Anneaux & arithmétique
(version non reprise)

Marc SAGE (collab. Michel WIGNERON)

20 août 2022

Table des matières

1 Anneaux, corps, algèbres

Dans l'ordre croissant de complexité des structures, l'anneau ("cartel d'entreprise") vient juste après le groupe (simple "regroupement") et juste avant le corps ("corps d'armée"). Il s'agit donc d'un groupe plus structuré – et le corps sera un anneau davantage structuré.

1.1 Anneaux, calcul dans les anneaux

DEF (anneau, anneau commutatif, notation A^*, groupe des inversibles $A^\times$). *On appelle* ***anneau***[1] *tout groupe additif muni d'une multiplication associative unifère et distributive sur l'addition. En d'autres termes, un anneau est un sextuplet* $\left(A, {}^{+,}_{\times,} {}^{0,}_{1} {}^{o}\right)$ *tel que*[2]

1. *le quadruplet* $(A, +, 0, o)$ *est un groupe additif*[3] *;*
2. *le triplet* $(A, \times, 1)$ *est un monoïde multiplicatif;*
3. $\times$ *se distribue sur* $+$*, au sens où chaques éléments* a, b, λ, μ *de* A *vérifient les égalités*
$$\lambda(a+b) = \lambda a + \lambda b \text{ et } (\lambda+\mu)a = \lambda a + \mu a.$$

Soit A *un anneau. L'anneau* A *est qualifié de* ***commutatif*** *lorsque sa multiplication*[4] *l'est. Le* ***groupe des inversibles*** *est le groupe* $A^\times$ *des inversibles du monoïde* $(A, \times)$*. De plus, on abrégera*

$$A^* := A \setminus \{0\} .$$

Exemples (anneaux).
$\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{H}$, $\mathbb{K}^{\mathbb{N}}_{cv}$ (suites scalaires convergentes), tous commutatifs (sauf $\mathbb{H}$).
$C^n(I, \mathbb{K})$ et $D^n(I, \mathbb{K})$ (fonctions scalaires de classe C^n, resp. n fois dérivables, pour chaque intervalle réel I et chaque $n \in \overline{\mathbb{N}}$).
Le quotient ${}^{\mathbb{Z}}\!/_{n}$ muni de la multiplication $\left(\overline{a}, \overline{b}\right) \mapsto \overline{ab}$ commutative (*cf.* section 1.7) (pour chaque naturel n)
Soit E un espace vectoriel. L'ensemble $L(E)$ des endomorphismes de E est alors un anneau pour la composition, non commutatif (sauf si E est inclus dans une droite).
Soient A un anneau et n un naturel. Forment alors des anneaux les matrices de $M_n(A)$, les fonctions de A^S (pour chaque ensemble S), les polynômes de $A[X]$ et ceux de $A[X_1, X_2, ..., X_n]$ mais pas ceux de $A_n[X]$.
Chaque singleton est un anneau où $1 = 0$, appelé un ***anneau nul*** (ou ***trivial***).

PROP (règles de calcul). *Soit* A *un anneau et soient* $a, b \in A$*.*

[1] en anglais : *ring*
[2] *Mméno* : on retrouve les quatre axiomes d'un espace vectoriel en remplaçant la multiplication interne de l'anneau par celle externe de l'espace vectoriel.
[3] En pratique, on ne mentionne jamais l'opposition $a \mapsto -a$ de l'anneau.
[4] En général, toute précision sur la structure d'un anneau concernera sa *multiplication*, l'addition étant déjà bien dotée avec sa structure de groupe.

1. *L'addition de A est abélienne*[5] :

$$a+b=b+a.$$

2. *Le zéro de A est absorbant pour la multiplication, au sens où*

$$a0=0=0a.$$

3. *On a la "règles des signes"*[6] :

$$(-a)\,b=-ab=a\,(-b)\ \ et\ \ (-a)\,(-b)=ab.$$

DEM (comme pour les espaces vectoriels)

1. On utilise l'associativité de $+$ et les deux distributivités de $\times$ pour écrire

$$\begin{aligned} & a+b+a+b=1\boxed{a+b}+1\boxed{a+b}=(1+1)\boxed{a+b} \\ = \ & \boxed{1+1}(a+b)=\boxed{1+1}a+\boxed{1+1}b=a+a+b+b\,; \end{aligned}$$

   il reste à soustraire a à gauche et b à droite.

2. On développe $0a=(0+0)\,a=0a+0a$ et l'on soustrait $0a$ (*idem* pour $a0$).

3. On factorise $ab+(-a)\,b=(a+(-a))\,b=0b=0$, ce qui montre que ab et $(-a)\,b$ sont opposés l'un de l'autre (*idem* pour $a\,(-b)$). On en déduit $(-a)\,(-b)=-\,(-ab)=ab$.

On renvoie au cours de première année pour la combinatoire du calcul dans les anneaux. Rappelons au besoin deux choses.

1. L'associativité et la commutativité de l'addition permettent (comme dans chaque groupe abélien) de *partitionner le domaine de sommation* comme on le souhaite, toujours *suivant ce que suggère la sommande*[7] (donc pas seulement en droites horizontales et verticales !). Formellement, ayant fixé une famille (a_i) indexée par un ensemble fini I partitionné en $\coprod_k I_k$, au niveau des sommes ce partitionnement s'écrit

$$\sum_{i\in I} a_i=\sum_k\sum_{i\in I_k} a_i.$$

2. Comme l'indique la collégienne égalité $(a+b)\,(c+d)=ac+ad+bc+bd$, *pour développer un produit de sommes, on pioche dans chaque somme-facteur*

[5] Ce qui justifie *a posteriori* la notation additive. Traditionnellement, l'addition des anneaux (comme celle des espaces vectoriels) est imposée abélienne par définition. Cette mini-preuve montre que cette imposition est inutile dans les anneaux unifères (comme dans les espaces vectoriels). Elle ne l'est toutefois pas dans les "anneaux sans unité" (appelés ***pseudo-anneaux***).

[6] En particulier, opposer revient à multiplier par -1.

[7] Développer un produit de polynômes suggère par exemple une partition en droites "diagonales" de pente -1.

un terme, on multiplie les termes choisis, puis l'on somme les produits ainsi formés. Cette combinatoire peut s'écrire[8]

$$\text{pour trois sommes :} \quad \sum_{x\in X} a_x \sum_{y\in Y} b_y \sum_{z\in Z} c_z = \sum_{X\times Y\times Z} a_x b_y c_z$$

$$\text{et plus généralement :} \quad \prod_{i\in I} \sum_{x\in X_i} a_i^x = \sum_{x\in \prod X_i} \prod_{i\in I} a_i^{x(i)}$$

$$\text{(cas particulier :} \quad \prod_{i\in I} \sum_{j\in J} a_i^j = \sum_{j\in J^I} \prod_{i\in I} a_i^{j(i)}\text{).}$$

Un test suffisant pour prétendre savoir calculer dans les anneaux en classes préparatoires consiste à prouver à la main que le déterminant préserve la multiplication, *uniquement* à l'aide de la définition polynomiale (aussi appelée *règle de Sarrus*).

Remarque. La règle des signes donne l'égalité $(-1)^2 = 1$, ce que montre que ± 1 sont des racines carrées de l'unité. Mais il peut y en avoir d'autres : par exemple, dans l'anneau séquentiel $\mathbb{R}^{\mathbb{N}}$, chaque élément de $\{-1,1\}^{\mathbb{N}}$. Explication : l'implication $(a-1)(a+1) = 0 \implies \begin{cases} a-1=0 \\ \text{ou} \\ a+1=0 \end{cases}$ n'est pas valable dans chaque anneau. Elle le sera dans chaque anneau *intègre*[9], en particulier dans chaque corps (où les racines carrées de l'unité sont bien ± 1).

Exercice d'application

Montrer que chaque anneau est nul ssi son unité vaut son zéro, ou encore ssi son zéro est inversible.

Soit A un anneau. Si A est un singleton, ses éléments coïncident alors, en particulier 1 et 0. Puisque $1 \in A^\times$, l'égalité $1 = 0$ implique l'inversibilité de 0. Enfin, vu le caractère absorbant de 0, son inversibilité implique pour chaque $a \in A$ les égalités $a = a1 = a00^{-1} = 0$, d'où l'implication $0 \in A^\times \implies A \subset \{0\}$, l'appartenance $0 \in A$ montrant par ailleurs que la dernière inclusion est en fait une égalité.

1.2 Anneaux intègres, corps

Diviseurs-de-zéro.

Le "théorème des zéros" affirmant qu'« *un produit d'éléments non nuls reste non nul* » est martelé dès le collège dans les anneaux numériques usuels. Il est *faux* dans

[8] Une fonction $j \in \prod_{i\in I} J_i$ code une façon de piocher dans chacune des $|I|$ sommes-facteurs un terme parmi les $|J_i|$ de la i-ième somme $\sum_{j\in J_i} a_i^j$.

[9] *Mméno* : on serait tenté de qualifier de *fourbe* tout anneau trompant notre attente du "théorème des zéros" ; s'il nous trompe, il ne saurait être honnête, *intègre* !

les algèbres de matrices où il y a des nilpotents, par exemple la matrice $\left(\begin{smallmatrix}0&1\\0&0\end{smallmatrix}\right)$ de carré nul, ainsi que dans les anneaux produits où $\binom{1}{0}\binom{0}{1}=\binom{0}{0}$.

Lorsque 0 peut s'écrire comme produit de deux éléments *chacun non nuls*, un tel facteur est appelé un ***diviseur-de-zéro***. Le "théorème des zéros" s'énonce donc « *il n'y a pas de diviseurs-de-zéro* ». Nous mettons des traits d'union à dessein pour marquer la différence avec un *élément divisant zéro*, çàd un élément d tel que $\exists d', dd' = 0$, énoncé toujours valide (prendre $d' = 0$). Un élément divisant 0 n'est donc pas toujours[10] un diviseur-de-0 !

Regardons les anneaux où ce théorème est vérifié, çàd où les éléments non nuls forment une partie stable par multiplication.

PROP-DEF (intégrité et régularité, anneau intègre). Soit A un anneau.

La multiplication stabilise A^* ssi elle y est régulière. En d'autres termes, le "théorème des zéros" est vrai ssi on peut simplifier par n'importe quel élément non nul.

*Dans ces conditions, lorsque de plus A est non nul et commutatif, on le qualifie d'**intègre**.*

DEM

Supposons A^* stable par $\times$. Soit $a \in A$ non nul. Soient $\lambda, \mu \in A$ distincts : le produit de $\lambda - \mu$ et de a (tous deux dans A^*) est alors non nul, ce qui (en développant) se réécrit $\lambda a \neq \mu a$. Contraposer montre que l'on peut simplifier par a à droite. On raisonnerait de même à gauche.

Supposons A^* régulier. Soient $a, b \in A^*$. Si par l'absurde le produit ab était nul, simplifier l'égalité $ab = a0$ par a donnerait l'absurde nullité de b.

EG (anneaux intègres) Sont intègres les anneaux numériques usuels $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$. Si A dénote un anneau intègre, alors $A[X]$ est intègre (et réciproquement) et le degré d'un produit de polynômes vaut la somme de leurs degrés.

CEG (anneaux "fourbes") Chaque produit d'au moins deux anneaux (eg des fonctions complexes), chaque anneau possédant des nilpotents non nuls (endomorphismes dans un espace vectoriel[11], anneau commutatif des polynômes en une matrice nilpotente non nulle).

RQ (le magma A^*). Les conditions de la proposition précédente peuvent s'énoncer « $(A^*, \times)$ est un magma (régulier) ». Vu d'une part l'associativité de $\times$ et d'autre part les implications

$$A^* \text{ unifère} \Longrightarrow A^* \neq \emptyset \Longrightarrow A \neq \{0\} \Longrightarrow 1 \neq 0 \Longrightarrow 1 \in A^* \Longrightarrow A^* \text{ unifère},$$

l'intégrité de A s'énonce aussi « $(A^*, \times)$ est un monoïde abélien (régulier) ». Ajoutons encore de la structure en demandant à ce monoïde d'être un *groupe*.

PROP-DEF (corps). Soit $(A, +, \times)$ un ensemble muni de deux lois. *Il est appelé un **corps**[12] lorsque l'une des conditions suivantes équivalentes est vérifiée :*

[10] La définition officielle parle de *diviseur de zéro* (sans traits d'union), créant une confusion avec la notion générale de diviseur, d'où notre choix d'écriture avec traits d'union. Bien sûr, les diviseurs-de-zéro sont les diviseurs de zéro *non nuls*.

[11] En dimension au moins 2, un anneau d'endomorphismes non seulement possède des diviseurs-de-zéro mais est *avant tout non commutatif*, deux raisons pour sa non-intégrité.

[12] en anglais : *field* (litt. "champ" : Galois parlait, pour désigner certains corps, de « champs de rationalité »)

1. *A est un anneau non nul commutatif*[13] *où chaque élément non nul est inversible ;*
2. *A est un anneau commutatif tel que $A^\times = A^*$;*
3. *$(A, +)$ et $(A^*, \times)$ sont deux groupes abéliens tels que $\times$ se distribue sur $+$.*

DEM

$1 \implies 2$ La condition d'inversibilité s'écrit $A^* \subset A^\times$, l'inclusion réciproque $A \setminus A^* \subset A \setminus A^\times$ équivalant à la non-inversibilité de 0, çàd à la non-nullité de A (que l'on a).

$2 \implies 3$ $A^\times$ est toujours un groupe multiplicatif, donc (dans notre cas) A^* aussi.

$3 \implies 1$ Puisque A^* est un groupe, il est unifère, donc A est non nul (*cf* implications ci-dessus).

Résumé des structures multiplicatives (HP). Soit A un groupe additif sur lequel se distribue une multiplication : c'est un anneau ssi $(A, \times)$ est un monoïde. Si l'on "oublie" 0 pour considérer la structure multiplicative de A^*, cette dernière va alors refléter les propriétés additionnelles de l'anneau A :

structure de $(A^*, \times)$	A vérifie le "théorème des zéros"	A est non nul	A est intègre	A est un corps
magma (régulier)	✓			
monoïde (régulier)	✓	✓		
monoïde abélien (régulier)	✓	✓	✓	
groupe abélien	✓	✓	✓	✓

.

Par exemple, le fait qu'un groupe est en particulier un monoïde régulier reflète que *chaque corps est intègre.*

EG (corps)

$\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ (pas $\mathbb{H}$, algèbre à division non commutative)

$K(X)$ et $K(X_1, X_2, ..., X_n)$ pour chaque corps K et pour chaque naturel n

$\mathbb{Z}/p$ pour chaque premier p, corps noté $\mathbb{F}_p$ ("F" pour "field"). Sera démontré à la section 2.4.

Exercice d'application

Soit A un anneau intègre. Montrer alors[14] *l'égalité $A[X]^\times = A^\times$.*

Soient $a, b \in A$ tels que $ab = 1$. Cette égalité pouvant se voir[15] dans $A[X]$, les polynômes a et b sont inversibles, ce qui montre l'inclusion $A[X]^\times \supset A^\times$

[13] Sans la commutativité, on parlera d'***algèbre à division***, telle celle formée par les quaternions.

[14] *Abus usuel* : identifier chaque $a \in A$ avec le polynôme $a + 0X + 0X^2 + \cdots$ donne sens aux inclusions $A \subset A[X]$.

[15] Formellement, appliquer le morphisme de monoïdes multiplicatifs $a \mapsto (a, 0, 0, 0, ...)$ de A vers $A[X]$.

Soient P et Q dans $A[X]$ tels que $PQ = 1$ et notons $\binom{p}{q} := \binom{\deg P}{\deg Q}$. Le coefficient de degré $p+q$ du polynôme $PQ = 1$ est (à gauche) un produit d'éléments non nuls (par définition de p et q), donc est non nul (car A est intègre), tandis qu'il vaut (à droite) δ^0_{p+q}. La non-nullité de ce dernier Kronecker livre l'égalité $0 = p + q$, d'où les nullités de p et de q (entiers positifs) Les polynômes P et Q sont donc constants et l'hypothèse $PQ = 1$ conclut aux appartenances $P, Q \in A^\times$.

1.3 Anneaux produit & sous-anneaux

Comme dans les espaces vectoriels, pour montrer qu'un ensemble est un anneau, on montre souvent qu'il est un "sous-anneau" d'un anneau "de référence".

DEF - PROP (anneau produit). *Soit (A_i) une famille d'anneaux. Alors le produit $\prod A_i$ est un anneau pour les lois produit, appelé* ***anneau produit*** *des A_i.*

CP (anneau puissance). Lorsque la famille est constante, on retrouve les anneaux puissances A^I (de fonctions).

CP (anneau nul). Lorsque la famille est vide, le produit est un singleton : l'anneau nul.

DEM Un produit de groupes (resp. monoïdes) étant un groupe (resp. monoïde), le point (1) (resp. (2)) ci-dessus est établi et il suffit de montrer que la multiplication produit se distribue sur l'addition produit, ce qui est immédiat en raisonnant coordonnée par coordonnée[16].

RQ (produit de corps) $\boxed{\textit{Aucun produit de corps n'est un corps !}}$ (sauf dans le cas d'un seul[17] facteur) Deux bonnes raisons à cela :

1. un anneau produit n'est jamais intègre (sauf, éventuellement, dans le cas d'un seul facteur),
2. les inversibles d'un produit de corps sont (par l'exercice précédent) les fonctions ne s'annulant jamais, lesquelles ne coïncident jamais avec les fonctions non nulles tout court (sauf dans le cas d'un seul facteur).

