Anneaux & arithmétique (reliquat)

Marc SAGE

1er mars 2017

Table des matières

1 Exercices

★ **Monoïdes algébriques.** Soit $n \in \mathbb{N}^*$. Notons $\omega := e^{\frac{2\pi i}{n}}$ et $\mathbb{R}[\omega]$ l'espace vectoriel des polynômes réels évalués en ω. *Montrer que l'ensemble des endomorphismes de l'espace vectoriel* $\mathbb{R}[\omega]$ *qui préservent la multiplication forme un monoïde dont on déterminera la structure.*

SOL Soit σ un tel endomorphisme. Puisque $\omega^n = 1$, une division euclidienne par $X^n - 1$ montre que $\mathbb{R}[\omega]$ est linéairement engendré par $1, \omega, \omega^2, ..., \omega^{n-1}$, l'endomorphisme σ est donc déterminé par les images de ces derniers ; préservant par ailleurs la multiplication, σ est caractérisée par $\sigma(\omega)$, laquelle image vérifie $\sigma(\omega)^n = \sigma(\omega^n) = \sigma(1) = 1$ et est donc une puissance de ω.

Réciproquement, on vérifie que pour chaque entier $k \in [|0, n[$ l'endomorphisme σ_k de $\mathbb{R}[\omega]$ qui envoie ω^i sur $(\omega^k)^i$ convient. Il est par ailleurs aisé d'établir $\sigma_p \circ \sigma_q = \sigma_{pq}$ pour chaques entiers $p, q \in [0, n[$, ce montre que le monoïde trouvé est isomorphe à celui multiplicatif $\mathbb{Z}/_n$.

★ **Groupes algébriques.** *Soit* $n \in \mathbb{N}^*$. *Notons* $\omega := e^{\frac{2\pi i}{n}}$ *et* $\mathbb{R}[\omega]$ *l'espace vectoriel des polynômes réels évalués en* ω. *Alors l'ensemble des automorphismes de l'espace vectoriel* $\mathbb{R}[\omega]$ *qui préservent de la multiplication forme un groupe.*

SOL Il s'agit de la version "groupes" de l'exercice *Monoïdes algébriques* où l'on avait obtenu le monoïde multiplicatif $\mathbb{Z}/_n$. Le groupe cherché est donc celui des inversibles de $\mathbb{Z}/_n$ (qui sera décrit au chapitre ? ? ?).

1.1 Anneaux – Corps – Algèbre

1.1.1 anneaux booléens

Montrer qu'est commutatif chaque anneau dont chaque élément est idempotent.

Solution proposée. Remarquons déjà que l'idempotence de 2 entraîne sa nullité (écrire $2 = 2^2 - 2$). Ensuite, étant donnés deux éléments a et b, on peut faire apparaître le défaut de commutativité $[a, b] := ab - ba \overset{2=0}{=} ab + ba$ dans le carré $(a + b)^2$, ce qui donne

$$[a, b] = (a + b)^2 - a^2 - b^2 = (a + b) - a - b = 0, \textit{ CQFD.}$$

1.1.2 Morphismes et homothéties

À quelle condition une homothétie dans un anneau commutatif en est-elle un endomorphisme ?

SOL Soit une homothétie $\lambda\cdot$ qui est un morphisme d'anneaux. L'additivité ne posant aucun problème[1], utilisons la multiplicativité : pour chaques a, b dans A on doit avoir $\lambda(ab) = (\lambda a)(\lambda b) = \lambda^2 ab$; prenant $a = b = 1$, on voit que λ est un idempotent, condition qui réciproquement suffit à la multiplicativité. En revanche, pour préserver l'unité, l'image λ de 1 doit valoir 1. Finalement, seule l'identité convient.

1.1.3 Caractéristiques

Un anneau de caractéristique nulle peut-il être fini ?
Un corps de caractéristique positive peut-il être infini ?

SOL

Un anneau de caractéristique nulle contient un sous-anneau isomorphe à $\mathbb{Z}$, donc contient un ensemble infini, donc est infini.

Le corps $\mathbb{F}_2$ est de caractéristique 2, il en est de même pour l'anneau $\mathbb{F}_2[X]$ et pour le corps $\mathbb{F}_2(X)$ qui sont infinis (chacun contient la suite injective des puissances de X).

1.1.4 Sous-anneaux

Soit S une partie d'un anneau A. *Montrer l'équivalence de :*

1. *S est un sous-anneau de A ;*
2. *S contient 1 et est stable par addition, soustraction et multiplication ;*
3. *S contient -1 et est stable par addition et multiplication.*

SOL

$1 \Longrightarrow 2$ Le sous-anneau S, étant stable par addition et opposition, est stable par soustraction $(a, b) \mapsto a + (-b)$.

$2 \Longrightarrow 3$ Étant stable par soustraction, S contient $1 - 1 = 0$, donc contient $0 - 1 = -1$.

$3 \Longrightarrow 1$ Étant stable par multiplication, S contient $(-1)^2 = 1$; étant stable par addition, il contient $1 + (-1) = 0$; enfin, la stabilité par $\times$ implique celle par opposition $a \mapsto (-1)a$.

