Si E est un K-espace de dimension finie, et $\phi \in \mathrm{End}(E)$, alors il existe des sous-$K[\phi]$-modules cycliques $E_i \subseteq E$ (des sous-espaces contenant un vecteur v_i tel que $E_i = K[\phi] \cdot v_i$, et qui sont donc ϕ-stables), tels qu'on ait une décomposition en somme directe $E = \bigoplus_{i=1}^k E_i$.*

Preuve. On décompose d'abord E en somme directe selon les différents facteurs irréductibles du polynôme minimal μ_ϕ, comme il est indiqué après le théorème 3.3.1. Il reste à prouver le théorème pour chaque noyau $\mathrm{Ker}(P_i^{m_i}[X := \phi])$ figurant dans cette décomposition (car les différentes décompositions se rassembleront alors en une grande somme directe donnant E), donc on supposera désormais que $\mu_\phi = P^m$ avec $P \in K[X]$ irréductible et $m \in \mathbf{N}$. La démonstration pour ce cas est par récurrence sur $\dim(E)$. Si $\dim(E) = 0$ on a une décomposition en 0 sous-modules (la seule raison qu'on vient de permettre $m = 0$, est de admettre une descente à ce cas de base). Sinon il existe d'après la proposition 3.2.7 un vecteur v tel que les hypothèses du lemme 3.4.1 soient vérifiées. Ce lemme nous donne un sous-espace ϕ-stable E' avec $\dim(E') < \dim(E)$, et $\mu_{\phi|_{E'}}$, qui divise μ_ϕ, ne contient pas d'autre facteur irréductible que P (on aura $\mu_{\phi|_{E'}} = 1$ si $E' = \{0\}$). L'hypothèse de récurrence s'applique donc à E', et en fournit une décomposition en somme directe de sous-$K[\phi]$-modules, et en y rajoutant E_v on en obtient une pour E. □

3.4.3. Corollaire. *Si E est un K-espace de dimension finie, et $\phi \in \mathrm{End}(E)$, il existe un vecteur $v \in E$ tel $\mu_{\phi,v} = \mu_\phi$, et un sous-espace ϕ-stable supplémentaire dans E au sous-$K[\phi]$-module cyclique $E_v = K[\phi] \cdot v$.*

Preuve. On sélectionne, dans chaque facteur $N_i = \mathrm{Ker}(P_i^{m_i}[X := \phi])$ de la première décomposition, le sous-$K[\phi]$-module cyclique maximal $K[\phi] \cdot v_i$ de la seconde décomposition (le module pour lequel le

lemme 3.4.1 produisait un supplémentaire), et on prend $C = \bigoplus_{i=1}^{l} K[\phi]\cdot v_i$. On montrera que C est encore un $K[\phi]$-module cyclique ; la somme des supplémentaires des $K[\phi]\cdot v_i$ dans N_i en fournit un supplémentaire ϕ-stable dans E. Pour la cyclicité de C, on établira $C = K[\phi]\cdot s$ pour $s = \sum_{i=1}^{l} v_i$. Cela résulte par exemple du théorème 3.3.1 appliqué à C, $\phi|_C$, et aux polynômes $P_i^{m_i}$: ce théorème redonne évidemment $C = \bigoplus_{i=1}^{l} K[\phi]\cdot v_i$, car on a vu que dans cette décomposition tout sous-module *contient* ces projection sur les facteurs, donc $K[\phi]\cdot s$ contient touts les $K[\phi]\cdot v_i$ et est égal à C tout entier. An autre argument est par le calcul de $\mu_{\phi,s} = \mathrm{ppcm}(\mu_{\phi,v_1},\ldots,\mu_{\phi,v_l})$, car pour que $\psi \in K[\phi]$ annule s, il est nécessaire qu'il annule chaque v_i (par linéarité $\psi(s) = \sum_{i=1}^{l}\psi(v_i)$), et comme $\mu_{\phi,v_i} = P_i^{m_i}$ pour $i = 1,\ldots,l$ qui sont premiers entre eux deux à deux, leur ppcm est égal à leur produit μ_ϕ. Du coup $\dim_K(K[\phi]\cdot s) = \deg_X(\mu_\phi) = \sum_{i=1}^{l}\deg_X(P_i^{m_i}) = \dim_K C$, et on a nécessairement $K[\phi]\cdot s = C$. □

La décomposition du théorème 3.4.2 est utile pour la classification des endomorphismes pour la relation de similitude. Deux K-espaces vectoriels V, W, munis chacun d'un endomorphisme $\phi \in \mathrm{End}(V)$ respectivement $\psi \in \mathrm{End}(W)$, seront appelés isomorphes pour cette structure s'il existe un isomorphe de K-espaces vectoriels $f : V \to W$ qui "commute" avec les endomorphismes dans le sens $f\circ\phi = \psi\circ f$. Ainsi les structures définies sur le même espace muni de deux endomorphismes ϕ, ψ sont isomorphes si et seulement si les endomorphismes sont similaires, car on aura $f\circ\phi\circ f^{-1} = \psi$. Cette notion sera surtout appliquée aux sous-espaces ϕ-stables (des sous-$K[\phi]$-modules) de notre espace E, munis de leurs restrictions respectives de ϕ. Elle permet notamment de dire que deux sous-$K[\phi]$-modules *cycliques* sont isomorphes si et seulement s'ils ont le même polynôme minimal (qui sera aussi polynôme caractéristique), car si $E_x = K[\phi]\cdot x$ et $E_y = K[\phi]\cdot y$ avec $\mu_{\phi,x} = \mu_{\phi,y}$, on peut définir une application K-linéaire $f : E_x \to E_y$ sur la base $\{\,\phi^i(x) : 0 \le i < \deg_X(\mu_{\phi,x})\,\}$ par $f(\phi^i(x)) = \phi^i(y)$, qui vérifie $f\circ\phi|_{E_x} = \phi|_{E_y}\circ f$. Il en découle directement que si on trouve pour E muni de ϕ respectivement de ψ des décompositions comme dans le théorème 3.4.2, avec le même nombre de facteurs et où les facteurs correspondants ont le même polynôme minimal, alors ϕ et ψ sont similaires (on étend les isomorphismes à la somme directe).