DEF-PROP (sous-anneau). *Une partie d'un anneau en est un* ***sous-anneau*** *si elle en est*[18] *? ? ?résumé -> sg stable par $\times$ qui conteitn 1 ? ? ?*

A. *un sous-groupe additif et*

M. *un sous-monoïde multiplicatif,*

autrement dit si[19]

[16] on a même l'équivalence (inutile ici), à savoir qu'une loi produit se distribue sur un autre loi produit ssi chaque première loi "facteur" se distribue sur la deuxième loi "facteur" correspondante

[17] Un produit vide de corps est un singleton, donc ne peut vérifier $1 \neq 0$: par conséquent un produit de zéro corps n'est pas un corps.

[18] A et M pour « **a**ddition » et « **m**ultiplication »

[19] I et L pour « **i**ndividus » et « **l**ois »

I. *elle contient le zéro et le un*[20] *de cet anneau ;*

L. *elle est stable par l'addition, l'opposition et la multiplication de cet anneau.*

Cette partie est alors un anneau pour les lois induites par l'anneau de base.

DEM Soit $(A, +, \times)$ un anneau, soit S un sous-anneau de A. Alors S est un sous-groupe additif de A, *a fortiori* un groupe additif, et est un sous-monoïde multiplicatif de A, *a fortiori* un monoïde multiplicatif. Enfin, spécialiser l'axiome de distributivité en des éléments de S montre que la multiplication de S se distribue sur son addition.

Application. Dans les exemples d'anneaux donnés section 1.1 :
$\mathbb{K}^{\mathbb{N}}_{cv}$ est un sous-anneau de l'anneau puissance $\mathbb{K}^{\mathbb{N}}$;
$C^n(I, \mathbb{K})$ et $D^n(I, \mathbb{K})$ sont des sous-anneaux de l'anneau puissance $\mathbb{K}^I$.

RQ (faux sous-anneaux). Comme pour les monoïdes, une partie peut, sans être un sous-anneau, être un anneau avec les mêmes neutres (mais pour d'autre lois), ou bien pour les mêmes lois (mais avec d'autres neutres) :

1. La partie $\mathbb{R} \times \{0\}$ est un anneau pour les lois produit (d'unité $(1, 0)$), est stable par les lois de $\mathbb{R}^2$ mais n'en est pas un sous-anneau car ne contient pas son unité $(1, 1)$.
2. La partie $\mathbb{R} \times \{0, 1\}$ est un anneau ayant pour multiplication celle de $\mathbb{R}^2$ et pour addition en abscisse celle de $\mathbb{R}$ et en ordonnée la loi constante nulle (la distributivité revient alors à l'égalité réelle $0 = 0 + 0$), il contient les zéro et un de $\mathbb{R}^2$ mais n'en est pas un sous-anneau car n'est pas stable par l'addition de $\mathbb{R}^2$ (le double de $(0, 1)$ sort de $\mathbb{R} \times \{0, 1\}$).

DEF PROP (sous-corps). *Un* ***sous-corps*** *d'un anneau est un sous-anneau qui est un corps.*

Une partie k d'un corps K en est un sous-corps ssi

1. *k est un sous-groupe (additif) de K ;*
2. *k^* est un sous-groupe de K^*.*

DEM

Supposons que k est un sous-corps de K. Alors k en est un sous-anneau, *a fortiori* un sous-groupe additif. Par ailleurs, k en est un sous-monoïde multiplicatif, donc est un corps dont la multiplication est celle de K, donc la partie $k^* = k^\times$ est un groupe pour la loi du groupe K^*, donc est un sous-groupe de K^*.

Supposons réciproquement les conditions 1 et 2. La seconde implique (avec l'absorbance de 0) que k est un sous-monoïde multiplicatif de K, donc (avec la première) que k est un sous-anneau de K. Cet anneau est par ailleurs un corps vu que $(k, +)$ et $(k^*, \times)$ sont des groupes (points 1 et 2).

EG-Exercice (un nombre algébrique). *Montrer que $\mathbb{Q}\left[\sqrt{7}\right]$ est un sous-corps de $\mathbb{C}$.*

[20] ne pas oublier l'unité !

SOL Il est clair que $\mathbb{Q}\left[\sqrt{7}\right]$ est un sous-groupe additif de $\mathbb{C}$ (comme $\mathbb{Q}[X]$). Montrons qu'est un groupe la partie $G := \mathbb{Q}\left[\sqrt{7}\right]^*$ formée des évaluations non nulles des polynômes rationnels en $\sqrt{7}$. Clairement, G contient 1 (polynôme constant) et est stable par multiplication (comme $\mathbb{Q}[X]\setminus\{0\}$) vu l'intégrité de $\mathbb{C}$. Soit par ailleurs $g \in G$, soit $P \in \mathbb{Q}[X]$ tel que $g = P\left(\sqrt{7}\right)$: quitte à effectuer une division euclidienne par $X^2 - 7$ (qui annule $\sqrt{7}$), on peut imposer $\deg P < 2$. Soient donc $a, b \in \mathbb{Q}$ tels que $g = a + b\sqrt{7}$. L'inverse dans $\mathbb{C}^*$ de g se réécrit alors[21]

$$\frac{1}{g} = \frac{1}{a+b\sqrt{7}} = \frac{a-b\sqrt{7}}{\left(a-b\sqrt{7}\right)\left(a+b\sqrt{7}\right)} = \frac{a}{a^2-7b^2} + \frac{-b}{a^2-7b^2}\sqrt{7},$$

lequel reste bien dans G.

On pourrait généraliser en remplaçant $\sqrt{7}$ par n'importe quelle complexe ***algébrique***, çàd solution d'une équation algébrique (non triviale), çàd annulé par un polynôme non nul (*cf.* exercices ? ? ?). Nous aurions pour cela besoin d'autres outils arithmétiques.

RQ (corps des fractions d'un anneau intègre) (HP). Une réciproque forte de l'exercice est valide, au sens où *chaque anneau intègre peut être "plongé" dans un corps*, le plus petit tel corps (à "isomorphisme" près) s'appelant le ***corps des fractions*** de l'anneau de base. Par exemple :

1. le corps $\mathbb{Q}$ peut être construit comme le corps des fractions de l'anneau intègre $\mathbb{Z}$.
2. le corps $A(X)$ pour chaque anneau intègre A peut être construit comme le corps des fractions de l'anneau intègre $A[X]$.

Sous-anneau engendré (HP). Comme dans les groupes et monoïdes, on montrerait (ayant fixé un anneau) que

1. *l'anneau plein est un sous-anneau,*
2. *l'ensemble des sous-anneaux est stable par intersection quelconque,*
3. *l'intersection des sous-anneaux incluant une partie donnée est (description "externe") le plus petit sous-anneau incluant cette partie (appelé le* ***sous-anneau engendré*** *par cette partie).*

Seule change, comparée aux cas des monoïdes ou des groupes, la description "interne". Dans le cas des anneaux, *le sous-anneau engendré par une partie est constitué des polynômes en les éléments de cette partie à coefficients relatifs*[22] :

$$\textit{dans les anneaux}^{23} : \langle G\rangle = \mathbb{Z}[G] := \left\{ P(g) \ ; \quad \begin{array}{c} n \in \mathbb{N},\ g \in G^n \\ P \in \mathbb{Z}[X_1, X_2, ..., X_n] \end{array} \right\}.$$

[21] La présence au dénominateur du réel $a - b\sqrt{7}$ est légitimée par l'irrationalité de $\sqrt{7}$.

[22] Le sous-anneau de $\mathbb{Z}[X]$ engendré par l'élément X est lui-même, d'où la cohérence de la notation "entre crochets".

[23] La lettre "G" utilisée rappelle que la partie entre chevrons est **g**énératrice (de son engendré).

Par exemple, le sous-anneau de $\mathbb{R}$ engendré par $\sqrt{7}$ vaut $\mathbb{Z}+\mathbb{Z}\sqrt{7}$, le sous-anneau de $\mathbb{C}$ engendré par $j := e^{\frac{2\pi i}{3}}$ vaut $\mathbb{Z}+\mathbb{Z}j+\mathbb{Z}j^2$. En non-commutatif, l'anneau $M_n(\mathbb{Z})$ est engendré par la matrice nilpotente $\begin{pmatrix} 0 & 0 \\ I_{n-1} & 0 \end{pmatrix}$ et sa transposée (c'est un exercice de pure algèbre matricielle). Enfin, la partie vide engendre le plus petit sous-anneau (appelé pour cela le ***sous-anneau premier***), formé des itérés de l'unité :

$$\textit{dans les anneaux} : \langle \emptyset \rangle = \langle 0, 1 \rangle = \mathbb{Z}[1] = \mathbb{Z} \cdot 1.$$

Sous-corps engendré (HP). On peut reprendre tout le paragraphe précédent en remplaçant « anneau » par « corps», seule la description interne change : *le sous-corps engendré par une partie est constitué des quotients de polynômes en les éléments de cette partie à coefficients relatifs*[24] :

$$\textit{dans les corps} : \langle G \rangle = \mathbb{Z}(G) := \left\{ \frac{P(g)}{Q(g)} \; ; \quad \begin{array}{c} n \in \mathbb{N},\ g \in G^n,\ Q(g) \neq 0 \\ P, Q \in \mathbb{Z}[X_1, X_2, ..., X_n] \end{array} \right\}.$$

De même, la partie vide engendre le plus petit sous-corps, appelé le ***sous-corps premier***.

Exercices d'application

1. *Soient A un anneau et S un e*nsemble. *Quels sont les inversibles de l'anneau A^S ? Que dire quand A est un corps ?*
2. *Soit $(A, +, *)$ un anneau et soit $S \subset A$. Traduire en français les trois relations suivantes et montrer leur équivalence :*

   (a) $\begin{matrix} S+S \\ S*S \end{matrix} \subset S \begin{matrix} \ni 0, 1 \\ \supset -S \end{matrix}$;

   (b) $\begin{matrix} S \pm S \\ S*S \end{matrix} \subset S \ni 1$;

   (c) $\begin{matrix} S+S \\ S*S \end{matrix} \subset S \ni -1.$

3. *Montrer que l'intégrité passe aux sous-anneaux, au sens où les sous-anneaux d'un anneau intègres sont intègres.*

---

1. Le groupe des inversibles d'un produit étant le produit des groupes des inversibles, on a les égalités $\left(A^S\right)^\times = \prod_S A^\times = A^{\times S}$. On trouve ainsi les fonctions ne prennant que des valeurs inversibles. Lorsque A est un corps, on obtient les fonctions ne s'annulant jamais.

[24] Le sous-corps de $\mathbb{Z}(X)$ engendré par l'élément X est lui-même, d'où la cohérence de la notation "entre parenthèses".

2. Les relations 2a signifient que S est stable par addition, multiplication, opposition et contient les unité et zéro de A, çàd que S est un sous-anneau. De même, les relations 2b expriment que la partie S est stable par addition, soustraction multiplication et contient l'unité de A. Enfin, les relation 2c disent que S est stable par addition, multiplication et contient moins l'unité.

   $\boxed{\text{2a}\Longrightarrow\text{2b}}$ La partie S est (en tant que sous-groupe additif) stable par soustraction, d'où l'inclusion $S - S \subset S$.

   $\boxed{\text{2b}\Longrightarrow\text{2c}}$ La partie S contient la différence $1-1=0$, donc contient $0-1=-1$.

   $\boxed{\text{2c}\Longrightarrow\text{2a}}$ La partie S contient le produit $(-1)(-1)=1$, donc contient la somme $1+(-1)=0$, *a fortiori* pour chaque $s \in S$ contient la différence $0-s=-s$, d'où l'inclusion $-S \subset S$.

   RQ – Cette exercice décrit les sous-anneaux en termes de lois "parties".

3. Soit A un sous-anneau d'un anneau intègre. Puisque ce dernier est commutatif, ses sous-monoïdes multiplicatifs le sont, donc A est commutatif. Le sous-anneau A contient par ailleurs 1 et 0, lesquels sont distincts dans chaque anneau intègre, donc est non nul. Soient enfin $a, b \in A$ tels que $ab = 0$: l'intégrité du gros anneau implique alors la nullité de a ou de b.

1.4 Morphismes d'anneaux

DEF (morphisme d'anneaux) *On appelle (**homo**)**morphisme d'anneaux** toute application entre anneaux qui est ? ? ?résumé : trois formules ? ? ?*

1. *un morphisme de groupes additifs et*
2. *un morphisme de monoïdes multiplicatifs,*

autrement dit qui respecte l'addition, la multiplication et l'unité[25].
*Un (**homo**)**morphisme de corps** est un morphisme d'anneaux entre corps.*

EGS Soit A un anneau.

1. L'inclusion canonique de chaque sous-anneau de A est un morphisme d'anneaux.
2. L'itération de l'unité $\left\{ \begin{array}{ccc} \mathbb{Z} & \longrightarrow & A \\ z & \longmapsto & z \cdot 1 \end{array} \right.$ est un morphisme d'anneaux.
3. L'évaluation (fonctionnelle) en un point donné est un morphisme d'anneaux de $A^S \longrightarrow A$ pour chaque ensemble S.
4. L'évaluation (polynomiale) en un point donné est un morphisme d'anneaux de $A[X_1, X_2, ..., X_n] \longrightarrow A$ pour chaque naturel n.
5. Chaque morphisme d'anneaux $\left\{ \begin{array}{ccc} A & \longrightarrow & B \\ a & \longmapsto & \overline{a} \end{array} \right.$ induit un morphisme d'anneaux $\left\{ \begin{array}{ccc} A[X] & \longrightarrow & B[X] \\ \sum a_n X^n & \longmapsto & \sum \overline{a_n} X^n \end{array} \right.$.

[25] Ne pas oublier l'unité !

EXO (morphisme de Frobenius) Soient A un anneau commutatif et p un premier tel que $p1 = 0$. *Montrer que l'élévation à la puissance p est un endomorphisme de l'anneau A.*

SOL La préservation de l'unité est triviale, celle de la multiplication découle de la commutativité : il reste l'addition. Soient $a, b \in A$. On veut la nullité de $(a+b)^p - a^p - b^p = \sum_{1 \leq n < p} \binom{p}{n} a^n b^{n-p}$, il suffirait celle de chaque itéré $\binom{p}{n}1$. Soit donc n un naturel de $[|1, p[$: puisque p est premier, il est étranger à n, donc l'égalité $p\binom{p-1}{n-1} = n\binom{p}{n}$ montrant $p \mid n\binom{p}{n}$ prouve (par GAUSS) la divisibilité $p \mid \binom{p}{n}$, d'où la nullité cherchée. ? ? ?séparer lemme ? ? ?

Comme pour les groupes et monoïdes, on définit un ***isomorphisme*** d'anneaux ainsi qu'un ***endomorphisme*** et un ***automorphisme*** d'un même anneau. Le ***noyau*** d'un morphisme d'anneaux est celui du morphisme *additif* associé, çàd est formé des éléments *annulés* par le morphisme. Si φ dénote un morphisme d'anneaux de source A, son noyau est noté

$$\operatorname{Ker} \varphi := \varphi^{-1}(\{0\}) = \{a \in A \ ; \ \varphi(a) = 0\}.$$

On montre de même que

1. *la composée de chaques morphismes d'anneaux (si elle fait sens) est un morphisme d'anneaux*,
2. *la réciproque de chaque isomorphisme d'anneaux est un isomorphisme d'anneaux*,
3. *l'identité est un morphisme d'anneaux*,

d'où l'on conclut pour chaque anneau A que

$$\begin{array}{c} \operatorname{End} A \textit{ est un monoïde dont le groupe} \\ \textit{des inversibles vaut } (\operatorname{End} A)^\times = \operatorname{Aut} A. \end{array}$$

Pareillement, on établirait que

1. *par chaque morphisme d'anneaux l'image directe de chaque sous-anneau source est un sous-anneau but,*
2. *par chaque morphisme d'anneaux l'image réciproque de chaque sous-anneau but est un sous-anneau source,*
3. *l'image de chaque morphisme d'anneaux est un sous-anneau*[26].

En revanche, le singleton nul ne contenant jamais[27] l'unité (sauf dans le cas d'un anneau nul),

$$\boxed{\textit{le noyau d'aucun morphisme d'anneaux n'est un sous-anneau}}$$

(sauf si l'anneau but est nul, auquel cas le noyau vaut tout l'anneau source) ;

[26] L'anneau source est un sous-anneau de lui-même.

[27] On peut être déçu mais certainement pas surpris : le noyau concerne la structure *additive*, la surprise serait plutôt qu'il se comporte "bien" vis-à-vis de la multiplication.

Ce noyau sera en revanche un *idéal*, notion arithmétique en fait bien plus intéressante que celle de sous-anneau[28]. Toutes les affirmations de ce paragraphe s'obtiennent en conjoignant celles prouvées dans les cadres des groupes et des monoïdes.

TH (lemme chinois). *Soient a et b deux naturels étrangers. Est alors un isomorphisme d'anneaux*

$$\left\{\begin{array}{ccc} \mathbb{Z}/_{ab} & \xrightarrow{\sim} & \mathbb{Z}/_{a} \times \mathbb{Z}/_{b} \\ \overline{z} & \longmapsto & (\widetilde{z}, \widehat{z}) \end{array}\right. .$$

DEM On sait déjà que l'application C ci-dessus est un isomorphisme de groupes additifs. Elle préserve par ailleurs la multiplication vu à $m, n \in \mathbb{Z}$ fixés les égalités

$$C(\overline{m})\, C(\overline{n}) = \left(\begin{smallmatrix}\widetilde{m} \\ \widehat{m}\end{smallmatrix}\right)\left(\begin{smallmatrix}\widetilde{n} \\ \widehat{n}\end{smallmatrix}\right) = \left(\begin{smallmatrix}\widetilde{m}\widetilde{n} \\ \widehat{m}\widehat{n}\end{smallmatrix}\right) = \left(\begin{smallmatrix}\widetilde{mn} \\ \widehat{mn}\end{smallmatrix}\right) = C(mn)\,.$$

EXO (plongement de corps) *Montrer que chaque morphisme de corps est injectif*[29]*.*

SOL Soit φ un morphisme de corps, soit $k \in \operatorname{Ker}\varphi$. Si k est non nul, son inverse ℓ fait sens et l'on peut écrire $1 = \varphi(1) = \varphi(k\ell) = \varphi(k)\,\varphi(\ell) = 0\varphi(\ell) = 0$, ce qu'on n'a pas dans le corps but.

RQ (corps & groupes) (HP) L'exercice qui précède montre qu'un morphisme de corps $k \hookrightarrow K$ se restreint en une application $k^* \longrightarrow K^*$ multiplicative. Réciproquement, pour chaques anneaux A et B, chaque application $A^* \longrightarrow B^*$ multiplicative se prolonge en une application $A \longrightarrow B$ également multiplicative. Par conséquent,

chaque application $k \longrightarrow K$ entre corps est un morphisme de corps
ssi les applications $\begin{array}{c} k \longrightarrow K \\ k^* \longrightarrow K^* \end{array}$ *font sens et sont des morphismes de groupes.*

On en déduirait, en utilisant uniquement[30] le langage des groupes, toutes les affirmations du paragraphe ci-dessus en remplaçant « anneau » par « corps ».

EXO (endomorphisme d'anneaux numériques). *Déterminer les endomorphismes du corps $\mathbb{Q}$, ceux du corps $\mathbb{R}$ et qui du corps $\mathbb{C}$ qui fixent $\mathbb{R}$.*

1. Un endomorphisme du corps $\mathbb{Q}$ est en particulier un endomorphisme du groupe additif $\mathbb{Q}$, donc est une homothétie ; devant par ailleurs préserver la multiplication, son rapport est un idempotent de $\mathbb{Q}$, à savoir 0 ou 1. Or le rapport nul est à exclure car notre endomorphisme doit préserver l'unité. Finalement, l'endomorphie de $\mathbb{Q}$ est triviale[31] : $\operatorname{End}\mathbb{Q} = \{\mathrm{Id}\}$.

[28] *Mnémo* : un idéal est l'équivalent chez les anneaux des sous-espaces vectoriels chez les espaces vectoriels. De fait, les noyaux de morphismes d'espaces vectoriels sont bien des sous-espaces vectoriels.

[29] On devra donc toujours penser un morphisme de corps comme une *inclusion*.

[30] Détail utile : si φ dénote un morphisme de corps, son injectivité permet d'écrire $\left\{\begin{array}{c} \varphi(S^*) = \varphi(S)^* \\ \varphi^{-1}(T^*) = \varphi^{-1}(T)^* \end{array}\right.$. pour chaque partie $\begin{array}{c} S \text{ source} \\ T \text{ but} \end{array}$.

[31] Affirmer $\operatorname{Aut} S = \{\mathrm{Id}_S\}$ pour une certaine structure S, c'est dire qu'on ne peut pas la déformer de l'intérieur tout en la préservant : on dit de manière imagée que la structure S est *rigide*.

2. Soit φ un endomorphisme du corps $\mathbb{R}$. Sa restriction à $\mathbb{Q}$ est alors un morphisme de groupes additifs, donc est (par un exercice sur les groupes) une homothétie. Son rapport est toujours un idempotent (de $\mathbb{R}$ cette fois) non nul, à savoir 1, de sorte que $\varphi = \mathrm{Id}$ sur les rationnels.

   Montrons par ailleurs que φ croît[32], ce qui "bouchera les trous". Étant donnés deux réels a et b rangés dans ce ordre, abréger $r := \sqrt{b-a}$ permet d'écrire

   $$\varphi(b) = \varphi\left(a + r^2\right) = \varphi(a) + \varphi(r)^2 \geq \varphi(a),$$ d'où la croissance annoncée.

   Concluons. Soit $a \in \mathbb{R}$, soient (q_n^-) et (q_n^+) deux suites resp. croissante et décroissante de rationnels tendant vers a. Pour chaque naturel n, les comparaisons $q_n^- \leq a \leq q_n^+$ donnent par croissance de φ celles $q_n^- \leq \varphi(a) \leq q_n^+$, d'où en prenant la limite celles $a \leq \varphi(a) \leq a$ et l'égalité voulue $\varphi(a) = a$. Finalement, le seul endomorphisme du corps $\mathbb{R}$.

3. Soit φ un endomorphisme du corps $\mathbb{C}$ qui fixe $\mathbb{R}$. Notons $i' := \varphi(i)$: vu les égalités $i'^2 = \varphi(i)^2 = \varphi\left(i^2\right) = \varphi(-1) = -1$, le complexe i' vaut $\pm i$. Soient par ailleurs $a, b \in \mathbb{R}$: l'image du complexe $a+bi$ vaut alors $\varphi(a)+\varphi(b)\varphi(i) = a+bi'$, ce qui montre que φ est ou bien l'identité, ou bien la conjugaison, lesquelles conviennent réciproquement. Finalement, le groupe cherché (car c'est un groupe) est isomorphe à $\mathbf{U}_2$.

   Remarque – **Culture (HP)**. Étant donnée une extension de corps $k \subset K$, l'ensemble des automorphismes de K qui fixent k est un groupe appelé le ***groupe de Galois*** de l'extension ${}^{K}\!/_{k}$. Nous venons par exemple de montrer $\mathrm{Gal}\left({}^{\mathbb{C}}\!/_{\mathbb{R}}\right) \cong \mathbb{U}_2$.

1.5 Idéaux

DEF (idéal). Soit A un anneau commutatif. *Un **idéal** de A est un sous-groupe additif de A stable par multiplication par chaque élément de A, çàd est une partie non vide (de A) stable par "combinaisons linéaires"*[33] *(à coefficients dans A).*

RQ (idéaux et lois "parties"). En termes de lois "parties", une partie $I \subset A$ est un idéal ssi[34] $I + I \subset I \underset{\ni 0}{\supset} AI$.

RQ (idéaux en non commutatif) (HP). Si A n'est plus commutatif, on préciserait ***à gauche*** ou ***à droite*** à côté de « idéal » et de « multiplication », un idéal ***bilatère*** étant un idéal des deux côtés. Par exemple, c'est un exercice de pure algèbre matricielle que de déterminer les idéaux bilatères de l'anneau $L(E)$ pour chaque espace vectoriel E de dimension finie.

[32] L'idée est qu'une comparaison $a \leq b$ s'exprime par une positivité $b - a \geq 0$, laquelle s'exprime dans le langage des anneaux : $\exists r \in \mathbb{R},\ b - a = r^2$. Il est donc attendu qu'un morphisme d'anneaux préserve les comparaisons.

[33] Commencer dès à présent à penser un idéal comme un sous-espace vectoriel, l'analogie aide.

[34] Comme dans les espaces vectoriels, la stabilité par opposition découle de celle par multiplication par -1.

Voyons à présent deux familles d'idéaux de référence (les idéaux *principaux* et les *noyaux* de morphismes d'anneaux) ainsi que trois moyens d'engendrer de nouveaux idéaux (par *somme*, *intersection* ou *idéal engendré*).

PROP DEF (idéal principal, anneau principal (HP)). Soit A un anneau commutatif.

Pour chaque $a \in A$, la partie $(a) := aA = Aa$ est un idéal[35]*, appelé l'**idéal principal** engendré par a.*

*L'anneau A est dit **principal** s'il est intègre et quand chacun de ses idéaux est principal.*

DEM Soit $a \in A$. La distributivité de $\times$ sur $+$ montre que multiplier par a est un morphisme de groupes additifs, donc son image (a) est un sous-groupe additif de A. Soient par ailleurs $\lambda \in A$ et $i \in (a)$, soit $\mu \in A$ tel que $i = \mu a$: alors $\lambda i = \lambda(\mu a) = (\lambda\mu)\, a \in (a)$.

Par exemple, les idéaux principaux engendrés resp. par 0 et par 1 sont l'***idéal nul*** $(0) = \{0\}$ et l'***idéal plein*** $(1) = A$. L'ensemble des multiples d'un même relatif (resp. polynôme) est un idéal de $\mathbb{Z}$ (resp. $\mathbb{K}[X]$). Réciproquement, un idéal étant en particulier un sous-groupe additif, nous avons déjà établi la principalité de $\mathbb{Z}$ (un théorème à venir énoncera celle de $\mathbb{K}[X]$).

Exercice (idéal sous-anneau). *Montrer que chaque idéal est un sous-anneau ssi il vaut l'anneau plein*[36]*, ou encore ssi il contient un inversible.*

SOL Soit I un idéal. Si I est un sous-anneau, il contient alors l'unité 1, qui est inversible. Si I contient un inversible i, alors pour chaque a de l'anneau l'idéal I va contenir $\left(ai^{-1}\right) i = a$, donc va inclure tout l'anneau. Enfin, l'anneau plein (1) est un idéal.

EXO (idéaux & corps). *Montrer que chaque anneau commutatif*[37] *est un corps ssi il possède exactement deux idéaux, (0) et (1). Retrouver le fait qu'un morphisme de corps est injectif.*

SOL

Soit k un corps. Puisque $1 \neq 0$, ses idéaux nul et plein sont distincts. Par ailleurs, un idéal non nul contient un élément non nul, à savoir un inversible, donc vaut l'idéal plein.

Soit réciproquement A un anneau dont les deux seuls idéaux sont $\{0\}$ et A. Puisque ces idéaux sont distincts, A est non nul. Soit par ailleurs $a \in A^*$: l'idéal (a) est alors non nul, donc vaut tout A, donc contient 1, ce qui s'écrit $1 \in Aa$, d'où l'inversibilité de a.

Soit enfin φ un morphisme de corps. Son noyau est alors un idéal du corps source, donc ou bien est nul (auquel cas on a gagné), ou bien contient 1 dont l'image 1 ne peut être nulle dans le corps but.

[35] Les *parenthèses* signalent un engendré au sens des *idéaux*, pas au sens des sous-anneaux (ce qu'indiqueraient des chevrons).

[36] Les notions de sous-anneau et d'idéal sont "orthogonales" : il n'y a qu'un seul "objet" situé à leur "intersection".

[37] La commutativité est indispensable, comme le montre l'exercice des anneaux matriciels dont les seuls idéaux bilatères sont ceux nul et plein.

PROP (idéaux & noyaux). *Le noyau de chaque morphisme d'anneaux est un idéal.*

DEM[38] Soit $\varphi : A \longrightarrow B$ un morphisme d'anneaux. En tant que noyau d'un morphisme entre groupes additifs, $\operatorname{Ker}\varphi$ est déjà un sous-groupe additif de A. Par ailleurs, étant donnés un $\lambda \in \lambda$ et un $k \in \operatorname{Ker}\varphi$, on aura $\varphi(\lambda k) = \varphi(\lambda)\varphi(k) = \varphi(\lambda)0 = 0$, d'où $\lambda k \in \operatorname{Ker}\varphi$.

RQ (HP) On peut réciproquement réaliser tout idéal comme le noyau d'un morphisme, celui de la projection canonique *modulo* cet idéal (*cf.* section 1.7).

PROP (sommes et intersections d'idéaux). *L'ensemble des idéaux d'un même anneau est stable par addition "parties" (même infinie) et par intersection (même infinie).*

DEM La même que pour les espaces vectoriels.

DEF PROP (idéal engendré[39]**).** Soit G une partie d'un anneau A. ***L'idéal engendré*** *par G est le plus petit idéal de A incluant G, défini (de façon "externe") par l'intersection (G) des idéaux incluant G. De façon "interne", (G) est formée des combinaison linéaires d'éléments de G (à coefficients dans A).*

CP (idéal finiment engendré) L'idéal engendré par une partie finie s'explicite aisément :

$$(a, b, c, ..., z) = (a) + (b) + (c) + \cdots + (z)\,.$$

Appliquons aux exemples de morphismes donnés section 1.4. Les inclusions canoniques de sous-anneaux ne sont pas très intéressantes : étant injectives, leurs noyaux sont nuls.

EG (fonctions & polynômes s'annulant en un lieu donné) Soit S un ensemble, soit $s \in S$. Les fonctions de $\mathbb{C}^S$ s'annulant en s constituent le noyau du morphisme "évaluation en s", donc forment un idéal $\operatorname{Ker}\operatorname{eval}_s$. Par conséquent, les fonctions s'annulant (au moins) sur un lieu $L \subset S$ constituent l'intersection des idéaux $\operatorname{Ker}\operatorname{eval}_\ell$ pour ℓ décrivant L, donc forment aussi un idéal de $\mathbb{C}^S$.

De même, les polynômes de $\mathbb{Z}[X]$ s'annulant sur une partie fixée d'un anneau forment un idéal de $\mathbb{Z}[X]$ comme intersection des noyaux des évaluations en les éléments de cette partie.

EG (caractéristique d'un anneau, sous-anneau premier) (HP). Soit A un anneau.

Le noyau de l'itération de l'unité est un idéal de $\mathbb{Z}$, donc principal, donc vaut $c\mathbb{Z}$ pour un certain naturel c appelé la ***caractéristique*** de A. Par exemple, pour chaque premier p, la caractéristique de $\mathbb{F}_p$ vaut p.

EXO (caractéristique première). *Montrer que la caractéristique de chaque anneau intègre est première ou nulle, puis que la caractéristique de chaque corps fini est première.*

[38] La démonstration qui suit est exactement celle de l'énoncé où l'on a remplacé « anneau », « idéal » et « multiplication externe » par « espace vectoriel », « sous-espace vectoriel » et « multiplication interne ».

[39] Cette définition-proposition est l'analogue dans les anneaux de celle d'un sous-espace vectoriel engendré.

SOL Soit A un anneau intègre et notons c sa caractéristique, supposée non nulle. Soient $a, b \in \mathbb{N}$ tels que $ab = c$. Appliquer le morphisme ci-dessus donne dans A les égalités $(a1)(b1) = (c1) = 0$, d'où (par intégrité) la nullité de $a1$ ou de $b1$, mettons $a1 = 0$. Alors a est dans le noyau $c\mathbb{Z}$ du morphisme $z \mapsto z1$, d'où la divisibilité $a \mid c$. Pour conclure, observons d'une part que chaque anneau de caractéristique nulle inclut (un sous-anneau isomorphe à) $\mathbb{Z}$ et est donc infini, d'autre part que chaque corps est intègre.

L'image $\mathbb{Z} \cdot 1 = \mathbb{Z}[1]$ de ce morphisme est le plus petit sous-anneau de A, appelé le ***sous-anneau premier*** de A et est isomorphe à $\mathbb{Z}/c$. Ainsi, chaque anneau de caractéristique nulle "inclut" $\mathbb{Z}$ et chaque corps de caractéristique positive[40] p "inclut" un $\mathbb{Z}/p = \mathbb{F}_p$.

TH (principalité des polynômes "corporels"). Soit k un corps. *Alors l'anneau $k[X]$ est principal.*

DEM Tout d'abord, le corps k étant intègre, l'anneau $k[X]$ est intègre. Soit ensuite I un idéal[41] de $k[X]$. Si I est nul, il vaut (0) qui est principal. Supposons donc I non nul. Alors la partie $D := \{\deg i \ ; \ i \in I \setminus \{0\}\}$ de $\mathbb{N}$ est non vide, appelons m son minimum et évoquons un $\iota \in I$ tel que $m = \deg \iota$. La stabilité de I par multiplication quelconque montre l'inclusion $(\iota) \subset I$; établissons la réciproque. Soit $i \in I$: une division euclidienne par ι (qui est bien non nul) nous donne deux polynômes Q et R tels que $i = Q\iota + R$ avec $\deg R < \deg \iota = m$. Alors le polynôme $R = i - Q\iota$ reste dans l'idéal I : s'il était non nul, son degré tomberait dans la partie D, d'où l'absurde comparaison $\deg R \geq \min D = m$. La nullité de R permet de conclure à l'appartenance $i = Q\iota \in (\iota)$.

***EXO (principalité[42] de $A[X]$).** Soit A un anneau. *Montrer que $A[X]$ est principal ssi A est un corps.* (On pourra établir pour un sens l'égalité $(a)+(X) = (1)$.)

SOL On vient de voir le sens réciproque. Supposons $A[X]$ principal. Alors A est intègre comme sous-anneau de l'anneau intègre $A[X]$. Soit par ailleurs $a \in A^*$. La somme $(a)+(X)$ étant un idéal, on peut évoquer un générateur $g \in A[X]$ de ce dernier. Puisque $a \in (a) + (X) = (g)$, il y a un polynôme p tel que $a = gp$, ce qui montre par intégrité la constance[43] de g (et p). Soit de même Q un polynôme tel que $X = gQ$: dériver puis évaluer en 0 donne l'égalité $1 = gQ'(0)$, d'où l'appartenance $1 \in (g) = (a) + (X)$. Soient donc deux polynômes U et V tels que $1 = Ua + VX$: évaluer en 0 donne l'égalité $1 = U(0)\, a$, concluant à l'inversibilité de a.

***EXO (ceg principal).** Soit k un corps. *Montrer que $k[X, Y]$ n'est pas principal.*

SOL Supposons le contraire. Soit P un générateur de l'idéal[44] $(X) + (Y)$. Ce dernier (P) incluant (X) et (Y), le polynôme P divise X et Y. L'idée est de montrer à la main que X et Y sont étrangers : alors P sera inversible, donc engendrera l'idéal

[40] Dans ce contexte, cet anglicisme signifie "*strictement* positive", donc première.

[41] *Micro-analyse* : si I est principal, mettons $I = (\iota)$, alors ι est de degré minimal parmi les éléments non nuls de I.

[42] Cet exercice montre que l'hypothèse "corporelle" dans le théorème précédent était nécessaire.