Mais d'autre part, même pour des décompositions de E pour un seul endomorphisme ϕ, le nombre de facteurs cycliques n'est pas toujours le même, car on a vu dans le corollaire qu'une somme directe de modules cycliques peut encore être cyclique. On ne pourra espérer de trouver un nombre indépendant de la décomposition choisie que si l'on exige des facteurs cycliques non triviaux (c'est-à-dire de dimension > 0) qui ne se décomposent pas en somme directe d'autres facteurs cycliques non triviaux ; cela veut dire (à cause de la décomposition des noyaux) que leurs polynômes minimaux sont des puissances d'un seul polynôme irréductible. (Un autre approche possible est d'essayer au contraire de former des modules cycliques "les plus gros possibles", et donc en nombre minimal ; on y reviendra.) Si $\mu_\phi = P^m$ avec $P \in K[X]$ irréductible, la décomposition du théorème 3.4.2 contiendra uniquement des facteurs avec un polynôme minimal de la même forme, mais éventuellement avec un exposant de P plus petit.

3.4.4. Lemme. *Si $\phi \in \mathrm{End}(E)$ est tel que $\mu_\phi = P^m$ avec $P \in K[X]$ irréductible, alors il existe des nombres naturels $k_1,\ldots,k_m$ tels que dans toute décomposition de E comme somme directe de sous-$K[\phi]$-modules cycliques, il y a k_i facteurs dont le polynôme minimal est P^i, pour $i = 1,\ldots,m$.*

Preuve. Posons $d = \deg_X(P)$ et $\psi = P[X := \phi] \in \mathrm{End}(E)$. Pour un sous-$K[\phi]$-module cyclique M de polynôme minimal P^i, et $j \in \mathbf{N}$, l'intersection $M \cap \mathrm{Ker}(\psi^j)$ est un sous-$K[\phi]$-module cyclique de polynôme minimal $P^{\min(i,j)}$, et donc de dimension $d\min(i,j)$: si $j \ge i$ l'intersection est égal à M tout entier, et si $j < i$ elle est égal a $\psi^{i-j}(M)$, et engendrée par $\psi^{i-j}(v)$ où v est un générateur de M. Il en découle que si on a une décomposition de E comme somme directe de sous-$K[\phi]$-modules cycliques avec k_i facteurs de polynôme minimal P^i pour $i = 1,\ldots,m$, alors $\dim_K \mathrm{Ker}(\psi^j) = d(\sum_{i<j} ik_i + j\sum_{i=j}^{m} k_i)$ pour $j \le m+1$, et donc $\dim_K \mathrm{Ker}(\psi^j) - \dim_K \mathrm{Ker}(\psi^{j-1}) = \sum_{i=j}^{m} k_i$ pour $j > 0$. Par conséquent on peut retrouver le nombre $k_j = (\dim_K \mathrm{Ker}(\psi^j) - \dim_K \mathrm{Ker}(\psi^{j-1})) - (\dim_K \mathrm{Ker}(\psi^{j+1}) - \dim_K \mathrm{Ker}(\psi^j))$ pour $0 < j \le m$, dans quelle équation le second membre ne dépend pas de la décomposition, et les k_j ne le font donc pas non plus. □

3.4.5. Corollaire. *Soit $\phi, \psi \in \mathrm{End}(E)$. La condition suivante est nécessaire et suffisante pour que ϕ et ψ soient similaires: $\mu_\phi = \mu_\psi$, et $\dim_K(\mathrm{Ker}(P^i[X := \phi])) = \dim_K(\mathrm{Ker}(P^i[X := \psi]))$ pour chaque diviseur irréductible P de μ_ϕ, et chaque $i > 0$ tel que P^i divise μ_ϕ.*

Preuve. Si ϕ et ψ sont similaires on a un isomorphisme pour les structures de E muni de ϕ et de ψ, ce implique directement les égalités mentionnées, donc la condition est clairement nécessaire. D'après le théorème 3.4.2 et la démonstration du lemme 3.4.4, la condition implique que E admet des décompositions en somme directe de $K[\phi]$-modules cycliques respectivement de $K[\psi]$-modules cycliques, avec une bijection entre les facteurs cycliques telle que les modules correspondants ont le même polynôme minimal, et sont donc isomorphes. Les isomorphismes se combinent par les sommes directes, pour obtenir un isomorphe de E en tant que $K[\phi]$-module avec E en tant que $K[\psi]$-module, ce qui montre que ϕ et ψ sont similaires. □