[43] *Rappel* : si A est intègre, alors $A[X]$ est intègre et le degré d'un produit vaut la somme des degrés des facteurs.

[44] *cf.* section 2.2 pour une interprétation en termes de p. g. c. d.

plein, d'où $1 \in (P) = (X) + (Y)$, donc 1 sera combinaison linéaire de X et de Y, d'où en évaluant en $(0,0)$ la contradiction $1 = 0$.

Soient $U, V \in k[X,Y]$ tels que $\begin{cases} X = PU \\ Y = PV \end{cases}$. Notons R l'anneau intègre $k[Y]$ et raisonnons dans $R[X] = k[Y][X]$ (clairement isomorphe à $k[X,Y]$). Dans l'égalité $Y = PV$, le terme de gauche est constant dans $R[X]$, donc de degré nul, donc P et V sont de degré nul dans $R[X]$, donc P y est constant, çàd P n'a pas de termes en Y. Échanger les rôles de X et de Y montrerait que P n'a pas non plus de termes en X, donc est constant dans $k[X,Y]$. N'étant par ailleurs pas nul (sinon X et Y le seraient), il est inversible.

RQ (idéaux & sous-espaces vectoriels) (HP) Si l'on remplace dans la définition d'un espace vectoriel le corps de base par un anneau (on parle alors de ***module***[45]), les idéaux d'un anneau A en sont les sous-A-modules, ce qui explique les fortes analogies entre idéaux et sous-espaces vectoriels. Par exemple, les idéaux principaux pourront être vus comme des "droites vectorielles", les idéaux finiment engendrés (on dit aussi ***de type fini***) comme des "sous-espaces vectoriels de dimension finie" et les idéaux ***maximaux*** (idéaux stricts maximaux pour l'inclusion) comme des "hyperplans vectoriels". De même, chaque groupe abélien peut-être vu comme un $\mathbb{Z}$-module, ce qui éclaire la présence de sommes de "droites entières" dans les groupes abéliens (à l'instar de $\mathbb{Z} + \mathbb{Z}\sqrt{2}$ dans $\mathbb{R}$).

1.6 Algèbres

DEF-PROP (algèbre, morphisme d'algèbres, sous-algèbre). *Une **algèbre** est un anneau qui est aussi un espace vectoriel*[46] *et dont les multiplications (interne et externe) sont compatibles*[47]*. En d'autres termes, une algèbre est un sextuplet $\left(A, \overset{+}{0}, \overset{\times}{1}, \cdot\right)$ tel que :*

1. $\left(A, \overset{+}{0}, \overset{\times}{1}\right)$ *est un anneau ;*
2. $\left(A, \overset{+}{0}, \cdot\right)$ *est un espace vectoriel ;*
3. $\times$ *et* $\cdot$ sont *compatibles au sens de l'"associativité" suivante : pour chaque scalaire λ et pour chaques vecteurs a et b, on a les égalités*

$$\lambda \cdot (a \times b) = (\lambda \cdot a) \times b = a \times (\lambda \cdot b)\text{, produit noté tout simplement } \lambda ab.$$

*Un (**homo**)**morphisme** d'algèbres est un morphisme d'anneaux et un morphisme d'espaces vectoriels entre algèbres*[48]*.*

*Une partie d'une algèbre en est une **sous-algèbre** si elle en est*

[45] Malgré son langage similaire, la théorie des modules est très différente de celle des espaces vectoriels. Les deux principales différences sont d'une part la *torsion* (annulation d'un "vecteur" après itération), d'autre part la présence de sous-modules ("sous-espaces vectoriels") *sans supplémentaire*.

[46] Si l'on souhaite préciser le corps de base (de l'espace vectoriel), on parlera alors de ***k*-algèbre** (si l'espace vectoriel associé est un k-espace vectoriel).

[47] Dans son *Moderne Algebra*, VAN DER WARDEN parlait au lieu d'algèbres de *systèmes hypercomplexes*, sans doute pour signaler l'entremêlement de plusieurs structures.

[48] Une application entre algèbres est donc un morphisme ssi elle préserve l'unité (*à ne pas oublier !*), l'addition et les deux multiplications.

A. *un sous-anneau et*

E. *un sous-espace vectoriel,*

autrement dit si

I. *elle contient le zéro et le un*[49] *de cette algèbre ;*

L. *elle est stable par combinaisons linéaires et par produits.*

Cette partie est alors une algèbre pour les lois induites par l'algèbre de base.

DEM Soit $(A, +, \times, \cdot)$ une algèbre, soit S une sous-algèbre de A. Alors S est un sous-anneau de A, *a fortiori* un anneau, et est un sous-espace vectoriel de A, *a fortiori* un espace vectoriel. Enfin, spécialiser l'axiome d'"associativité" en des éléments de S montre que les multiplications de S sont compatibles.

Exemples (algèbres & co). Soient k un corps, P une partie de $\mathbb{C}$ et p un point de P.

1. Sont alors des k-algèbres : le corps k lui-même et ses puissances, l'anneau $k[X]$ des polynômes, celui $M_n(k)$ des matrices (pour chaque naturel n) et celui $L(E)$ des endomorphismes de chaque k-espace vectoriel E.
2. Quand $k = \mathbb{K}$, l'espace vectoriel $\mathbb{K}^{\mathbb{N}}_{\text{cv}}$ des suites scalaires convergentes est une sous-algèbre de l'algèbre puissance $\mathbb{K}^{\mathbb{N}}$. De même, l'espace vectoriel des fonctions de $\mathbb{K}^P$ admettant une limite en p est en une sous-algèbre.
3. Dans chaque algèbre produit (par exemple $\mathbb{K}^P$), la projection sur une coordonnée fixée – ou, en termes fonctionnels, l'évaluation en point fixé – est un morphisme d'algèbres.
4. Dans $\mathbb{K}^{\mathbb{N}}_{\text{cv}}$, l'opérateur "limite" est un morphisme d'algèbres. Dans la sous-algèbre de $\mathbb{K}^P$ formée des fonctions convergeant en p, l'opérateur $\lim_p$ est un morphisme d'algèbres.

(HP) On montre aisément (en combinant les propositions analogues sur les anneaux et sur les espaces vectoriels) que :

1. *chaque produit d'algèbres est une algèbre (appelé* ***algèbre produit****) ;*
2. *chaque intersection de sous-algèbres est une sous-algèbre,*
3. *l'algèbre pleine est une sous-algèbre,*
4. *l'intersection des sous-algèbres incluant une partie fixée est la plus petite sous-algèbre incluant cette partie (appelée* ***sous-algèbre engendrée*** *par cette partie) ;*
5. *l'identité est un morphisme d'algèbres,*
6. *la composée de chaques morphismes d'algèbres (si elle fait sens) reste un morphismes d'algèbres,*
7. *la réciproque de chaque isomorphisme d'algèbres est un isomorphisme d'algèbres,*
8. $\operatorname{End} A$ *est un monoïde de groupe des inversibles* $(\operatorname{End} A)^\times = \operatorname{Aut} A$ *(pour chaque algèbre* A*) ;*

[49] Ne pas oublier l'unité !

9. *l'image directe de chaque sous-algèbre (source) par chaque morphisme d'algèbres est une sous-algèbre (but) ;*
10. *l'image réciproque de chaque sous-algèbre (but) par chaque morphisme d'algèbres est une sous-algèbre (source),*
11. *l'image de chaque morphisme d'algèbres est une sous-algèbre,*
12. *le noyau de chaque morphisme d'algèbre est un idéal mais n'est jamais une sous-algèbre (sauf si l'algèbre but est nulle).*

De façon interne, *la sous-k-algèbre engendrée*[50] *par une partie est constituée des polynômes en les éléments de cette partie à coefficients dans k :*

$$\text{dans les } k\text{-algèbres : } \langle G\rangle = k[G] := \left\{ P(g) \ ; \quad \begin{array}{c} n \in \mathbb{N},\ g \in G^n \\ P \in k[X_1, X_2, ..., X_n] \end{array} \right\}.$$

Le lecteur aura sans doute observé que, quand on remplace le corps k par l'anneau $\mathbb{Z}$, on retrouve la description "interne" des sous-anneaux engendrés. Cette observation ouvre une description (HP) des anneaux comme algèbres.

RQ (algèbre & morphismes d'anneaux) (HP). Soit A un anneau non nul.

Chaque k-algèbre A induit un morphisme de k-algèbres $\left\{ \begin{array}{ccc} k & \hookrightarrow & A \\ \lambda & \longmapsto & \lambda \cdot 1_A \end{array} \right.$ injectif.

Réciproquement, chaque morphisme d'anneaux $k \hookrightarrow A$ (pensé comme une injection) induit une structure de k-algèbre sur A où l'action externe de k est donnée par[51] la multiplication de A. L'algèbre linéaire peut alors être utilisée pour étudier A : nous pouvons en considérer des bases, parler de sa dimension... En théorie des corps, on abrège souvent

$$[A, k] := \dim_k A.$$

Des exemples sont les morphismes $\left\{ \begin{array}{ccc} \mathbb{R} & \hookrightarrow & \mathbb{C} \\ \lambda & \longrightarrow & \lambda + 0i \end{array} \right.$, $\left\{ \begin{array}{ccc} \mathbb{Q} & \hookrightarrow & \mathbb{Q}\left[\sqrt{2}\right] \\ \lambda & \longrightarrow & \lambda + 0\sqrt{2} \end{array} \right.$, $\left\{ \begin{array}{ccc} \mathbb{C} & \hookrightarrow & \mathbb{C}[X] \\ \lambda & \longrightarrow & \lambda + 0X + 0X^2 + \cdots \end{array} \right.$ et $\left\{ \begin{array}{ccc} \mathbb{R} & \hookrightarrow & M_{42}(\mathbb{R}) \\ \lambda & \longrightarrow & \mathrm{diag}(\lambda, \lambda, ..., \lambda) \end{array} \right.$.

Remplaçons à présent dans les définitions d'une k-algèbre, d'un morphisme d'algèbres et d'une sous-algèbre le corps k par un anneau[52] R commutatif : tout alors s'adapte en remplaçant « k-espace vectoriel » par « R-module ». Comme ci-dessus, une R-algèbre induit un morphisme de R-algèbres $r \mapsto r \cdot 1$ et, réciproquement, un morphisme d'anneaux $R \xrightarrow{\varphi} A$ induit sur l'anneau but A une structure de R-algèbres en définissant comme action externe $r \cdot a := \varphi(r)\, a$ pour chaque $(r, a) \in R \times A$. C'est ainsi que chaque anneau devient une $\mathbb{Z}$-algèbre en imposant $\varphi : z \mapsto z \cdot 1$. En fin de compte :

les algèbres ne sont pas plus générales que les morphismes d'anneaux[53] *.*

[50] La sous-k-algèbre de $k[X]$ engendré par l'élément X est elle-même, d'où la cohérence de la notation "entre crochets".

[51] Ici rayonne particulièrement le parallèle entre les axiomes définissant un espace vectoriel et ceux définissant un anneau.

[52] R comme *ring*

[53] Ce qui laisse quand même un vaste champ d'investigation.

EXO (théorème de la base télescopique). Soient $k \subset K \subset L$ trois corps ? ? ?. *Montrer l'égalité dimensionnelle*

$$[L,k] = [L:K]\,[K:k]\,.$$

SOL Soient $\begin{cases} (a_i) \text{ une } k\text{-base de } K \\ (b_j) \text{ une } K\text{-base de } L \end{cases}$. Il suffit pour conclure d'établir que la famille $(a_i b_j)$ est une k-base de L. Le côté générateur découle des inclusions $L \subset \sum_j Kb_j \subset \sum_j \left(\sum_i ka_i\right) b_j = \sum_{i,j} k\,(a_i b_j)$. Soit par ailleurs une relation de liaison $\sum_{i,j} \lambda_{i,j} a_i b_j = 0$. Elle se réécrit $\sum_i \left(\sum_j \lambda_{i,j} a_i\right) b_j = 0$, d'où (par liberté des b_j) la nullité de chaque $\sum_j \lambda_{i,j} a_i$ et (par liberté des a_i) celle de chaque $\lambda_{i,j}$.

1.7 Quotients (HP)

Nous suivrons la même discussion que pour les groupes : peut-on calculer dans un anneau tout en considérant "nulle" une partie donnée ? Seuls sont au programme les quotients de $\mathbb{Z}$ donnés dans les exemples d'anneaux et de corps, à savoir les anneaux ${}^{\mathbb{Z}}\!/_{n}$ pour n décrivant $\mathbb{N}$.

Rappelons le vocabulaire et nos notations : étant donnée une partie I d'un anneau, les ***classes* modulo** I sont les translatés $\overline{a} := a + I$ de cette partie, l'ensemble de ces translatés est noté ${}^{A}\!/_{I} := \{\overline{a}\ ;\ a \in A\} = \{a + I\}_{a \in A}$ et l'***égalité* modulo** I est la relation $\overset{I}{=}$ formée des couples (a,b) tels que $b \in \overline{a}$.

RQ PROP (loi quotient, loi "parties", compatibilité) (HP).
Soit M un magma partitionné par une relation d'équivalence $\sim$. Définissons sur le quotient ${}^{M}\!/_{\sim}$ une loi de la manière suivante : deux classes C et Γ se composent en la classe du composé de (c,γ) *pour n'importe quels* $\begin{matrix} c \in C \\ \gamma \in \Gamma \end{matrix}$. Cette "définition" est loin d'être univoque car le composé $\overline{c\gamma}$ dépend *a priori* des représentants[54] c et γ "choisis" :

demander que cette "loi" de ${}^{M}\!/_{\sim}$ fasse sens, c'est précisément affirmer la compatibilité de la loi de M avec la relation $\sim$.
On aura alors les égalités $\overline{m\mu} = \overline{m\mu}$ pour chaques $m, \mu \in M$.

Dans le cas d'un groupe abélien quotienté par l'égalité *modulo* un sous-groupe, on retrouve la loi "parties". Cette dernière n'a pas besoin de discussion sur le "choix" des représentants pour faire sens et c'est pourquoi nous l'avons préférée à la loi quotient "définie" ci-dessus. Dans un cas comme dans l'autre, le but est de retrouver le calcul "comme dans M" *via* les égalités $\overline{m\mu} = \overline{m\mu}$.

DEM

[54] la question étant de savoir si l'ensemble $\{\overline{c\gamma}\}_{\gamma\in\Gamma}^{c\in C}$ est un singleton, on peut toujours définir explicitement $C\Gamma := \cup\{\overline{c\gamma}\}_{\gamma\in\Gamma}^{c\in C}$ et se demander ensuite si $\forall C, \Gamma \in {}^{M}\!/_{\sim},\ \forall\,(c,\gamma) \in C\times\Gamma,\ C\Gamma = \overline{c\gamma}$ (traduction propre de l'énoncé « *cette "loi" de ${}^{M}\!/_{\sim}$ fait sens* »)

Supposons la loi de M compatible avec $\sim$. Soient $C, \Gamma \in {}^{M}\!/_{\sim}$, soient $\begin{array}{c} c, c' \in C \\ \gamma, \gamma' \in \Gamma \end{array}$.
On a alors $\left\{ \begin{array}{c} c \sim c' \\ \gamma \sim \gamma' \end{array} \right.$, d'où (par compatibilité) $c\gamma \sim c'\gamma'$, ce qui montre que la classe du composé $c\gamma$ ne dépend pas des représentants c et γ.

Supposons cette fois la "loi" ci-dessus faisant sens. Soient m, m', μ, μ' tels que $\left\{ \begin{array}{c} m \sim m' \\ \mu \sim \mu' \end{array} \right.$.
On a alors les égalités $\left\{ \begin{array}{c} \overline{m} = \overline{m'} \\ \overline{\mu} = \overline{\mu'} \end{array} \right.$, d'où (en appliquant la loi ci-dessus) $\overline{m\mu} = \overline{m'\mu'}$, çàd $\overline{m\mu} = \overline{m'\mu'}$, ou encore $m\mu \sim m'\mu'$.

Plaçons-nous à présent dans un anneau quotienté par un sous-groupe additif (où l'on a donc $\overline{a} + \overline{b} = \overline{a+b}$ pour l'addition "partie") et tachons d'obtenir les égalités $\overline{a}\overline{b} = \overline{ab}$. Si l'on pouvait y parvenir *via* la multiplication partie, on aurait en particulier l'égalité $\overline{0}\overline{0} = \overline{0}$; or, dans le cas d'un quotient ${}^{\mathbb{Z}}\!/_{n}$, cette égalité implique l'inclusion $(n) \subset \left(n^2\right)$, d'où le fait que n soit multiple de son carré, ce qui est impossible dès que l'on impose $n \geq 2$. Nous allons donc revenir à la définition par représentants.

PROP DEF (anneau quotient par un idéal bilatère) (HP). Soient A un anneau et I une partie de A. *Les conditions suivantes sont alors équivalentes :*

1. *l'égalité* modulo I *est une relation d'équivalence sur A compatible avec les deux lois de A ;*
2. *font sens dans le quotient ${}^{A}\!/_{I}$ les deux "lois"* $\begin{array}{l} (C,\Gamma) \overset{+}{\longmapsto} \overline{c+\gamma} \text{ pour n'importe quel } (c,\gamma) \in C \times \Gamma \\ (C,\Gamma) \overset{\times}{\longmapsto} \overline{c\gamma} \text{ pour n'importe quel } (c,\gamma) \in C \times \Gamma \end{array}$;
3. *I est un idéal bilatère de A.*

*Dans ces conditions, le quotient par la relation d'équivalence $\overset{I}{=}$ et celui ${}^{A}\!/_{I}$ des translatés de I coïncident et forment un même anneau, appelé l'**anneau quotient** de A par I, dans lequel on a*[55] $\left\{ \begin{array}{c} \overline{a} + \overline{0} = \overline{a} = \overline{0} + \overline{a} \\ \overline{a} + \overline{b} = \overline{a+b} \\ -\overline{a} = \overline{-a} \end{array} \right.$ *et* $\left\{ \begin{array}{c} \overline{a}\overline{1} = \overline{a} = \overline{1}\overline{a} \\ \overline{a}\overline{b} = \overline{ab} \end{array} \right.$ *pour chaques $a, b \in A$.*

DEM

$\boxed{1 \Longrightarrow 2}$ Suit immédiatement de la proposition précédente.

$\boxed{2 \Longrightarrow 3}$ L'addition donnée munit ${}^{A}\!/_{I}$ d'une structure de groupe additif où $\overline{0} + \overline{0} = \overline{0}$ (tout passer sous la barre) : la partie I est donc (*cf.* section **??**) un sous-groupe additif de A. Soit par ailleurs $(\lambda, i) \in A \times I$: on a alors $\overline{\lambda i} = \overline{\lambda}\overline{i} = \overline{\lambda}\overline{0} = \overline{\lambda 0} = \overline{0}$, d'où $\lambda i \in I$ (et de même pour $i\lambda$).

$\boxed{3 \Longrightarrow 1}$ Puisque I est un sous-groupe additif de A, l'égalité *modulo I* est une relation d'équivalence sur A compatible avec l'addition A. Montrons sa compatibilité avec $\times$. Soient $a, \alpha, b, \beta \in A$ tels que $\left\{ \begin{array}{c} a \overset{I}{=} \alpha \\ b \overset{I}{=} \beta \end{array} \right.$. Soient $i, j \in I$ tels que $\left\{ \begin{array}{c} \alpha = a + i \\ \beta = b + j \end{array} \right.$.

[55] Ces égalités pourraient s'énoncer : « la projection canonique *modulo I* est un morphisme d'anneaux ».

On a alors les égalités $\alpha\beta = (a+i)(b+j) = ab+aj+ib+ij$ où les trois derniers termes restent dans l'idéal bilatère I, *a fortiori* leur somme, d'où l'appartenance $\alpha\beta \in ab+I$.

RQ (quotient par un idéal principal). Soit A un anneau commutatif, soit $a \in A$. "Tuer" a revient à "tuer" ses multiples, çàd à raisonner *modulo* l'idéal (a), ce qui motive l'abréviation

$$A/a := A/(a).$$

Exemples 1 (quotients d'entiers). Le quotient $\mathbb{Z}/n$ est un anneau pour chaque naturel n.

RQ (algèbres quotients). Soit A une algèbre, soit I un idéal bilatère de A. Un idéal (à gauche) d'une algèbre en étant en particulier un sous-espace vectoriel (pour chaque scalaire λ, multiplier à gauche par $\lambda \cdot 1$ revient à appliquer l'homothétie de rapport λ), l'anneau quotient A/I est aussi un espace vectoriel pour les lois "quotient", l'"associativité" s'obtenant aisément en passant tout "sous la barre". Il est donc une algèbre, appelée l'***algèbre quotient*** de A par I.

Exemples 2 (quotients de polynômes). Soient A un anneau et P un polynôme unitaire[56].

1. *Le quotient* $\mathcal{A} := A[X]/P$ *est une* A*-algèbre dont une base est* $\left(\overline{X}^n\right)_{0\leq n<\deg P}$.
2. *Dans cette algèbre, le polynôme*[57] P *possède une racine.*
3. *Lorsque* A *est un corps, l'algèbre* $\mathcal{A}$ *est un corps ssi* P *est irréductible.*

SOL

1. Le quotient de l'A-algèbre $A[X]$ par l'idéal (P) reste une A-algèbre. Une division euclidienne par P (légitime vu l'unitarité de ce dernier) montre le caractère générateur de la famille $\left(\overline{X}^n\right)_{0\leq n<\deg P}$. Soit par ailleurs $\sum_{0\leq n<\deg P} a_n\overline{X}^n = 0$ une relation de liaison. Elle se réécrit $\overline{\sum a_n X^n} = \overline{0}$, çàd $\sum a_n X^n \in (P)$, ce qui force la nullité du multiple de gauche pour des questions de degrés.
2. Notons avec un indice $\mathcal{A}$ l'action du morphisme $A[X] \longrightarrow \mathcal{A}[X]$. Appelons (a_n) la suite des coefficients de $P = \sum a_n X^n$: on a alors $P_{\mathcal{A}} = \sum \overline{a_n} X^n_{\mathcal{A}}$, d'où (en notant λ l'élément de $\mathcal{A}$ formé par la classe de X) les égalités

$$P_{\mathcal{A}}(\lambda) = \sum \overline{a_n}\lambda^n = \sum \overline{a_n}\overline{X}^n = \overline{\sum a_n X^n} = \overline{P} = 0.$$

3. Supposons que A est un corps. Ce dernier étant commutatif, l'anneau $A[X]$ l'est aussi, donc le quotient $\mathcal{A}$ également. Le polynôme P est de plus non nul (car unitaire à coefficients dans un corps) et est par ailleurs non inversible ssi l'idéal (P) est strict, çàd ssi le quotient $\mathcal{A}$ n'est pas nul.

[56] Vu qu'on va considérer l'idéal (P), ce qui suit tient pour chaque P *associé à un polynôme unitaire*, çed dont le coefficient dominant est inversible.

[57] On identifie abusivement P avec son image par le morphisme d'anneaux $A[X] \longrightarrow \mathcal{A}[X]$ induit par le morphisme d'anneaux

$$\left\{\begin{array}{ccc} A & \hookrightarrow A[X] \twoheadrightarrow & \mathcal{A} \\ a & \longmapsto & a+0X+0X^2+\cdots \ mod\ P \end{array}\right. .$$

.

Supposons de plus que $\mathcal{A}$ est un corps. Soient $F, G \in A[X]$ tels que $P = FG$: dans A, on en déduit $0 = \overline{P} = \overline{FG} = \overline{F}\,\overline{G}$, d'où (par intégrité) la nullité de $\overline{F}$ ou de $\overline{G}$, disons $P \mid F$, çàd $FG \mid F$, çàd (vu que $A[X]$ est intègre) $G \mid 1$, d'où $G \sim 1$.

Supposons cette fois P irréductible. Soit $f \in \mathcal{A}$ non nul, soit $F \in A[X]$ tel que $f = \overline{F}$. Puisque F est non nul *modulo* P, ce dernier ne divise pas F, donc lui est étranger, d'où (par BÉZOUT, valide puisque A est un corps) deux polynômes U et V tels que $FU+PV = 1$. Projeter *modulo* P donne $\overline{FU}+\overline{0}\overline{V} = \overline{1}$, çàd $f\overline{U} = \overline{1}$, d'où l'inversibilité de f.

REMARQUE – Cette démonstration doit rappeler celle de « ${}^{\mathbb{Z}}\!/_{p}$ *est un corps ssi* p *est un irréductible de* Z » en passant par BÉZOUT.

Applications.

1. Le polynôme X^2+1 est irréductible sur le corps $\mathbb{R}$, l'algèbre ${}^{\mathbb{R}[X]}\!/_{X^2+1}$ est donc un corps de dimension (réelle) 2 dont une base est $\left(\overline{1}, i\right)$ avec $i := \overline{X}$. Autant pour la construction algébrique du corps des complexes.
2. Le polynôme $X^2 - 7$ est irréductible sur le corps $\mathbb{Q}$, l'algèbre ${}^{\mathbb{Q}[X]}\!/_{X^2-7}$ est donc un corps de dimension (rationnelle) 2 dont une base est $\left(\overline{1}, r\right)$ avec $r := \overline{X}$. Nous avons déjà rencontré ce corps $\mathbb{Q}\left[\sqrt{7}\right]$ en exercice (section 1.3).
3. Soient p un premier, n un naturel non nul, P un polynôme irréductible de $\mathbb{F}_p[X]$ de degré n. Alors l'algèbre ${}^{\mathbb{F}_p[X]}\!/_{P}$ est un $\mathbb{F}_p$-espace vectoriel de dimension n, donc isomorphe (en tant que $\mathbb{F}_p$-espace vectoriel) à $\mathbb{F}_p^n$, donc est de cardinal $\left|\mathbb{F}_p^n\right| = |\mathbb{F}_p|^n = p^n$. On obtient ainsi un[58] corps de cardinal p^n. Par exemple, le corps de cardinal 4 est (isomorphe à) ${}^{\mathbb{F}_2[X]}\!/_{X^2+X+1}$.

RQ (corps & algèbre intègre de dimension finie). Comme le montre la démonstration ci-dessus, on pourrait dans le point (3) remplacer « $\mathcal{A}$ *est un corps* » par « $\mathcal{A}$ *est intègre* ». De fait, il est aisé de montrer que *chaque algèbre de dimension finie intègre est un corps* : pour chaque élément a non nul, l'endomorphisme $a\,\mathrm{Id}$ est injectif par intégrité, donc surjectif (par finitude de la dimension), donc atteint 1, d'où l'inversibilité de a.

RQ (idéaux et quotients). Chaque idéal bilatère est le noyau du morphisme "projection canonique *modulo* cet idéal". Les idéaux bilatères sont donc exactement les noyaux de morphismes.

EG 3 (isomorphisme quotient). *Chaque morphisme d'anneaux* $A \xrightarrow{\varphi} B$ *induit un isomorphisme d'anneaux* $\left\{ \begin{array}{ccc} {}^{A}\!/_{\mathrm{Ker}\,\varphi} & \xrightarrow{\sim} & \mathrm{Im}\,\varphi \\ \overline{a} & \longmapsto & \varphi(a) \end{array} \right.$. Idem *en remplaçant « anneaux » par « algèbres ».*

DEM L'application Φ ci-dessus fait sens et est un isomorphisme de groupe additifs. Elle préserve par ailleurs la multiplication vu à $a, b \in A$ fixés les égalités.

$$\Phi\left(\overline{a}\overline{b}\right) = \Phi\left(\overline{ab}\right) = \varphi(ab) = \varphi(a)\,\varphi(b) = \Phi\left(\overline{a}\right)\Phi\left(\overline{b}\right).$$

[58] Il y a en fait unicité "du" corps de cardinal p^n (à isomorphisme près).

Par ailleurs, le groupe source est un anneau par la remarque précédente et le groupe but aussi comme chaque image par un morphisme d'anneaux. Dans le cas algébrique, Φ est en outre linéaire vu pour chaque scalaire λ et à $a \in A$ fixé les égalités

$$\Phi(\lambda\overline{a}) = \Phi\left(\overline{\lambda a}\right) = \varphi(\lambda a) = \lambda\varphi(a) = \lambda\Phi(\overline{a}).$$

Application (lemme chinois). Soient a et b deux naturels étrangers. Lorsque φ est $\left\{\begin{array}{ccc} \mathbb{Z} & \longrightarrow & {}^{\mathbb{Z}}\!/_{a} \times {}^{\mathbf{Z}}\!/_{b} \\ z & \longmapsto & (\widetilde{z}, \widehat{z}) \end{array}\right.$, on retrouve le théorème du cours (section 1.4).

Culture (nombres & anneaux). Nous avons présenté le point de vu moderne des idéaux : ce par quoi l'on peut quotienter dans les anneaux. Le point de vue historique les ferait plutôt émerger de considérations *arithmétiques* où l'on essayait[59] de sauvegarder le théorème de décomposition en facteur premiers en remplaçant les nombres naturels n par des nombres "idéaux" (n). L'algèbre commutative (étude des anneaux commutatifs) maintient donc des liens étroits avec la théorie des nombres, c'est pourquoi elle ne cesse n'être un champ toujours actif et difficile de la recherche mathématique.

Le lecteur curieux pourra consulter l'*Invitation aux Mathématiques de Fermat-Wiles* d'Yves Hellegouarch (à contenu mathématique) ainsi que *Le dernier théorème de Fermat* de Simon Singh qui trace à destination du grand public une histoire de la fameuse conjecture arithmétique. Pour un point de vue plus géométrique sur ces questions, l'ouvrage grand public *Amour et maths* d'Edward Frenkel en donne une idée – sans oublier toute l'œuvre de feu Alexandre Grothendieck qui a révolutionné la géométrie algébrique.

2 Arithmétique

Traditionnellement, l'arithmétique désigne l'étude des nombres (entiers). Les questions de divisibilité sont y centrales et ne concernent que la structure *multiplicative* de $\mathbb{N}$, c'est pourquoi nos définitions seront formulées dans le cadre général d'un monoïde multiplicatif. Nous les appliquerons au monoïde multiplicatif d'un anneau intègre, à l'instar de $\mathbb{Z}$ ou de $k[X]$, les seuls au programme. On fixe pour toute cette section :

1. k un corps (penser à $\mathbb{R}$ ou $\mathbb{C}$) ;
2. A un anneau commutatif (penser à $\mathbb{Z}$ ou $k[X]$) ;
3. M un monoïde abélien (penser à A^* quand A est intègre).

[59] Ce résumé outrageusement réducteur n'est qu'une incitation à aller lire des ouvrages traitant véritablement d'*histoire* des mathématiques, comme *Moderne Algebra and the Rise and Mathematical Structures* de Leo Corry.

2.1 Divisibilité, association

DEF-PROP (diviseur, multiple). *Soient d et m dans M. On dit que d **divise** m, que d est un **diviseur** de m, que m est **divisible** par d, ou que m est un **multiple** de d, si*

$$d \mid m \overset{\text{déf.}}{\iff} \exists d' \in M,\ dd' = m.$$

*La relation $\mid$ s'appelle la **divisibilité** (de M). Elle est réflexive, transitive et compatible*[60] *avec la loi de M.*

DEM Soient $a, b, c \in M$.

L'égalité $a = a1$ montre la divisibilité $a \mid a$.

Imposons $\begin{cases} a \mid b \\ b \mid c \end{cases}$, soient $\lambda, \mu \in M$ tels que $\begin{cases} b = a\lambda \\ c = b\mu \end{cases}$: on a alors $c = (a\lambda)\,\mu = a\,(\lambda\mu)$, d'où $a \mid c$.

Soient enfin $\alpha, \beta \in M$ tels que $\begin{cases} a \mid \alpha \\ b \mid \beta \end{cases}$, soient λ, μ tels que $\begin{cases} a\lambda = a \\ b\mu = \beta \end{cases}$: multiplier donne alors $\alpha\beta = a\lambda b\mu = (ab)\,\lambda\mu$, d'où $ab \mid \alpha\beta$.

RQ (divisibilité et quotients) (HP) En termes de quotients, la relation de divisibilité dans M est tout simplement l'égalité *modulo* M vu l'équivalence (à $a, b \in M$ fixés)

$$a \mid b \iff aM \ni b.$$

EXO (divisibilité et idéaux). Soient $a, b \in M$. *Montrer l'équivalence*[61]

$$a \mid b \iff aM \supset bM.$$

SOL

Supposons $a \mid b$, soit $\alpha \in M$ tel que $a\alpha = b$. Un élément bm de bM s'écrit alors $a\,(\alpha m)$, donc appartient à aM.

Supposons à présent $aM \supset bM$. Alors l'élément $b = b1 \in bM$ tombe dans aM, d'où un $\alpha \in M$ tel que $b = \alpha a$, ce qui montre $a \mid b$.

EG 1 (divisibilités dans $\mathbb{N}$). Dans le monoïde multiplicatif des naturels :

2 divise 18,

42 est un multiple de 6 et de 7,

13 n'est divisible que par 1 et par lui-même,

les diviseurs de 24 forment $\{1, 2, 3, 4, 6, 8, 12, 24\}$,

1 divise chaque naturel et

0 est divisible par chaque naturel.

EG 2 (divisibilités dans $\mathbb{R}[X]$). Dans le monoïde multiplicatif des polynômes réels :

X divise $X^7 + 7X^2$,

[60] La réflexivité de $\mid$ (resp. sa transitivité, sa compatibilité) vient du caractère unifère de M (resp. associatif, commutatif).

[61] Une divisibilité équivaut donc à l'inclusion réciproque des sous-monoïdes engendrés correspondants. Cela deviendra important dans les anneaux.

$X^2 - 2$ est multiple de $X + \sqrt{2}$,
$eX^2 + e$ est un diviseur de $X^2 + 1$,
5 est divisible par 18, 42, $\sqrt{7}$ et π.

On pourrait se demander, comme cela est le cas dans $\mathbb{N}$, si la divisibilité est une relation d'*ordre*. Or on constate chez les polynômes que *la divisibilité ne voit pas les scalaires non nuls*, lesquels sont multiples les uns des autres, niant ainsi l'anti-réflexivité de $|$. De même, dans le monoïde multiplicatif $\mathbb{Z}$, toutes les questions de divisibilité sont définies *au signe près*, 2 et -2 étant par exemple multiples l'un de l'autre sans être égaux. Dans ces deux cas, les "invisibles" par $|$ sont exactement les inversibles, ce qui incite à raisonner *modulo* ces derniers.

DEF PROP (relation d'association $\sim$). *Imposons M régulier*[62] *et soient $a, b \in M$. Il est alors équivalent de dire*

1. *a et b se divisent réciproquement ;*
2. *a et b sont égaux* modulo *un inversible.*

Dans ce cas, on dit que a et b sont ***associés*** *et on note*

$$a \sim b \overset{\text{déf.}}{\iff} \begin{cases} a \mid b \\ b \mid a \end{cases} \iff \exists i \in M^\times,\ b = ai.$$

*La relation $\sim$ s'appelle l'**association** (de M) et est une relation d'équivalence. En particulier, les associés de 1 sont les inversibles :*

$$a \sim 1 \iff a \in M^\times.$$

DEM

Soit $i \in M^\times$ tel que $b = ai$. On a alors d'une part $a \mid b$, d'autre part $a = b\frac{1}{i}$, d'où $b \mid a$, ce qui montre l'association $a \sim b$.