Le cas les plus simple des modules cycliques sont ceux avec polynôme minimal $(X-\lambda)^i$. Si $i=1$ on a juste une droite vectorielle contenue dans le sous-espace propre pour λ, mais si $i>1$ le module est un sous-espace de dimension i contenu dans l'espace caractéristique pour λ mais pas dans le sous-espace *propre* pour λ ; plus précisément, le module intersecte cet espace propre en un sous-espace de dimension 1. L'espace caractéristique se décompose en de tels modules (où l'exposant i peut varier). Si $v \in E$ est générateur du module cyclique (donc $v \in \mathrm{Ker}((\phi-\lambda\,\mathrm{id})^i) \setminus \mathrm{Ker}((\phi-\lambda\,\mathrm{id})^{i-1})$, alors $\phi^{i-1}(v),\ldots,\phi^2(v),\phi(v),v$ est une base du sous-espace (il est habituel de prendre les vecteurs dans cet ordre), et la matrice de ϕ sur cette base sera de la forme (illustrée pour $i=5$)

$$\begin{pmatrix} \lambda & 1 & 0 & 0 & 0 \\ 0 & \lambda & 1 & 0 & 0 \\ 0 & 0 & \lambda & 1 & 0 \\ 0 & 0 & 0 & \lambda & 1 \\ 0 & 0 & 0 & 0 & \lambda \end{pmatrix}.$$

Une telle matrice, qui apparaîtra comme bloc diagonal de la matrice de ϕ sur une base adaptée à toute la décomposition en modules cycliques, s'appelle un *bloc de Jordan*. On peut avoir plusieurs sous-$K[\phi]$-modules avec polynômes minimaux de la forme $(X-\lambda)^i$ pour la même valeur propre λ, et dans ce cas les blocs de Jordan se combinent en une forme illustrée ici pour le cas suivant : un sous-module avec polynôme minimal $(X-\lambda)^3$, deux sous-modules avec polynôme minimal $(X-\lambda)^2$, et un sous-module avec polynôme minimal $X-\lambda$:

$$\begin{pmatrix} \lambda & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \lambda & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \lambda & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \lambda & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \lambda & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \lambda & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \lambda & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & \lambda \end{pmatrix}.$$

Un endomorphisme dont le polynôme minimal est une puissance de $X-\lambda$ possède toujours une matrice d'une telle forme sur une base adaptée (appelée base de Jordan). L'ordre des blocs de Jordan n'est pas imposé, mais un choix raisonnable est de les ordonner par taille, faiblement croissante (car les vecteurs de la base sont le plus naturellement énumérés de droite à gauche, et les modules cycliques sont trouvés, dans la preuve du théorème 3.4.2, du plus grand au plus petit). Plus généralement, si μ_ϕ est scindé dans $K[X]$, on peut décomposer l'espace E en une somme directe de sous-espaces caractéristiques pour ϕ, et le polynôme minimal de la restriction de ϕ au sous-espace caractéristique pour λ est une puissance de $X-\lambda$. Le choix d'une base de Jordan dans chaque sous-espace caractéristique donne donc une base de E, appelée toujours base de Jordan pour ϕ, dans laquelle la matrice de ϕ est diagonale en blocs qui correspondent aux différentes valeurs propres, chaque bloc étant à son tour diagonal en blocs de Jordan ; la matrice de cette forme s'appelle *forme normale de Jordan* de ϕ. Dans le cas d'un endomorphisme (ou d'une matrice) diagonalisable, la forme normale de Jordan est la même que la forme diagonale.

Quand le polynôme minimal d'un endomorphisme $\phi \in \mathrm{End}(E)$ n'est pas scindé, il n'existe pas de base de E dans laquelle la matrice de ϕ est une forme normale de Jordan (on pourra trouver une telle forme normale pour une matrice de ϕ en utilisant une extension du corps K, mais ni la forme normale, ni la matrice de passage n'auront leurs coefficients dans K). Si l'on veut considérer néanmoins de formes normales qui permettent de caractériser des classes de similitude, il faudra décider quelle matrice préférer

pour un (sous-)module cyclique. Ces modules sont caractérisés par leur polynôme minimal M, ils sont de dimension $d = \deg_X(M)$ (donc M est aussi le polynôme caractéristique du module), et si v est un générateur du module, c'est-à-dire $\mu_{\phi,v} = M$, alors on a vu que $v, \phi(v), \ldots, \phi^{d-1}(v)$ est une K-base du module. La matrice de ϕ dans cette base est

$$\begin{pmatrix} 0 & 0 & 0 & \ldots & 0 & -c_0 \\ 1 & 0 & 0 & \ldots & 0 & -c_1 \\ 0 & 1 & 0 & \ldots & 0 & -c_2 \\ \vdots & 0 & 1 & \ddots & \vdots & \vdots \\ \vdots & \vdots & \ddots & \ddots & 0 & \vdots \\ 0 & 0 & \ldots & 0 & 1 & -c_{d-1} \end{pmatrix}$$

où $M = c_0 + c_1X + c_2X^2 + \cdots + c_{d-1}X^{d-1} + X^d$, car ϕ envoie chaque vecteur de la base choisie vers le suivant, sauf que le dernier est envoyé vers $\phi^d(v) = -c_0v - c_1\phi(v) + -c_2\phi^2(v) + \cdots + -c_{d-1}\phi^{d-1}(v)$. Cette matrice s'appelle la *matrice compagnon* du polynôme M. Chaque polynôme unitaire dans $K[X]$ possède une matrice compagnon, dont il est le polynôme minimal (et aussi le polynôme caractéristique, par le théorème de Cayley-Hamilton). La forme d'une matrice compagnon porte à l'évidence le fait que l'espace est un $K[\phi]$-module cyclique, et que le premier vecteur de la base canonique en est un générateur.

Par contre cette forme n'indique rien sur une éventuelle décomposition du polynôme M. Si M se décompose en facteurs premiers entre eux, on sait que le module cyclique possède une décomposition en somme directe de module cycliques, et la matrice compagnon sera alors similaire à une matrice diagonale en blocs de matrices compagnon des polynômes dans la décomposition de M. Si on cherche une forme normale mettant en évidence de telles décompositions (et qui seront diagonales dans le cas diagonalisable), il faudrait donc mieux exclure des matrices compagnon pour des polynômes autres que des puissances $M = P^k$ d'un polynômes irréductible P. Dans ce dernier cas, il serait alors logique de mettre en évidence P et k (ce qui ne fait pas la matrice compagnon de M), mais on n'a pas de somme directe, donc cette matrice compagnon *ne sera pas similaire* à une matrice diagonale en k blocs tous matrice compagnon de P (sauf bien sûr si $k = 1$). Dans le cas $P = X - \lambda$ on avait utilisé la base formée de $v, P\cdot_\phi v, P^2\cdot_\phi v, \ldots, P^{k-1}\cdot_\phi v$ (dans l'ordre opposé) pour trouver un bloc de Jordan comme forme normale ; dans le cas $d = \deg_X(P) > 1$, cette famille de vecteurs ne suffit pas, mais on pourra la compléter avec ses images par ϕ^j pour $j = 1, \ldots, d-1$, pour trouver l'ensemble $\{\, P^iX^j \cdot_\phi v : 0 \leq i < k, 0 \leq j < d \,\}$, qui est une K-base du module cyclique car les degrés des polynômes utilisés parcourent sans répétitions tous les nombres naturels inférieurs à $dk = \deg_X(M)$. La matrice de ϕ dans cette base, qu'on ordonne par degré *décroissant* du polynôme concerné (pour généraliser les blocs de Jordan), sera proche d'une matrice diagonale en blocs, de la façon suivante (illustrée pour $k = 3$ et $P = X^d - p_{d-1}X^{d-1} - \cdots - p_1X^1 - p_0$:

$$\begin{pmatrix} p_{d-1} & 1 & 0 & \ldots & 0 & & & & & & & & & \\ \vdots & 0 & \ddots & \ddots & \vdots & & & & & & & & & \\ \vdots & \vdots & \ddots & 1 & 0 & \ddots & & & & & & & & \\ p_1 & 0 & \ldots & 0 & 1 & 0 & \ddots & & & & & & & \\ p_0 & 0 & \ldots & 0 & 0 & 1 & 0 & \ddots & & & & & & \\ & & & & & p_{d-1} & 1 & 0 & \ldots & 0 & & & & \\ & & & & & \vdots & 0 & \ddots & \ddots & \vdots & & & & \\ & & & & & \vdots & \vdots & \ddots & 1 & 0 & \ddots & & & \\ & & & & & p_1 & 0 & \ldots & 0 & 1 & 0 & \ddots & & \\ & & & & & p_0 & 0 & \ldots & 0 & 0 & 1 & 0 & \ddots & \\ & & & & & & & & & & p_{d-1} & 1 & 0 & \ldots & 0 \\ & & & & & & & & & & \vdots & 0 & \ddots & \ddots & \vdots \\ & & & & & & & & & & \vdots & \vdots & \ddots & 1 & 0 \\ & & & & & & & & & & p_1 & 0 & \ldots & 0 & 1 \\ & & & & & & & & & & p_0 & 0 & \ldots & 0 & 0 \end{pmatrix}.$$

On aura donc des blocs diagonaux qui sont des matrices compagnon de P renversées (les ordres les lignes et des colonnes sont inversés), et qui sont reliés par des coefficients 1 juste au dessus de la diagonale principale, à la manière des blocs de Jordan. On appellera ici cette forme, qui n'est pas souvent mentionnée dans la littérature (et l'est parfois sous sa forme renversée), un bloc de Jordan généralisé. Le fait qu'on trouve effectivement cette matrice sur la base indiquée se démontre par les calculs simples suivants: on a $\phi(P^iX^j \cdot_\phi v) = P^iX^{j+1} \cdot_\phi v$ pour tout $j < d$ (donc ici l'image d'un vecteur de la base en est encore un), ainsi que

$$\phi(P^iX^{d-1} \cdot_\phi v) = P^iX^d \cdot_\phi v = P^i(P + p_{d-1}X^{d-1} + \cdots + p_1X^1 + p_0) \cdot_\phi v,$$

dont chaque terme donne un multiple d'un vecteur de la base, sauf $P^k \cdot_\phi v = 0$. On vérifiera que pour $P = X - \lambda$, la matrice compagnon étant réduite à sa plus petite forme possible, de taille 1×1 et avec coefficient $p_0 = \lambda$, on retrouve un bloc de Jordan pour la valeur propre λ.

Une forme normale d'un endomorphisme ϕ peut maintenant être formulée, quelle forme existera indépendamment de la question si μ_ϕ (ou de façon équivalente χ_ϕ) est scindé ou non, et qui se réduit à la forme normal de Jordan si celle-ci existe. C'est une forme diagonale en blocs qui sont des blocs de Jordan généralisés, chacun pour un polynôme irréductible (unitaire) P et un exposant k. L'existence de cette forme normale est assurée par les théorèmes 3.3.1 et 3.4.2 (ou par la démonstration de ce dernier), qui donnent une décomposition de l'espace vectoriel en modules cycliques dont le polynôme minimal est une puissance d'un polynôme irréductible. L'ordre des blocs n'est pas imposé, et il serait difficile de spécifier en général un ordre préféré parmi les polynômes irréductibles qui peuvent intervenir ; mais comme pour les blocs de Jordan il est naturel d'exiger que les blocs pour un même polynôme irréductible soient regroupés, et que dans ce groupe les blocs soient ordonnés par taille croissante. Le lemme 3.4.4 assure le caractère "forme normale" : deux endomorphismes sont similaires si et seulement si les mêmes polynômes irréductibles P interviennent, et si pour chaque tel P la matrice formée de blocs de Jordan généralisés associés (dont l'ordre est standardisé comme indiqué) sont identiques pour les deux endomorphismes.