Supposons réciproquement $a \sim b$. Soient $\lambda, \mu \in M$ tels que $\begin{cases} b = a\lambda \\ a = b\mu \end{cases}$. On a donc $a = a\lambda\mu$, d'où (par régularité) $1 = \lambda\mu$, d'où l'inversibilité de λ.

L'association est symétrique par construction (le connecteur *et* étant commutatif), ses réflexivité et transitivité découlent de[63] celles de $|$. On en déduit les équivalences

$$a \sim 1 \iff 1 \sim a \iff \exists i \in M^\times,\ \underbrace{a = 1i}_{\iff a = i} \iff a \in M^\times.$$

RQ (représentants modulo $\sim$). Le choix d'un représentant *modulo* $\sim$ est canonique dans les anneaux au programme :

1. pour $\mathbb{Z}$, on choisira le représentant *positif* ;

[62] Le cas typique est celui où $M = A^*$ lorsque l'anneau A est intègre.

[63] La relation $\sim$ n'est autre que la symétrisée de $|$, la ***symétrisée*** d'une relation R étant la relation (symétrique !) formée des couples (a, b) tels que aRb et bRa.

2. pour $k[X]$, on choisira le représentant *unitaire*[64].

RQ (association et quotients) (HP). En termes quotients, l'association est l'égalité *modulo* $M^\times$. Le cours (HP) sur les quotients de monoïdes montrerait que, pour chaque partie $S \subset M$, *la relation* $\overset{S}{=}$ *est d'équivalence et compatible avec la loi de* M *ssi* S *est un sous-groupe (distingué) de* $M^\times$, ce qui est trivialement le cas quand $S = M^\times$. On peut donc considérer le monoïde ${}^{M}\!/_{M^\times}$ et la divisibilité[65] y devient cette fois une relation d'*ordre*. C'est dans ce monoïde que s'expriment les véritables propriétés arithmétiques de M.

EXO (symétricité de la divisibilité). *Montrer que la divisibilité dans* M *est symétrique ssi* M *est un groupe. Expliciter alors* $|$.

SOL Soient $a, b \in M$.

Supposons $|$ symétrique. L'égalité $1a = a$ montre la divisibilité $1 \mid a$, çàd $a \mid 1$, d'où un $a' \in M$ tel que $aa' = 1$, ce qui énonce l'inversibilité de a.

Réciproquement, si M est un groupe, on a alors $a = b\left(b^{-1}a\right)$, donc chaque élément divise chaque autre et la relation $|$est trivialement symétrique. Il s'agit alors de la relation d'équivalence grossière M^2 ne possédant qu'une seule classe d'équivalence.

2.2 Plus petit diviseur commun & plus grand multiple commun

Soient deux naturels a et b. Observons qu'un diviseur commun à a et b est un minorant de la partie $\{a, b\}$ pour l'ordre $|$: s'il fait sens, le plus grand diviseur commun à a et b est donc le plus grand minorant de $\{a, b\}$, çàd l'*infimum* de la paire $\{a, b\}$, noté $a \wedge b$. De même, s'il fait sens, le plus grand multiple commun à a et b est le *supremum* de $\{a, b\}$, noté $a \vee b$. Voyons comment les idéaux vont éclairer la présentation.

Lemme (divisibilité et idéaux). Soient $a, b \in A$. *Alors la divisibilité (dans* A*) équivaut à l'inclusion réciproque des idéaux principaux associés :*

$$a \mid b \iff (a) \supset (b)\,.$$

DEM Découle d'un exercice proposé dans les monoïdes appliqué au monoïde multiplicatif A.

RQ (HP) En observant par ailleurs l'égalité $(a)(b) = AaAb = abA^2 = abA = (ab)$ pour la multiplication "parties", nous venons de montrer qu'est un isomorphisme de monoïdes ordonnés[66] $\begin{cases} \left({}^{A}\!/_{A^\times}, \times, |\right) & \xrightarrow{\sim} & (\mathcal{I}_A^{\mathrm{pp}}, \times, \supset) \\ a & \overset{\iota}{\longmapsto} & (a) \end{cases}$ où $\mathcal{I}_A^{\mathrm{pp}}$ dénote l'ensemble des idéaux principaux de A. Un *infimum* pour $|$ devient ainsi un *infimum* pour $\supset$, çàd un *supremum* pour $\subset$: or un idéal incluant deux idéaux doit inclure

[64] La classe des inversibles pourra toujours être représentée par 1.

[65] relation d'une part formée des couples de classes (C, Γ) tels que $\exists\,(c, \gamma) \in C \times \Gamma,\ c \mid \gamma$, d'autre part vérifiant $\overline{a} \mid \overline{b} \iff a \mid b$ pour chaques $a, b \in M$

[66] un ***magma ordonné*** est un magma muni d'une relation d'ordre compatible avec sa loi

leur somme (laquelle est bien un idéal), donc la somme $(a)+(b)$ devrait être l'image par ι du p. g. c. d. de a et de b. De même, un idéal inclus dans deux idéaux doit être inclus dans leur intersection (laquelle est bien un idéal), donc l'intersection $(a)\cap(b)$ devrait être l'image par ι du p. p. c. m. de a et de b. Ces images feront sens dans $\mathcal{I}_A^{\mathrm{pp}}$ si A est principal – ce qu'on a pour $\mathbb{Z}$ et pour $k[X]$ (au programme) –, auquel cas l'isomorphisme ι s'enrichit et permet de traduire élégamment en termes idéaux les opérations et relation arithmétiques de A :

$$\begin{cases} \left({}^{A}\!/_{A^\times}, \times, \wedge, \vee, |\right) & \xrightarrow{\sim} & (\{\text{idéaux de } A\}, \times, +, \cap, \supset) \\ a & \longmapsto & (a) \end{cases} \quad \text{quand } A \text{ est principal.}$$

DEF PROP (p. g. c. d & p. p. c. m.). Soit S une partie de M.

*Un **plus grand commun diviseur (p. g. c. d.)** de S est un élément divisant chaque $s\in S$ et multiple de chaque tel commun diviseur. Tous les p. g. c. d. de S sont associés.*

*Un **plus petit commun multiple (p. p. c. m.)** de S est un élément multiple de chaque $s\in S$ et divisant chaque tel commun multiple. Tous les p. p. c. m. de S sont associés.*

Lorsqu'un choix de représentants modulo $\sim$ *a été effectué,* $\underline{\underline{le}}$ ***p. g. c. d.*** / $\underline{\underline{le}}$ ***p. p. c. m.*** *de S est le représentant de la classe* modulo $\sim$ *des* *p. g. c. d.* / *p. p. c. m.* *de S. On le note*[67] $\wedge S = \bigwedge_{s\in S} s$ / $\vee S = \bigvee_{s\in S} s$.

DEM

Soient d et δ deux p. g. c. d. de S. Alors d est multiple de chaque commun diviseur de S, *a fortiori* de δ, d'où $\delta \mid d$. La symétrie des rôles de d et δ donne alors $d\mid\delta$. Démonstration analogue pour les p. p. c. m. de S.

RQ (p. g. c. d. & *infimum*, p. p. c. m. & *supremum*) (HP). Bien sûr, la "bonne" définition du p. g. c. d. (resp. p. p. c. m.) de S serait dans ${}^{M}\!/_{M^\times}$ l'*infimum* (resp. le *supremum*) pour $\mid$ de la partie ${}^{S}\!/_{M^\times}$, identifié à son représentant choisi dans M.

EG (p. g. c. d.).

1. Dans $\mathbb{Z}$, on a $15\wedge(-51)=3$ et $2\wedge 3=1$.
2. Dans $k[X]$, on a $\pi X\wedge\frac{X^{42}}{-\sqrt{18}}=X$ et $\left(X^2+X\right)\wedge\left(\frac{X}{2}-\frac{X^2}{2}-1\right)=X+1$.
3. Dans A, chaque élément a vérifie $\begin{cases} a\wedge 1=1 \\ a\wedge 0\sim a \end{cases}$ et $\begin{cases} a\vee 1\sim a \\ a\vee 0=0 \end{cases}$.

TH (existence de p. g. c. d. et de p. p. c. m.). Soit S une partie (finie ou non) de $\mathbb{Z}$ ou de $k[X]$. *Alors :*

1. *chaque générateur de l'idéal $\sum_{s\in S}(s)$ est un p. g. c. d. de S ;*
2. *chaque générateur de l'idéal $\bigcap_{s\in S}(s)$ est un p. p. c. m. de S.*

[67] *Mnémo* : prendre des diviseurs dans $\mathbb{N}$ "rapetisse", comme l'intersection $\cap$, d'où la notation analogue $\wedge$ pour le p. g. c. d.. De même pour les multiples, l'union $\cup$ et le p. p. c. m. $\vee$.

DEM Soit $\sigma \in S$.

La somme $\sum_{s\in S}(s)$ est un idéal, donc principal, on peut en évoquer un générateur Δ. Alors $(\Delta) = \sum_{s\in S}(s)$ inclut (σ), donc Δ divise σ. Soit par ailleurs d un diviseur de chaque $s \in S$. On a alors $d \mid \sigma$, çàd $(\sigma) \subset (d)$, d'où $\sum_{s\in S}(s) \subset (d)$, çàd $(\Delta) \subset (d)$, ou encore $d \mid \Delta$. Démonstration analogue pour les p. p. c. m. de S, une intersection d'idéaux étant un idéal incluant chacun de ses intersectés.

REMARQUE – On retiendra donc les identités $\begin{cases} \sum_{s\in S}(s) = (\wedge S) \\ \bigcap_{s\in S}(s) = (\vee S) \end{cases}$.

EG (idéaux & p. g. c. d.).

1. Dans $\mathbb{Z}$, on a $(15) + (51) = (3)$ et $(2) + (3) = (1)$.
2. Dans $k[X]$, on a $(X) + \left(X^{42}\right) = (X)$ et $\left(X^2 + X\right) + \left(X^2 - X + 2\right) = (X + 1)$.

EXO (contenu d'un produit de polynômes). On appelle ***contenu*** d'un polynôme le p. g. c. d. de ses coefficients. Soient P et Q deux polynômes de $\mathbb{Z}[X]$ de contenu 1. *Montrer que leur produit est de contenu* 1. (hint : réduire *modulo* chaque premier[68])

SOL Soit p un premier. Alors la réduction $\mathbb{Z} \longrightarrow {}^{\mathbb{Z}}\!/_{p}$ *modulo* p induit un morphisme d'anneaux $\mathbb{Z}[X] \xrightarrow{\rho} {}^{\mathbb{Z}}\!/_{p}[X]$; puisque p ne divise pas chaque coefficient de P (sinon p diviserait leur p. g. c. d.), l'image de P par ρ est non nulle (de même pour Q). L'anneau ${}^{\mathbb{Z}}\!/_{p}$ étant par ailleurs intègre (c'est un corps), l'anneau ${}^{\mathbb{Z}}\!/_{p}[X]$ est aussi intègre, d'où la non-nullité de $\rho(P)\,\rho(Q) = \rho(PQ)$, donc p ne divise pas le p. g. c. d. des coefficients de PQ. Ceci tenant pour chaque premier p, ce p. g. c. d. vaut 1.

Les conséquences du caractère euclidien sont les mêmes que pour $\mathbb{Z}$ (ou pour chaque anneau principal), chacune découlant de la précédente :

1. principalité ;
2. relation de BÉZOUT[69] pour les étrangers ;
3. lemmes[70] de GAUSS[71] ;
4. lemme d'EUCLIDE[72] ;
5. unicité (*modulo* $\sim$) de la factorisation en irréductibles (*cf.* section 2.3).

Les démonstrations pour l'anneau $k[X]$ se calquent parfaitement depuis celle dans $\mathbb{Z}$. Montrons par l'exemple l'implication $1 \Longrightarrow 2$ pour insister sur l'éclairage

[68] Ce résultat se généraliserait aisément à n'importe quel anneau principal (il suffirait alors d'établir que les irréductibles de A sont les p tels que ${}^{A}\!/_{p}$ est intègre).

[69] *Relation de* BÉZOUT : deux éléments sont étrangers ssi 1 en est combinaison linéaire.

[70] *Lemme de* GAUSS *1* : si un polynôme divise un produit de deux polynômes et est étranger à l'un des facteurs, alors ce polynôme divise l'autre facteur.

[71] *Lemme de* GAUSS *2* : deux polynômes étrangers divisent un troisième polynôme ssi leur produit le divise.

[72] *Lemme d'*EUCLIDE : chaque polynôme irréductible divise un produit ssi il divise l'un des facteurs de ce produit.

par les idéaux : quand A est principal (*e. g.* $\mathbb{Z}$ ou $k[X]$), on a pour chaques $a, b \in A$ les équivalences

$$a \wedge b = 1 \iff (a \wedge b) = (1) \iff 1 \in (a \wedge b) \iff 1 \in (a)+(b) \iff \exists \lambda, \mu \in A, 1 = \lambda a + \mu b.$$

Par ailleurs, l'existence d'une division euclidienne permet, *via* l'algorithme d'EUCLIDE[73], d'obtenir le p. g. c. d. de deux polynômes et, *via* l'algorithme étendu d'EUCLIDE, d'exprimer dans un second temps ce p. g. c. d. comme combinaison linéaire de ces polynômes (expression également appelée une relation de BÉZOUT).

EG (algorithme d'Euclide étendu). Trouvons une relation de BÉZOUT pour les polynômes $6X^4 + 8X^3 \widetilde{-7X^2} - 5X - 1$ et $\overline{6X^3 - 4X^2 - X - 1}$ (les symboles coiffants sont juste des repères visuels). L'algorithme d'EUCLIDE donne successivement

$$\begin{aligned}
6X^4 + 8X^3 \widetilde{-7X^2} - 5X - 1 &= \overline{(6X^3 - 4X^2 - X - 1)}\,(X + 2) + 2X^2 \widehat{-2X} + 1, \\
\overline{6X^3 - 4X^2 - X - 1} &= (2X^2 \widehat{-2X} + 1)\,(3X + 1) + \overbrace{-2X - 2}^{} \\
\text{et } 2X^2 \widehat{-2X} + 1 &= \overbrace{(-2X - 2)}^{}\,(2 - X) + \overrightarrow{5}.
\end{aligned}$$

Nos deux polynômes sont bien étrangers (on peut toujours diviser par 5). On obtient ensuite, en réinjectant l'expression du terme tout à droite d'une égalité dans l'égalité juste au-dessus :

$$\begin{aligned}
\overrightarrow{5} &= 2X^2 \widehat{-2X} + 1 + \overbrace{(-2X - 2)}^{}\,(X - 2) && \text{on remplace } \overbrace{\cdots}^{} \\
&= 2X^2 \widehat{-2X} + 1 + \left[\overline{6X^3 - 4X^2 - X - 1} - (2X^2 \widetilde{-2X} + 1)\,(3X + 1)\right](X - 2) && \text{on regroupe} \\
&= (X - 2)\,\overline{(6X^3 - 4X^2 - X - 1)} + \left(5X - 3X^2 + 3\right)(2X^2 \widehat{-2X} + 1) && \text{on remplace } \widehat{\cdots} \\
&= (X - 2)\,\overline{(6X^3 - 4X^2 - X - 1)} + \left(5X - 3X^2 + 3\right)\begin{bmatrix} 6X^4 + 8X^3 \widetilde{-7X^2} - 5X - 1 \\ -\overline{(6X^3 - 4X^2 - X - 1)}\,(X + 2) \end{bmatrix} && \text{on regroupe} \\
&= \left(3X^3 + X^2 - 12X - 8\right)\overline{(6X^3 - 4X^2 - X - 1)} + \left(5X - 3X^2 + 3\right)(6X^4 + 8X^3 \widetilde{-7X^2} - 5X - 1) && \text{on souffle !}
\end{aligned}$$

2.3 Décomposition en irréductibles

Comme dans $\mathbb{N}$, une question naturelle est de chercher à factoriser un élément autant que possible, les briques "infactorisables" étant (dans le cas entier) les nombres premiers. Vu à $a \in M$ fixé les factorisations triviales $a = \left(ai^{-1}\right) i = i^{-1}\,(ai)$ pour chaque inversible i, on ne peut espérer une unicité qu'en raisonnant *modulo* les inversibles. Ce raisonnement rendant triviale la factorisation de ces derniers, on préfère les exclure du problème de factorisation et, en conséquence, des briques "infactorisables".

[73] Aussi appelé *anthyphérèse*, signifiant *soustraire alternativement.*

DEF (irréductible). *Un **irréductible** de M est un élément qui n'est ni inversible*[74] *ni produit de deux non-inversibles.*

*Imposons A intègre. Un **irréductible***[75] *de l'anneau A est un irréductible du monoïde A^*, çàd un élément non nul et non inversible vérifiant les implications $\forall a, b \in A^*,\ ab = p \Longrightarrow \begin{cases} a \sim 1 \\ \text{ou} \\ b \sim 1 \end{cases}$.*

CEG EXO (fonctions non irréductibles). Soit f une fonction positive s'annulant. *Montrer que f n'est pas irréductible.*

SOL Tout d'abord, f est non inversible car s'annule. Il s'agit donc de factoriser f en produit de deux fonctions non inversibles, çàd s'annulant, ce qui est immédiat en écrivant $f = \sqrt{f}\sqrt{f}$.

EXO (irréductibles & lemme d'Euclide). Imposons M régulier. Soit $p \in M$ non inversible vérifiant le lemme d'Euclide. *Montrer que p est irréductible.*

SOL Soient $a, b \in M$ tels que $p = ab$. D'après le lemme d'Euclide, on a par exemple $p \mid a$, çàd $ab \mid a$, çàd (par régularité) $b \mid 1$, çàd $b \sim 1$.