Si on se contente des matrices compagnon sans vouloir factoriser les polynômes correspondants (une opération dont on est après tout pas sûr qu'elle soit effectivement faisable), on peut se passer de la décomposition des noyaux, et au contraire essayer de décomposer l'espace en somme directe de sous-modules les plus grands (et donc les moins nombreux) possibles. Un sous-module cyclique dont le polynôme minimal (de sa restriction de ϕ) coïncide avec celui de ϕ, et dont l'existence est assuré par le corollaire 3.4.3, est un candidat évident comme composante d'un tel somme directe, car il est de dimension maximale pour un sous-module cyclique. Ce corollaire permet d'affiner le théorème 3.4.2 comme suit.

3.4.6. Théorème. *Soit E est un K-espace de dimension finie, et $\phi \in \mathrm{End}(E)$. Il existe une liste finie de polynômes unitaires $F_1, \ldots, F_k \in K[X]$ telle que $1 \neq F_1 \mid \cdots \mid F_k$ et telle qu'il existe une décomposition $E = \bigoplus_{i=1}^k E_i$, où E_i est un sous-$K[\phi]$-module cyclique de polynôme minimal F_i, pour $i = 1, \ldots, k$. Les polynômes F_i sont appelés les facteurs invariants de ϕ, et on a $F_k = \mu_\phi$ ainsi que $F_1 \cdots F_k = \chi_\mu$.*

Preuve. Observons d'abord que les dernières affirmations découlent des propriétés précédentes : le polynôme caractéristique d'un sous-$K[\phi]$-module cyclique est le même que son polynôme minimal, et dans une somme directe de sous-modules, les polynômes minimal et caractéristique de la somme sont respectivement le ppcm et le produit de ces polynômes pour les composantes. L'existence des F_i avec une décomposition correspondante se montre par récurrence sur $\dim(E)$. Si $\dim(E) = 0$ la liste vide avec somme directe vide conviennent. Si $\dim(E) > 0$ on a $\deg_X(\mu_\phi) > 0$, et application du corollaire 3.4.3 fournit un sous-module cyclique C avec $\mu_{\phi|_C} = \mu_\phi$, ainsi qu'un sous-espace ϕ-stable E' tels que $E = E' \oplus C$. L'hypothèse de récurrence appliquée à E' en donne une décomposition $E' = \bigoplus_{i=1}^{k-1} E_i$, et en prenant $E_k = C$ on a $E = \bigoplus_{i=1}^k E_i$. Or comme $\mu_{\phi|_{E'}} \mid \mu_\phi$, les polynômes minimaux F_i des composantes E_i de E' divisent tous $\mu_\phi = \mu_{\phi|_C} = F_k$, ce qui avec l'hypothèse de récurrence montre $F_1 \mid \cdots \mid F_k$.

Pour l'unicité des F_i, on utilisera le lemme 3.4.4, et pour le faire on commence par décomposer le polynôme minimal $\mu_\phi = P_1^{m_1} \ldots P_l^{m_l}$ en puissances de polynômes irréductibles distincts, et on applique le théorème 3.3.1 pour cette décomposition à E et à chaque composante E_i. Il est facile à voir que

$\mathrm{Ker}(P_j^{m_j}[X := \phi])$ contient $\mathrm{Ker}(P_j^{m_j}[X := \phi|_{E_i}])$ pour tout i, j, et comme on a

$$\bigoplus_{j=1}^{l} \mathrm{Ker}(P_j^{m_j}[X := \phi]) = E = \bigoplus_{i=1}^{k} E_i = \bigoplus_{i=1}^{k}\bigoplus_{j=1}^{l} \mathrm{Ker}(P_j^{m_j}[X := \phi|_{E_i}]) = \bigoplus_{j=1}^{l}\bigoplus_{i=1}^{k} \mathrm{Ker}(P_j^{m_j}[X := \phi|_{E_i}])$$

on peut conclure que $\mathrm{Ker}(P_j^{m_j}[X := \phi]) = \bigoplus_{i=1}^{k} \mathrm{Ker}(P_j^{m_j}[X := \phi|_{E_i}])$ pour $j = 1, \ldots, l$. Or comme $\mu_{\phi|_{E_i}} = F_i$, le polynôme minimal du sous-$K[\phi]$-module cyclique $\mathrm{Ker}(P_j^{m_j}[X := \phi|_{E_i}])$ est $\mathrm{pgcd}(F_i, P_j^{m_j})$. C'est une puissance de P_j, disons $\mathrm{pgcd}(F_i, P_j^{m_j}) = P_j^{d_{i,j}}$, et la condition de divisibilité $F_1 \mid \cdots \mid F_k$ donne après application du pgcd : $P_j^{d_{1,j}} \mid \cdots \mid P_j^{d_{k,j}}$, c'est-à-dire $d_{1,j} \leq \cdots \leq d_{k,j}$. En appliquant le lemme 3.4.4 au sous-$K[\phi]$-module $\mathrm{Ker}(P_j^{m_j}[X := \phi])$, on voit que le k-uplet $(d_{1,j}, \ldots, d_{k,j})$ est entièrement déterminé par les nombres $k_1, \ldots, k_{m_j}$ dans le lemme, car k_i parmi $d_{1,j}, \ldots, d_{k,j}$ sont égaux à i, pour $i = 1, \ldots, m_j$. En détail, soit $k_0 = k - k_1 - \cdots - k_{m_j}$ de sorte que $k = \sum_{i=0}^{m_j} k_i$, alors le k-uplet est formé de k_0 fois un 0, ensuite k_1 fois un 1, et ainsi de suite jusqu'à k_{m_j} fois une valeur m_j. Ceci montre que $k \geq \sum_{i=1}^{m_j} k_i$ pour $j = 1, \ldots, l$, et que, étant donné k, les nombres $d_{1,j}, \ldots, d_{k,j}$ pour $j = 1, \ldots, l$ sont indépendants de la décomposition $E = \bigoplus_{i=1}^{k} E_i$ utilisée (car les modules $\mathrm{Ker}(P_j^{m_j}[X := \phi])$ n'y dépendent pas), et donc aussi les polynômes $F_i = P_1^{d_{i,1}} \ldots P_l^{d_{i,l}}$. Il reste juste à montrer l'unicité du nombre k de polynômes dans la liste, qui résulte de l'exigence $F_1 \neq 1$, qui implique que l'un au moins des exposants $d_{1,1}, \ldots, d_{1,l}$ doit être non nul ; ceci force k à être égal au maximum des valeurs de $k_1 + \cdots + k_{m_j}$ obtenues dans les différentes applications du lemme 3.4.4 (pour que pour ce cas on aura $k_0 = 0$, et donc $d_{1,j} > 0$). □

La démonstration ci-dessus à l'air très compliqué, mais l'idée est assez simple : par le théorème du décomposition des noyaux, la question peut être réduite à des questions dans les noyaux $\mathrm{Ker}(P_j^{m_j}[X := \phi])$ individuels, dans lesquels le lemme 3.4.4 donne les multiplicités des différents types de sous-modules cycliques, et la condition $F_1 \mid \cdots \mid F_k$ force ces modules d'être ordonnés en ordre faiblement croissant (avec éventuellement un nombre de modules triviaux au début pour atteindre le bon nombre de composantes).

3.4.7. Corollaire (forme normale rationnelle). *Pour tout endomorphisme ϕ d'un K-espace E de dimension finie, il existe un matrice unique qui est la matrice de ϕ sur une certaine base de E, et qui est diagonale en blocs, dont les blocs sont des matrices compagnon pour une liste de polynômes unitaires dont chaque polynôme divise le suivant. Deux endomorphismes sont similaires si et seulement si les matrices ainsi associées à l'un et à l'autre sont identiques.*

Preuve. Une telle matrice donne lieu à une décomposition en somme directe de sous-$K[\phi]$-modules comme décrite dans le théorème, en prenant les sous-espaces engendrés pas les parties de la base correspondantes aux blocs. Réciproquement une telle décomposition donne lieu à une base sur laquelle la matrice de ϕ est de la forme décrite, en choisissant dans chaque module une base dans laquelle la restriction de ϕ est donnée par une matrice compagnon. La dernière partie découle de l'unicité de la matrice. □

3.5. *Le théorème de Cayley-Hamilton pour des matrices sur un anneau commutatif.*

On a démontré le théorème de Cayley-Hamilton (3.2.9) pour les endomorphismes d'un K-espace vectoriel, en utilisant essentiellement le fait que la multiplicité d'une valeur propre λ comme racine du polynôme caractéristique est égal à la dimension du sous-espace caractéristique pour λ. Cette propriété est une conséquence de la définition du polynôme caractéristique comme un déterminant, et le fait qu'un endomorphisme est trigonalisable dès que son polynôme caractéristique (ou son polynôme minimal) est scindé. Pour pouvoir se servir de ce résultat, il était nécessaire d'étendre le corps de base (ce qui ne change ni le polynôme caractéristique, ni le polynôme minimal) à un corps sur lequel ces polynômes sont scindés. Sans une telle extension, l'utilisation du polynôme caractéristique serait plus difficile, car son rapport avec l'endomorphisme n'est pas facile à exprimer en l'absence de valeurs propres. Pour le polynôme minimal cela est plus facile : il suffit de considérer aussi ses facteurs irréductibles de degré plus grand que 1.

On peut néanmoins comprendre le théorème de Cayley-Hamilton sans avoir recours à une extension de corps. Pour la matrice compagnon M d'un polynôme unitaire P, dont le polynôme minimal est égal à P de façon évidente (par le lemme 3.2.3), on peut vérifier sans faire appel au théorème de Cayley-Hamilton que P en est aussi le polynôme caractéristique ; c'est un exercice classique, qui utilise une suite

d'opérations sur la matrice $X\,\mathrm{id} - M$ avant d'en prendre le déterminant. Pour une matrice diagonale en blocs qui sont des matrices compagnon, le polynôme caractéristique est le produit de ceux des blocs, et le polynôme minimal en est le ppcm. Ainsi le théorème 3.4.2 implique celui de Cayley-Hamilton.

Mais cela reste une démonstration par des arguments *structurels* (notamment la décomposition en modules cycliques) qui dépendent du fait qu'on considère des matrices à coefficients dans un corps. Mais formulé sous la forme $\chi_A[X := A] = 0 \in \mathrm{Mat}_n(R)$ pour tout $A \in \mathrm{Mat}_n(R)$, le théorème a un sens pour tout anneau commutatif R (la commutativité est nécessaire pour définir χ_A), et par des arguments générales on peut déduire de la *forme* de l'énoncé (une identité algébrique où tout dépend de façon polynomiale des coefficients de A), que la validité du théorème de Cayley-Hamilton doit s'étendre à ce cas. On va donner une démonstration de ce théorème en tant que identité algébrique, d'une telle façon qu'elle soit valable dans le généralité de matrices carrées sur un anneau commutatif.