EXO (irréductibilité & nombre de diviseurs). *Montrer que chaque élément d'un monoïde régulier est irréductible ssi il possède, modulo $\sim$, exactement deux diviseurs.*

SOL Imposons M régulier et soit $p \in M$.

$\boxed{\Longrightarrow}$ Il est clair que 1 et p sont des diviseurs de p, qui plus est distincts vu la non-association $p \not\sim 1$ (p est non inversible). Montrons que ce sont les seuls. Soit $d \mid p$, soit $d' \in M$ tel que $dd' = p$: puisque p n'est pas produit de deux non-inversibles, on a l'inversibilité de d (auquel cas on a fini) ou celle de d' (auquel cas on a les associations $d = d1 \sim dd' = p$, ce qui conclut).

$\boxed{\Longleftarrow}$ Si p est inversible, alors ses diviseurs sont inversibles et donc égaux *modulo* $\sim$ (à 1), ce qui est absurde. Soient $a, b \in M$ tels que $ab = p$. Alors a et b divisent p, donc sont associés chacun à 1 ou à p. Si les deux sont non inversibles, çàd si $a \sim p \sim b$, on aura alors les associations $p1 = ab \sim pp$, d'où (par régularité) l'absurde association $1 \sim p$.

Soit $a \in M$ non inversible. L'algorithme naïf de décomposition de a en produit d'irréductibles est le suivant : si a est irréductible, on a terminé, sinon a est le produit de deux non-inversibles et l'on peut boucler l'algorithme sur chacun de ces facteurs. En observant que, dans le second cas, chacun des facteurs divise *strictement* a (*modulo* $\sim$), on voit que l'algorithme terminera toujours ssi le monoïde ${}^{M}\!/_{M^\times}$ ne contient pas de suite strictement décroissante[76] pour $\mid$. C'est bien le cas quand $M = \mathbb{Z}^*$ vu les implications $\forall a, b \in \mathbb{Z}^*,\ \begin{cases} a \mid b \\ a \not\sim b \end{cases} \Longrightarrow |a| < |b|$. C'est aussi le cas si $M = k[X]^*$ vu l'implication similaire en remplaçant "modules" par "degrés". Précisons ce dernier point et décrivons les briques "infactorisables" de $k[X]$.

[74] On exclut les inversibles des irréductibles non pas parce que cela sauve l'unicité de la décomposition en produit d'irréductibles (c'est vrai, agréable mais anecdotique), on le fait tout simplement parce que les inversibles et les irréductibles se comportent très différemment.

[75] Un (nombre) ***premier*** est ainsi un irréductible *positif* de l'anneau $\mathbb{Z}$.

[76] *Culture HP* : on parle alors d'ordre ***noethérien***, par hommage à la mathématicienne allemande Emmy Noether.

Lemme (irréductibilité de polynômes). On se place dans l'anneau $k[X]$.

1. *Aucun polynôme irréductible n'est constant*[77].
2. *Chaque polynôme de degré* 1 *est irréductible.*
3. *Aucun polynôme irréductible n'a de racine, à moins qu'il ne soit de degré* 1.
4. *Chaque polynôme de degré* 2 *ou* 3 *est irréductible ssi il n'a pas de racines.*

DEM

1. Un polynôme irréductible étant non nul et non inversible, son degré ne vaut ni $-\infty$ ni 0, donc vaut au moins 1.
2. Soit P un polynôme de $k[X]$ de degré 1. N'étant pas constant, il est non nul et non inversible. Soient par ailleurs F, G deux polynômes tels que $P = FG$. Appliquer les degrés (c'est là qu'on utilise le cadre *corporel*[78]) donne $1 = \deg F + \deg G$ dans $\mathbb{N} \cup \{-\infty\}$, d'où $\binom{\deg F}{\deg G} \in \left\{\binom{1}{0}, \binom{0}{1}\right\}$; dans chacun des cas, l'un des facteurs est de degré nul, donc inversible.
3. Soit P un polynôme irréductible de degré autre que 1. Le premier point montrant $\deg P \geq 1$, on a $\deg P \geq 2$. Soit par l'absurde λ une racine de P : alors P est divisible par $X - \lambda$ (qui n'est pas inversible), le codiviseur $\frac{P}{X-\lambda}$ étant de degré $\deg P - \deg(X - \lambda) \geq 2 - 1$, *a fortiori* non inversible, donc P est produit de deux non-inversibles : *contradiction.*
4. Soit P un polynôme de degré 2 ou 3. (Noter que P n'est pas inversible.) On vient de voir qu'il n'était pas irréductible s'il s'annulait.

   Soient réciproquement F et G deux non-inversibles (çàd chacun de degré non nul) tels que $FG = P$. Ce dernier étant non nul, F et G sont également non nuls, donc chacun de leurs degrés vaut au moins 1. Enfin, leur somme valant $\deg P < 4$, ces degrés ne peuvent tous les deux valoir au moins 2, donc F ou G est de degré 1, d'où une racine pour $FG = P$.

Théorème (factorialité de $k[X]$). *Chaque polynôme non constant de* $k[X]$ *est produit de polynômes irréductibles, avec unicité*[79] modulo $\sim$ *à l'ordre des facteurs près.*

DEM Pour chaque polynôme P, notons fpi_P l'énoncé « P se factorise en produit d'irréductibles » et pour chaque naturel n abrégeons D_n l'énoncé $\forall P \in k_n[X] \setminus k$, fpi_P. Établissons $\forall n \in \mathbb{N}^*$, D_n par récurrence.

Puisque $k_1[X] \setminus k$ se réduit aux polynômes affines, l'énoncé D_1 découle du lemme.

Soit $n \in \mathbb{N}^*$ tel que D_n. Soit P un polynôme de degré $\in [|1, n+1|]$. Si P est irréductible, on a trivialement fpi_P ; imposons le contraire. La non-inversibilité de P permet alors d'évoquer deux polynômes non inversibles F, G tels que $P = FG$. Comme dans le lemme, les degrés de F et G valent au moins 1, donc (puisque $\deg P \leq n+1$) valent au plus n. On a finalement les appartenances $F, G \in k_n[X] \setminus k$ et l'on peut utiliser les hypothèses fpi_F et fpi_G qui, conjointement, impliquent fpi_P, ce qui conclut à D_{n+1}.

[77] Un polynôme irréductible est donc de degré au moins 1.

[78] on pourrait même remplacer k par un anneau intègre

[79] Même dans $\mathbb{Z}$, l'unicité ne tient que *modulo* $\sim$, vu par l'exemple les deux décompositions de $-6 = (-2)\,3 = 2\,(-3)$.

L'unicité se montre exactement comme dans l'anneau $\mathbb{Z}$: la présence d'une division euclidienne permet (*via* l'algorithme d'Euclide) d'établir une relation de Bézout entre deux quelconques éléments étrangers, cette dernière permet de montrer le lemme de Gauss, d'où le lemme d'Euclide et enfin l'unicité voulue (*cf.* cours de première année).

EG !!! $X^4+1=\left(X^4+2X^2+1\right)-2X^2$

RQ (noethérianité) (HP). Proposons une preuve (rédigée un peu lâchement) de l'existence dans les anneaux principaux à l'aide du langage *idéal*. On commence par établir que chaque ensemble non vide d'idéaux possède un élément maximal. Si ce n'était pas le cas, on pourrait construire dans un tel ensemble une suite strictement croissante, mettons $(a_1)\subsetneq(a_2)\subsetneq\cdots$; la réunion des (a_n) est alors un idéal, donc principal, mettons $=(g)$, donc $g\in\bigcup_n(a_n)$ tombe dans un (a_N), d'où les absurdes inclusions $(g)\subset(a_N)\subsetneq(a_{N+1})\subset\bigcup_n(a_n)=(g)$. Appliquons cela à l'ensemble $\mathcal{I}$ (supposé par l'absurde non vide) des idéaux (a) où a parcourt les éléments non nuls, non inversibles, qui ne sont *pas* produits d'irréductibles. Soit (m) maximal[80] dans $\mathcal{I}$: en particulier, m n'est pas irréductible, donc se décompose $m=ab$ en deux facteurs non inversibles, chacun divisant *strictement* m, d'où la stricte inclusion $(m)\subsetneq(a)$ et la non-appartenance $(a)\notin\mathcal{I}$ (a ne peut être nul sans que m le soit). Par conséquent, a se décompose en produits d'irréductibles, de même pour b, *a fortiori* pour leur produit $ab=m$, d'où $(m)\in\mathcal{I}$: *contradiction.*

PROP (irréductibles de $\mathbb{K}[X]$).
Les irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré 1.
Les irréductibles de $\mathbb{R}[X]$ sont d'une part les polynômes de degré 1*, d'autre part les polynômes de degré* 2 *sans racine réelle.*

DEM On a déjà vu que les polynômes de degré 1 et ceux de degré 2 sans racine étaient irréductibles.

Le fait que chaque polynôme complexe non constant s'annule[81] montre par une récurrence immédiate qu'un tel polynôme est produit de facteurs chacun de degré 1, donc ne saurait être irréductible à moins d'être associé à un tel facteur, çàd d'être de degré 1.

Soit $P\in\mathbb{R}[X]$ irréductible. Les racines complexes de P sont de deux types : les réelles (qui correspondent à des diviseurs de P de la forme $X-\lambda$ où λ est réel) et les autres (deux à deux conjuguées, dont les paires conjuguées correspondent[82] à des

[80] Exhiber un tel idéal "maximal" revient à exhiber un diviseur minimal, ce que l'on faisait (dans les cas particuliers de $\mathbb{Z}$ et des $k[X]$) en évoquant un module ou un degré minimal dans $\mathbb{N}$, évocation reformulant une récurrence. Le caractère principal permet donc d'effectuer une "récurrence" directement sur les idéaux sans se ramener dans $\mathbb{N}$. Un anneau (commutatif) sans suite strictement croissante d'idéaux est dit ***noethérien***.

[81] Sera établi au chapitre ? ? ?evn2 ? ? ? avec des outils de compacité.

[82] Pour chaque complexe λ non réel, on a en effet la factorisation

$$(X-\lambda)\left(X-\overline{\lambda}\right)=(X-\operatorname{Re}\lambda)^2+\underbrace{|\lambda|^2-|\operatorname{Re}\lambda|^2}_{>0}.$$

diviseurs de P de degré 2 sans racine réelle). Puisque P est irréductible, il est associé à l'un de ces diviseurs.

***EXO (irréductibles de $\mathbb{Z}[X]$).** *Montrer qu'un polynôme de $\mathbb{Z}[X]$ est irréductible ssi il est de contenu 1 et irréductible dans $\mathbb{Q}[X]$.*

Soit P un polynôme à coefficients relatifs dont on note c le contenu.

1. Supposons $c = 1$ et P irréductible dans $\mathbb{Q}[X]$.

   Le polynôme P étant non nul et non inversible dans $\mathbb{Q}[X]$, il est de degré 1 dans $\mathbb{Q}[X]$, donc[83] de degré 1 dans $\mathbb{Z}[X]$, donc est non nul et non inversible dans $\mathbb{Z}[X]$.

   Soit une décomposition $P = FG$ dans $\mathbb{Z}[X]$: c'est en particulier une décomposition dans $\mathbb{Q}[X]$, donc F ou G est inversible dans $\mathbb{Q}[X]$, donc est un rationnel non nul de $\mathbb{Z}[X]$, çàd est un relatif, mettons $f := F \in \mathbb{Z}$. Alors le contenu de $fG = P$ vaut d'une part f fois celui de G, d'autre part celui de P, à savoir 1, donc f divise 1, d'où l'inversibilité de F.

2. Supposons P irréductible de $\mathbb{Z}[X]$. Comme ci-dessus, P est non nul et non inversible dans $\mathbb{Q}[X]$ car P est degré au moins 1.

   Factorisons $P = c\frac{P}{c}$: comme $\deg \frac{P}{c} \geq 1$, le facteur de droite $\frac{P}{c}$ est non inversible, ce qui impose l'inversibilité de l'autre facteur c, çàd $c \sim 1$, çàd $c = 1$.

   Soit à présent une décomposition $P = FG$ dans $\mathbb{Q}[X]$. En notant f et g les plus petits dénominateurs communs des coefficients de F et de G respectivement, les polynômes fF et gG tombent dans $\mathbb{Z}[X]$ et sont chacun de contenu 1, donc (*cf.* un exercice section 2.2) leur produit fgP également ; or ce dernier a pour contenu $fg\ c = fg$, ce qui impose $f \sim 1 \sim g$ (dans $\mathbb{Z}$), de sorte que F et G sont déjà dans $\mathbb{Z}[X]$. L'irréductible de P montre alors l'inversibilité de F ou de G dans $\mathbb{Z}[X]$, donc l'un d'eux vaut ± 1, *a fortiori* est un inversible de $\mathbb{Q}[X]$, ce qui conclut.

2.4 Indicatrice d'Euler

DEF (fonction φ d'Euler). *On appelle* ***indicatrice d'*Euler** *l'application*

$$\varphi := \left\{ \begin{array}{ccc} \mathbb{N}^* & \longrightarrow & \mathbb{N}^* \\ n & \longmapsto & \mathrm{Card}\left\{a \in [|1,n|] \ ; \ a \wedge n = 1\right\} \end{array} \right. .$$

EG (indicatrice d'une puissance d'un premier). Soient p un premier et $k \geq 1$ un naturel. L'unique diviseur premier de p^k étant p, être non étranger à p^k revient à être multiple de p ; or[84] $\left[|1, p^k|\right]$ contient $\left\lfloor \frac{p^k}{p} \right\rfloor = p^{k-1}$ tels multiples, d'où l'égalité

$$\varphi\left(p^k\right) = p^k - p^{k-1}.$$

PROP (inversibles de $\mathbb{Z}/n$ et corollaires). Soient $n \in \mathbb{N}^*$ et $z \in \mathbb{Z}$.

[83] *Rappel* : *le degré est inchangé par extension des scalaires*, au sens où, pour chaque anneau commutatif B dont A est un sous-anneau, le degré d'un polynôme de $A[X]$ est celui de son image par le morphisme $A[X] \hookrightarrow B[X]$ induit par l'inclusion canonique $A \hookrightarrow B$.

[84] *Rappel* : le nombre de multiples de a dans $[1, N]$ vaut $\left\lfloor \frac{N}{a} \right\rfloor$.

1. *La classe* $\overline{z}$ *est inversible dans* ${}^{\mathbb{Z}}\!/_{n}$ *ssi* z *et* n *sont étrangers.*
2. *Le nombre d'inversibles de l'anneau* ${}^{\mathbb{Z}}\!/_{n}$ *vaut*
$$\varphi(n) = \text{Card } \left({}^{\mathbb{Z}}\!/_{n}\right)^{\times}.$$
3. *L'anneau* ${}^{\mathbb{Z}}\!/_{n}$ *est un corps ssi* n *est premier.*
4. *Si* z *est étranger à* n*, on a alors*
$$z^{\varphi(n)} = 1 \text{ modulo } n$$
5. *On a pour chaques* $a, b \in \mathbb{N}^*$ *étrangers l'égalité*
$$\varphi(ab) = \varphi(a)\,\varphi(b).$$

DEM.

1. Reprenons la preuve décrivant les générateurs du groupe additif ${}^{\mathbb{Z}}\!/_{n}$ (section **??**) : on y avait l'équivalence $z \wedge n = 1 \Longleftrightarrow \exists \lambda \in \mathbb{Z},\ \overline{\lambda z} = \overline{1}$. Or on a par ailleurs les équivalences
$$\exists \lambda \in \mathbb{Z},\ \overline{\lambda z} = \overline{1} \Longleftrightarrow \exists \lambda \in \mathbb{Z},\ \overline{\lambda}\overline{z} = \overline{1} \Longleftrightarrow \exists \Lambda \in {}^{\mathbf{Z}}\!/_{n},\ \Lambda\overline{z} = \overline{1} \Longleftrightarrow \overline{z} \in \left({}^{\mathbb{Z}}\!/_{n}\right)^{\times}.$$
2. Immédiat par définition de $\varphi(n)$ et d'après le point précédent.
3. L'anneau $A := {}^{\mathbb{Z}}\!/_{n}$ est un corps ssi $A^{\times} = A^*$, *i. e.* ssi $|A^{\times}| = |A^*|$, *i. e.* ssi $\varphi(n) = n - 1$, *i. e.* ssi chaque entier de $[\![1, n[$ est étranger à n, *i. e.* ssi n est premier[85].
4. Dans le groupe $\left({}^{\mathbb{Z}}\!/_{n}\right)^{\times}$, où tombe bien $\overline{z}$ d'après le premier point, le théorème de Lagrange donne $\overline{z}^{\text{Card}\left({}^{\mathbb{Z}}\!/_{n}\right)^{\times}} = \overline{1}$, çàd $z^{\varphi(n)} = 1$ *modulo* n.
5. En abrégeant $C_n := {}^{\mathbb{Z}}\!/_{n}$ pour chaque naturel n, on peut écrire[86] ? ? ?th chinois + gpe unités ? ? ?
$$\varphi(ab) = \text{Card}\, C_{ab}^{\times} = \text{Card } (C_a \times C_b)^{\times} = \text{Card}\left(C_a^{\times} \times C_b^{\times}\right) = \text{Card}\, C_a^{\times}\ \text{Card}\, C_b^{\times} = \varphi(a)\,\varphi(b).$$

RQ (généraliser le petit théorème de Fermat). Quand n est un premier p, le point (4) exprime le **petit théorème de Fermat** : $a^{p-1} = 1\ [p]$ pour chaque naturel a non multiple de p.