La clef d'une telle démonstration is une identité qui pour toute matrice carrée B décrit l'homothétie de facteur $\det(B)$ comme un multiple (à gauche ou à droite) de B. Soit, pour $j = 1, \ldots, n$ et $B \in \mathrm{Mat}_n(R)$, $f_{j,B} : R^n \to R$ l'application qui à $x \in R^n$ associe le déterminant de la matrice obtenue à partir de B en remplaçant la colonne j par x. Comme le déterminant est multilinéaire et alternée, l'application $f_{j,B}$ est R-linéaire, et $f_{j,B}(B_{[i]}) = 0$ si $B_{[i]}$ est la colonne i de B avec $i \neq j$. Aussi $f_{j,B}(B_{[j]}) = \det B$ pour tout j, donc

$$f_{j,B}(B_{[i]}) = \delta_{i,j} \det B \qquad \text{pour tout } i, j \in \{1, \ldots, n\}. \tag{10}$$

Comme toute application R-linéaire $R^n \to R$, les $f_{j,B}$ peuvent être représentées par une matrice à une ligne, dont le coefficient i est la valeur de l'application au i-ème élément e_i de la base canonique de R^n. Si on arrange ces n matrices l'une en dessous de l'autre, on obtient une matrice $C_B \in \mathrm{Mat}_{n,n}(R)$ qui correspond à l'application linéaire $R^n \to R^n$, qui envoie $x \mapsto (f_{1,B}(x), \ldots, f_{n,B}(x))$. Il découle de (10) que

$$C_B \cdot B = \det(B).I_n \qquad \text{où } I_n \in \mathrm{Mat}_{n,n}(R) \text{ est la matrice identité } (I_n)_{i,j} = \delta_{i,j}. \tag{11}$$

On appelle C_B (ou plutôt sa transposée, pour des mauvaises raisons qui suivront) la comatrice de B. Dans ce qui suit le seul point important sera qu'une matrice $C_B \in \mathrm{Mat}_{n,n}(R)$ existe qui vérifie (11), mais on peut expliciter facilement ses coefficients : on a vu que $(C_B)_{j,i} = f_{j,B}(e_i)$, ce qui est le déterminant de la matrice obtenue en remplaçant la colonne j de B par e_i. Dans cette matrice la colonne j de B a disparue, et comme e_i a des coefficients 0 hors de la position i, ce qui reste de la ligne i de B n'a pas d'influence sur $f_{j,B}(e_i)$ non plus ; on voit que $f_{j,B}(e_i) = (-1)^{i-j} \det B'$ où B' est la matrice obtenue en supprimant la colonne j et la ligne i de B. On remarque le changement de correspondance avec lignes et colonnes pour les indices i, j entre la matrice C_B et B, ce qui explique la transposée mentionnée ci-dessus. En tout cas cette description explicite, en combinaison avec la symétrie du déterminant lui-même, rend évident le fait que la transposition de la matrice B de départ changera aussi la comatrice par une transposition, et on a donc $(C_B)^\top \cdot B^\top = \det(B).I_n$, ce qui est équivalent à $B \cdot C_B = \det(B).I_n$, d'où toute matrice commute avec la transposée de sa comatrice.

Pour approcher le théorème de Cayley-Hamilton, on applique ce qui précède, et en particulier la formule (11), à la matrice $B = XI_n - A \in \mathrm{Mat}_{n,n}(R[X])$, dont le polynôme caractéristique $\chi_A \in R[X]$ est le déterminant. On trouve ainsi pour une certaine matrice $C \in \mathrm{Mat}_{n,n}(R[X])$ que

$$C \cdot (XI_n - A) = \det(XI_n - A).I_n = \chi_A I_n = (XI_n - A) \cdot C. \tag{12}$$

Les membres de cette identité sont dans $\mathrm{Mat}_{n,n}(R[X])$: ce sont des matrices carrées à coefficients polynomiaux. Il est cependant tentant de les considérer comme des polynômes en X à coefficients dans $S = \mathrm{Mat}_{n,n}(R)$, dans quelle interprétation l'identité exprime que $X - A$ est facteur à droite ou à gauche de χ_A (on n'écrit plus les facteurs I_n, car c'est l'élément 1 de S). Mais il faut faire attention, car cet anneau $S[X]$ est un anneau de polynômes sur un anneau *non commutatif* S ; aussi, si on veut changer de point de vue, il est nécessaire de prouver que l'identification entre $\mathrm{Mat}_{n,n}(R[X])$ et $\mathrm{Mat}_{n,n}(R)[X] = S[X]$ est en fait un isomorphisme d'anneaux. Le premier point n'est pas vraiment un problème, car (contrairement à beaucoup d'ouvrages) nous avons pris soin de ne pas exiger la commutativité des coefficients dans notre définition de base des polynômes, 1.4.1 ; ceci dit, la prudence est de mise car de nombreux résultats ne

sont pas valable sans hypothèse de commutativité. Le second point est facile à régler, car d'après le théorème 1.5.1 il existe un morphisme d'anneaux unique $S[X] \to \mathrm{Mat}_{n,n}(R[X])$ qui est l'identité sur S et qui envoie $X \mapsto XI_n$ (élément du centre de $\mathrm{Mat}_{n,n}(R[X])$), et dont on vérifie qu'il coïncide avec notre "changement de point de vue" (essentiellement parce que $(XI_n)^i = X^i I_n$).

On peut donc affirmer que (12) exprime des décompositions $C(X-A) = \chi_A = (X-A)C$ dans l'anneau de polynômes $S[X]$. Le théorème de Cayley-Hamilton affirme que la substitution $X := A$ annule le polynôme caractéristique χ_A, et il semble que la décomposition donnée démontre cela tout de suite, car cette substitution annule de façon évidente les facteurs $X - A$. Mais cet argument n'est pas valable, car il suppose que la substitution est un *morphisme* d'anneaux $S[X] \to S$, et le théorème 1.5.1 qui affirme cela dépend de l'hypothèse que l'élément substitué, dans notre cas la matrice $A \in S$, commute avec tous les éléments de S, et cela n'est pas vrai en général. Néanmoins, on verra qu'ici les coefficients de C, c'est-à-dire de la comatrice de $XI_n - A$ considérée comme polynôme en X à coefficients matriciels, sont tous dans le sous-anneau *commutatif* $R[A]$ de $S = \mathrm{Mat}_{n,n}(R)$, d'où chaque décomposition indiquée se produit dans $R[A][X]$; la substitution définit alors un morphisme d'anneaux $R[A][X] \to R[A]$, qui justifie que l'annulation de $X - A$ entraîne celle de χ_A. Mais pour pouvoir utiliser cet argument, il faut d'abord prouver la commutation, qui n'est pas du tout évidente à partir de la définition de la comatrice.

Pour arriver à une démonstration du théorème à l'aide de cette décomposition, plusieurs méthodes sont possibles. La méthode la plus transparente est d'observer qu'on peut déduire de l'unicité d'une division avec reste à gauche par le polynôme unitaire $X - A$ que $C \in R[A][X]$. La proposition 1.5.12 nous affirme cette unicité (qui est aussi valable pour la division à droite, mais le quotient et reste peuvent être différents entre les deux cas). On raisonne alors ainsi : d'après (12), la division à gauche avec reste de χ_A par $X - A$ dans $S[X]$ a pour solution un quotient C et un reste nul ; la même division dans $R[A][X]$ (qui est possible car χ_A et $X - A$ sont dans $R[A][X]$) produit aussi un quotient et un reste, et ils ne peuvent pas être différents de ceux trouvés dans $S[X]$ car cela donnerait une deuxième solution dans cet anneau. Par conséquent le quotient C de la division dans $S[X]$ est en fait dans $R[A][X]$, ce qui permet d'appliquer le morphisme $R[A][X] \to R[A]$ d'évaluation en A à l'identité $\chi_A = (X-A)C$ donnant $\chi_A[X := A] = 0$.

Une autre méthode consiste à analyser $C(XI_n - A) = \chi_A I_n$ comme identité dans $\mathrm{Mat}_{n,n}(R[X])$ sans faire appel aux polynômes à coefficients dans un anneau non-commutatif. Ceci faisant, on se rendra néanmoins compte du fait que cette analyse relève essentiellement du calcul d'une division euclidienne (dans un contexte non-commutatif) dont le quotient correspond à C et dont le reste est nul. On écrit $\chi_A = X^n + d_{n-1}X^{n-1} + \cdots + d_1X + d_0$, et $C = C_{n-1}X^{n-1} + \cdots + C_1X + C_0$ avec $C_i \in \mathrm{Mat}_{n,n}(R)$, autrement dit C_i est la matrice qui à chaque position contient le coefficient de X^i dans le polynôme qui est l'entrée de C à cette position (ces polynômes sont de degré au plus $n-1$ par la définition de comatrice, et aussi par l'équation qu'on est en train d'analyser). Le bilinéarité le produit matriciel donne

$$(XI_n - A)C = X^nC_{n-1} - X^{n-1}AC_{n-1} + X^{n-1}C_{n-2} - X^{n-2}AC_{n-2} + \cdots + X^2C_1 - XAC_1 + XC_0 - AC_0$$

et cela est égal à $X^nI_n + X^{n-1}d_{n-1}I_n + \cdots + Xd_1I_n + d_0I_n$. Cette égalité ne peut se produire que lorsque les matrices par laquelle chaque X^i est multiplié sont identiques, ce qui donne les $n+1$ équations

$$C_{n-1} = I_n, \quad -AC_{n-1} + C_{n-2} = d_{n-1}I_n, \quad \ldots, -AC_1 + C_0 = d_1I_n, \quad -AC_0 = d_0I_n.$$

Les équations au milieu donnent les relations récurrentes $C_{i-1} = d_iI_n + AC_i$ pour $i = n-1, \ldots, 1$. En posant $d_n = 1$, ces équations avec la première se résolvent par $C_{i-1} = \sum_{k=i}^{n} A^{k-i}d_k$. Alors la dernière équation donne

$$0 = d_0I_n + AC_0 = d_0I_n + \sum_{k=1}^{n} A^k d_k = \chi_A[X := A].$$

On voit bien comment les C_i pour i décroissant sont des approximations successives du quotient de la division de χ_A par $X - A$ (à gauche, mais comme les deux commutent, les approximations pour la division à droite sont identiques), et que le fait que la division s'avère exacte entraîne l'annulation de $\chi_A[X := A]$. D'ailleurs, en substituant $X := 0$, on voit que la comatrice (transposée) C_0 de $-A$ est égal à $\chi_A^{\downarrow}[X := A]$ où $P^{\downarrow} = (P - P[X := 0])/X$, ce qui montre encore qu'une telle comatrice est dans $R[A]$.

Une dernière méthode : déduire de (12) que $C \in Z_A[X]$ où $Z_A = \{\, M \in \mathrm{Mat}_{n,n}(R) : AM = MA \,\}$; la substitution $X := A$ définit un morphisme $Z_A[X] \to Z_A$, ce qui permet de conclure comme avant.

Table de matières.

semestre pair 2010/2011, *Marc van Leeuwen*