RQ (calcul de $\varphi(n)$). Le point (5) permet de calculer $\varphi(n)$ une fois connue la décomposition de n en facteurs premiers, grâce aux identités $\varphi\left(p^k\right) = p^{k-1}(p-1)$. Par exemple, on aura :
$$\begin{aligned}
\varphi(18!) &= \varphi\left(2^{16} \cdot 3^8 \cdot 5^3 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17\right) \\
&= \varphi\left(2^{16}\right)\varphi\left(3^8\right)\varphi\left(5^3\right)\varphi\left(7^2\right)\varphi(11)\,\varphi(13)\,\varphi(17) \\
&= 2^{15}1 \cdot 3^7 2 \cdot 5^2 4 \cdot (7 \cdot 6) \cdot 10 \cdot 12 \cdot 16 \\
&= 2^{26}3^9 5^3 7.
\end{aligned}$$

[85] Un démonstration directe est possible en utilisant l'identité de Bézout, cachée dans l'égalité $\left|A^{\times}\right| = \varphi(n)$.

[86] *Rappel* : on a pour chaques monoïdes M et N l'égalité $(M \times N)^{\times} = M^{\times} \times N^{\times}$.

Exercice (une identité utile). Soit $n \in \mathbb{N}^*$. *Montrer que* $\sum_{d|n} \varphi(d) = n$.

SOL On partitionne l'ensemble des n fractions $\frac{1}{n}, \frac{2}{n}, ..., \frac{n}{n}$ selon leur dénominateur minimal, lequel peut être n'importe quel diviseur de n (penser à $\frac{1}{d}$ pour chaque $d \mid n$). À $d \mid n$ fixé, les fractions irréductibles de dénominateur d sont celles de la forme $\frac{k}{d}$ pour k étranger à d (la fraction est irréductible) et tel que $k \in [|1, d]$ (puisque $0 < \frac{k}{d} \leq 1$), donc sont en nombre $\varphi(d)$.

Deux applications de cette identité sont proposées en exercices, l'une dans le calcul d'un déterminant, l'autre dans une preuve de la cyclicité des sous-groupes de k^* lorsque k est fini.

3 Le point des compétences

Formulaire

1. Généralités

- Un ***anneau*** est un quintuplet $\left(A, \overset{+}{0}, \overset{\times}{1}\right)$ où[87] :

1. le triplet $(A, +, 0)$ est un groupe additif[88] ;
2. la loi $\times$ (appelée la ***multiplication*** de A) est associative et admet 1 pour neutre (appelé l'***unité*** de A), au sens où chaques éléments a, b, c de A vérifient les égalités ;
$$a(bc) = (ab)c \text{ et } 1a = a = a1 \ ;$$
3. $\times$ se distribue sur $+$, au sens où chaques éléments a, b, λ, μ de A vérifient les égalités
$$\lambda(a+b) = \lambda a + \lambda b \text{ et } (\lambda + \mu)a = \lambda a + \mu a.$$

- Un anneau est dit ***commutatif*** si sa multiplication est commutative :

$$A \text{ commutatif} \overset{\text{déf.}}{\iff} \forall a, b \in A, \ ab = ba.$$

- Une ***algèbre*** est un sextuplet $\left(A, \overset{+}{0}, \overset{\times}{1}, \cdot\right)$ tel que :

1. $\left(A, \overset{+}{0}, \overset{\times}{1}\right)$ est un anneau ;
2. $\left(A, \overset{+}{0}, \cdot\right)$ est un espace vectoriel ;
3. $\times$ et $\cdot$ sont compatibles au sens de l'"associativité" suivante : pour chaque scalaire λ et pour chaques vecteurs a et b, on a les égalités
$$\lambda \cdot (a \times b) = (\lambda \cdot a) \times b = a \times (\lambda \cdot b), \text{ produit noté tout simplement } \lambda ab.$$

[87] *Mméno* : on retrouve les quatre axiomes d'un espace vectoriel en remplaçant la multiplication interne de l'anneau par celle externe de l'espace vectoriel.

[88] En pratique, on ne mentionne jamais l'opposition $a \mapsto -a$ de l'anneau.

• Un anneau est dit ***intègre*** s'il est non nul, commutatif et si le produit de chaques éléments non nuls reste non nul :

$$A \text{ intègre} \overset{\text{déf.}}{\iff} \left\{ \begin{array}{c} 1 \neq 0 \quad \text{et} \quad A \text{ commutatif} \\ \forall a, b \in A,\ ab = 0 \Longrightarrow \text{ou} \left\{ \begin{array}{l} a = 0 \\ b = 0 \end{array} \right. \end{array} \right. .$$

Dans ce cas, on peut alors simplifier par chaque élément non nul :

$$A \text{ intègre} \Longrightarrow \left[\begin{array}{c} \forall s \in A^* \\ \forall a, b \in A \end{array} \ , \ \left\{ \text{ou} \begin{array}{l} as = bs \\ sa = sb \end{array} \right. \Longrightarrow a = b \right].$$

• Un ***corps*** est un anneau non nul commutatif où chaque élément non nul est inversible.

• *Exemples* : soient I un intervalle réel, E un $\mathbb{K}$-espace vectoriel, S un ensemble et $n \in \mathbb{N}$. Alors :

Sont des corps $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$.

Sont des anneaux intègres $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{K}[X]$ et $\mathbb{K}[X_1, X_2, ..., X_n]$.

Sont des $\mathbb{K}$-algèbres $\mathbb{K}$, $\mathbb{K}[X]$, $L(E)$, $M_n(\mathbb{K})$, $\mathbb{K}^S$, $\mathbb{K}^{\mathbb{N}}_{cv}$ (suites scalaires convergentes), $C^n(I, \mathbb{K})$ et $D^n(I, \mathbb{K})$ (fonctions scalaires de classe C^n, resp. n fois dérivables), $\mathbb{K}[X_1, X_2, ..., X_n]$.

Tous ces anneaux sont commutatifs sauf peut-être $M_n(\mathbb{K})$ et $L(E)$.

2. Créations de structures

• **Anneau produit** : chaque produit cartésien d'anneaux est un anneau pour les lois "coordonnée par coordonnée"

$$\begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_\ell \end{pmatrix} \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_\ell \end{pmatrix} = \begin{pmatrix} a_1 b_1 \\ a_2 b_2 \\ \vdots \\ a_\ell b_\ell \end{pmatrix} \qquad \text{et} \qquad (a_i)_{i \in I} (b_i)_{i \in I} = (a_i b_i)_{i \in I} .$$

• Un ***sous-anneau*** est une partie contenant les neutres (0 et 1) et qui est stable par addition, oppposition et multiplication. Une telle partie est alors un anneau pour les lois induites par l'anneau de base :

$$S \text{ sous-anneau de } A \iff \left\{ \begin{array}{l} 0 \in S \text{ et } \boxed{1 \in S} \text{ (à ne pas oublier !)} \\ \forall s, t \in S, \left\{ \begin{array}{c} s + t \in S \\ -s \in S \\ st \in S \end{array} \right. \end{array} \right. \Longrightarrow S \text{ anneau pour les lois de } A.$$

• Une ***sous-algèbre*** est un sous-anneau qui est aussi un sous-espace vectoriel, çàd est une partie contenant les neutres[89] (0 et 1) et stable par combinaisons linéaires et par produits. Une telle partie alors une algèbre pour les lois induites par l'algèbre de base :

$$S \text{ sous-algèbre de } A \iff \left\{ \begin{array}{l} 0 \in S \text{ et } \boxed{1 \in S} \text{ (à ne pas oublier !)} \\ \forall s, t \in S \\ \forall \lambda \in \mathbb{K} \end{array} \ , \ \left\{ \begin{array}{c} \lambda s + t \in S \\ st \in S \end{array} \right. \right. \Longrightarrow S \text{ algèbre pour les lois de } A.$$

[89] Ne pas oublier l'unité !

- Un ***sous-corps*** est un sous-anneau qui est un corps.

3. Morphismes

- Un ***morphisme d'anneaux*** est une application entres anneaux qui préserve les lois et les neutres :

$$f : A \longrightarrow B \text{ morphisme d'anneaux} \iff \left\{ \begin{array}{ll} A \text{ et } B \text{ anneaux} & \\ \boxed{f(1) = 1} & \text{(à ne pas oublier !)} \\ \forall a, b \in G, & f(a+b) = f(a) + f(b) \\ & f(ab) = f(a) f(b) \end{array} \right. .$$

- Chaque morphisme d'anneaux préserve le zéro ainsi que l'opposition :

$$f : A \longrightarrow B \text{ morphisme d'anneaux} \Longrightarrow \left\{ \begin{array}{l} f(0_A) = 0_B \\ \forall a \in A,\ f(-a) = -f(a) \end{array} \right.$$

- Un ***morphisme d'algèbres*** est un morphisme d'anneaux qui est aussi un morphisme d'espaces vectoriels.

- *Exemples* : soient A un anneau, S un ensemble, $s \in S$, $n \in \mathbb{N}$ et $a \in A^n$. Alors

Sont des morphismes d'anneaux : l'itération de l'unité $\left\{ \begin{array}{ccc} \mathbb{Z} & \longrightarrow & A \\ z & \longmapsto & z \cdot 1 \end{array} \right.$, l'évaluation $\left\{ \begin{array}{ccc} A^S & \longrightarrow & A \\ f & \longmapsto & f(s) \end{array} \right.$ (fonctionnelle) en s, l'évaluation $\left\{ \begin{array}{ccc} A[X_1, X_2, ..., X_n] & \longrightarrow & A \\ P & \longmapsto & P(a) \end{array} \right.$ (polynomiale) en a.

Sont des morphismes d'algèbres la limite $\left\{ \begin{array}{ccc} \mathbb{K}^{\mathbb{N}}_{cv} & \longrightarrow & \mathbb{K} \\ s & \longmapsto & \lim s \end{array} \right.$, les évaluations $\left\{ \begin{array}{ccc} \mathbb{K}^S & \longrightarrow & \mathbb{K} \\ f & \longmapsto & f(s) \end{array} \right.$ et $\left\{ \begin{array}{ccc} \mathbb{K}[X_1, X_2, ..., X_n] & \longrightarrow & \mathbb{K} \\ P & \longmapsto & P(a) \end{array} \right.$.

- Le ***noyau*** d'un morphisme d'anneaux est son noyau vu en tant que morphismes de groupes *additifs*. Chaque morphisme d'anneaux est injectif ssi son noyau vaut le singleton *nul* :

$$\text{si } f \ : \ A \longrightarrow B \text{ morphisme d'anneaux, alors } \left\{ \begin{array}{l} \operatorname{Ker} f = \{a \in A \ ; \ f(a) = 0\} \\ f \text{ injectif } \iff \operatorname{Ker} f = \{0\} \end{array} \right. .$$

Toutefois, $\boxed{\operatorname{Ker} f \textit{ n'est pas un sous-anneau !}}$ (sauf si B est l'anneau nul)

- Un ***isomorphisme d'anneaux*** est un morphisme d'anneaux bijectif. La réciproque de chaque isomorphisme d'anneaux reste un isomorphisme d'anneaux :

$$f \text{ isomorphisme d'anneaux} \iff \left\{ \begin{array}{l} f \text{ morphisme d'anneaux} \\ f \text{ bijection} \end{array} \right. \Longrightarrow f^{-1} \text{ isomorphisme d'anneaux.}$$

4. Idéaux

Soit A un anneau commutatif.

• Un ***idéal***[90] de A est un sous-groupe additif stable par multiplication par[91] chaque élément de A :

$$I \text{ idéal de } A \overset{\text{déf.}}{\iff} \begin{array}{c} \forall i,j,k \in I \\ \forall a \in A \end{array} \quad , \quad \begin{array}{c} ai+jk \in I \\ 0 \in I \end{array} \quad .$$

Par exempe, la partie $aA = Aa$ est un idéal pour chaque $a \in A$.

• Le noyau de chaque morphisme d'anneaux est un idéal (de l'anneau source) :

$$f : A \longrightarrow B \text{ morphisme d'anneaux} \Longrightarrow \operatorname{Ker} f \text{ idéal de } A.$$

• Les idéaux de l'anneau $\mathbb{Z}$ sont ses sous-groupes additifs :

$$I \text{ idéal de } \mathbb{Z} \iff \exists n \in \mathbb{N},\ S = n\mathbb{Z}.$$

• La ***divisibilité***[92] de A est la relation binaire formée des couples $(d,m) \in A^2$ tels que

$$d \mid m \overset{\text{déf.}}{\iff} \exists d' \in M,\ dd' = m. \qquad \left(\begin{array}{c} d \text{ et } d' \text{comme« } \mathbf{d}\text{iviseur »} \\ m \text{ comme « } \mathbf{m}\text{ultiple »} \end{array} \right)$$

En termes d'idéaux, on a pour chaques $d, m \in A$ l'équivalence

$$d \mid m \iff mA \subset dA.$$

5. Anneaux cycliques $\mathbb{Z}/n$

• On appelle ***indicatrice d'*Euler** l'application

$$\varphi := \left\{ \begin{array}{ccc} \mathbb{N}^* & \longrightarrow & \mathbb{N}^* \\ n & \longmapsto & \operatorname{Card}\{a \in [|1,n|] \ ;\ a \wedge n = 1\} \end{array} \right. .$$

• Pour évaluer φ sur des produits de premiers, on dispose des égalités

$$\begin{array}{rl} \forall p \text{ premier}, \forall \alpha \in \mathbb{N}^*, & \varphi(p^\alpha) = p^\alpha - p^{\alpha-1} \text{ et} \\ \forall a,b \in \mathbb{N}^*,\ a \wedge b = 1 \Longrightarrow & \varphi(ab) = \varphi(a)\varphi(b). \end{array}$$

• **Théorème d'Euler**. On a les congruences

$$\begin{array}{c} \forall n \in \mathbb{N}^* \\ \forall z \in \mathbb{Z} \end{array} \ ,\ z \wedge n = 1 \Longrightarrow z^{\varphi(n)} = 1 \textit{ modulo } n$$

En particulier, lorsque n est premier, on a $\varphi(n) = n-1$ et l'on retrouve le "petit théorème de Fermat".

Soit n un naturel.

[90] Observer l'analogie entre idéal (d'un anneau) et sous-espace vectoriel (d'un espace vectoriel).

[91] Comme dans les espaces vectoriels, la stabilité par opposition découle de celle par multiplication par -1.

[92] Le programme impose inutilement l'intégrité de A pour ces définition et équivalences.

- Le groupe $\mathbb{Z}/_n$ est un anneau commutatif pour la multiplication

$$(C,\Gamma) \overset{\times}{\longmapsto} \overline{c\gamma} \text{ pour n'importe quel } (c,\gamma) \in C \times \Gamma,$$
$$\text{laquelle vérifie alors } \forall a,b \in \mathbb{Z},\ \overline{a}\,\overline{b} = \overline{ab}.$$

En particulier, la projection canonique $a \mapsto \overline{a}$ est un morphisme d'anneaux.

- **Lemme chinois.** Soient a et b deux naturels étrangers. Est alors un isomorphisme d'anneaux

$$\left\{ \begin{array}{ccc} \mathbb{Z}/_{ab} & \xrightarrow{\sim} & \mathbb{Z}/_a \times \mathbb{Z}/_b \\ \overline{z} & \longmapsto & (\widetilde{z},\widehat{z}) \end{array} \right. .$$

- Les inversibles de l'anneau $\mathbb{Z}/_n$ sont les classes d'entiers premiers avec n :

$$\forall z \in \mathbb{Z},\ \left(\overline{z} \text{ inversible dans } \mathbb{Z}/_n\right) \Longleftrightarrow (z \wedge n = 1).$$

Leur nombre vaut par conséquent $\varphi(n)$.

- L'anneau $\mathbb{Z}/_n$ est un corps ssi n est premier.

6. Arithmétique polynomiale

Soit K un sous-corps de $\mathbb{C}$. Pour chaque polynôme P, abrégeons (P) l'idéal $K[X]P$.

- Chaque idéal de $K[X]$ est formé des multiples d'un certain polynôme :

$$I \text{ idéal de } K[X] \Longleftrightarrow \exists P \in K[X],\ I = (P).$$

- **P. g. c. d., Euclide, Bézout**. Soient $P, Q \in K[X]$. Ils admettent alors un p. g. c. d. (plus grand commun diviseur) défini par le polynôme <u>unitaire</u> $P \wedge Q$ tel que

$$(P) + (Q) = (P \wedge Q).$$

L'algorithme d'Euclide "étendu" permet alors d'expliciter deux polynômes $U, V \in K[X]$ tels que

$$P \wedge Q = PU + QV \text{ (identité de Bachet-Bézout)}$$

- **Lemmes de Gauss** : on a pour chaques polynômes A, B, D, M les implications

$$\left\{ \begin{array}{c} D \mid AB \\ D \wedge A = 1 \end{array} \right. \Longrightarrow D \mid B \quad \text{et} \quad \left\{ \begin{array}{c} A \wedge B = 1 \\ A, B \mid M \end{array} \right. \Longrightarrow AB \mid M$$

deux polynômes étrangers divisent un troisième polynôme ssi leur produit le divise.

- Un polynôme est dit ***irréductible*** s'il n'est ni inversible ni produit de deux non-inversibles :

$$P \text{ irréductible dans } K[X] \overset{\text{déf.}}{\Longleftrightarrow} \left\{ \begin{array}{c} P \text{ non constant} \\ \forall A, B \in K[X],\ \left[AB = P \Longrightarrow \exists \lambda \in K^*,\ \left\{ \begin{array}{l} P = \lambda A \\ \text{ou } P = \lambda B \end{array} \right. \right] \end{array} \right. .$$

- Les irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré 1.
- Les irréductibles de $\mathbb{R}[X]$ sont d'une part les polynômes de degré 1, d'autre part les polynômes de degré 2 sans racine réelle.
- Chaque polynôme non constant de $k[X]$ est produit de polynômes irréductibles unitaires, avec unicité à l'ordre des facteurs près.

Exercices d'entraînement