[1] la distributivité dans un anneau s'exprime exactement en disant que toutes ses homothéties sont additives

1.1.5 Anneaux "exotiques"

Montrer que les polynômes rationnels à termes constants entiers forment un anneau $\mathbb{Z}+X\mathbb{Q}[X]$ *(et plus généralement* $\mathbb{Z}_n[X]+X^{n+1}\mathbb{Q}[X]$ *pour chaque naturel* n*).*

SOL On se place dans l'anneau $\mathbb{Q}[X]$. Soit $n\in\mathbb{N}$. Abrégeons $I:=\left(X^{n+1}\right)$. Le sous-groupe $\mathbb{Z}_n[X]$ et l'idéal I sont des sous-groupes additifs de $\mathbb{Q}[X]$, donc leur somme est un groupe. Ce dernier contient $\mathbb{Z}_n[X]\ni -1$. Il reste à montrer sa stabilité par multiplication. Or, d'une part le produit de deux polynômes de $\mathbb{Z}_n[X]$ tombe dans $\mathbb{Z}_{2n}[X]\subset\mathbb{Z}_n[X]+I$, d'autre part les trois autres termes du développement de $(\mathbb{Z}_n[X]+I)^2$ sont multiples de I, donc inclus dans I puisque ce dernier est un idéal.

1.1.6 Algèbres de convolution

Soit M un monoïde. On définit le ***support*** de chaque $f\in\mathbb{K}^M$ par

$$\operatorname{Supp} f:=\{m\in M\ ;\ f(m)\neq 0\}.$$

On note $\mathbb{K}^{(M)}$ les applications de $\mathbb{K}^M$ à support fini indexées par M. On y définit le ***produit de convolution*** (ou ***produit de Cauchy***) par

$$(f,g)\overset{*}{\mapsto}\left(m\mapsto\sum_{ab=m}f(a)\,g(b)\right).$$

Montrer l'inclusion $\operatorname{Supp}(f*g)\subset\operatorname{Supp} f\operatorname{Supp} g$ *pour chaques* $f,g\in\mathbb{K}^{(M)}$ *et trouver un neutre pour* $*$*. En déduire que l'espace vectoriel* $\mathbb{K}^{(M)}$ *est une algèbre pour le produit de convolution*[2]*.*

SOL Soient $f,g\in\mathbb{K}^{(M)}$ et $m\in M$.

Tout d'abord, la somme $\sum_{ab=m}f(a)\,g(b)$ fait sens car les seuls couples (a,b) y contribuant vérifient $f(a)\,g(b)\neq 0$, çàd $\begin{cases} f(a)\neq 0\\ g(b)\neq 0\end{cases}$, donc tombent dans $(\operatorname{Supp} f)(\operatorname{Supp} g)$ qui est fini (par finitude des supports de f et de g). Ceci montre que la fonction $f*g$ fait sens dans $\mathbb{K}^M$. Par ailleurs, si $m\in\operatorname{Supp}(f*g)$, la somme ci-dessus est non nulle, donc l'un de ses termes est non nul, d'où un $(a,b)\in M^2$ tel que $\begin{cases} f(a)\,g(b)\neq 0\\ ab=m\end{cases}$, d'où $m\in(\operatorname{Supp} f)(\operatorname{Supp} g)$ comme ci-dessus.

Montrons enfin que le Dirac en 1 (notons-le δ) est neutre pour $*$: dans la somme $[f*\delta](m)=\sum_{ab=m}f(a)\,\delta_b^1$, le seul b contribuant vaut 1, ce qui impose $a=m$ et il ne reste que $f(m)$ (idem pour $\delta*f$).

La distributivité de $+$ sur $*$ et la compatibilité des multiplications sont immédiates vu la forme de la sommande.

RQ Le produit de convolution possède une version continue. On dira qu'une fonction $f\in\mathbb{K}^{\mathbb{R}}$ est ***à support compact*** si elle s'annule en-dehors d'un segment.

[2] Lorsque $M=\mathbb{N}$, on retrouve l'anneau des polynômes $\mathbb{K}[X]=\mathbb{K}^{(\mathbb{N})}$.

Notons $C_c^\infty(\mathbf{R},\mathbf{K})$ le s.-e. v. de $C^\infty(\mathbf{R},\mathbf{K})$ formé des fonctions de $\mathbb{K}^{\mathbb{R}}$ à support compact. On défini alors le ***produit de convolution*** sur $C_c^\infty(\mathbf{R},\mathbf{K})$ par

$$f*g : x \mapsto \int_{t\in\mathbb{R}} f(t)\, g(x-t)\, dt.$$

On montre alors que $*$ *est commutatif, associatif et n'a pas de neutre.* (Le "neutre" serait un ***Dirac*** centré en 0.) Le produit de convolution permet d'éclairer la théorie de Fourier ainsi que le théorème de Stone-Weierstrass.

1.1.7 "auto"-sous-anneau

Trouver un anneau qui est isomorphe à l'un de ses sous-anneaux stricts.

SOL On doit clairement chercher dans les anneau infinis. Des anneaux classiques sont les anneaux de polynômes $P_I := \mathbb{Z}[(X_i)]_{i\in I}$ pour chaque ensemble I : il est immédiat de vérifier que P_I et P_J sont isomorphes dès que I et J sont équipotents. Ainsi, en choisissant un ensemble d'indéterminées qui soit équipotent à l'une de ses parties strictes (par exemple $I := \mathbb{Z} \simeq \mathbb{N} =: J \subsetneq I$), on obtient un isomorphisme de P_I sur le sous-anneau strict P_J.

1.1.8 Sous-trucs & morphismes

Soient M un truc et S une partie de M. *Montrer qu'il y a au plus une structure de truc sur S telle que l'inclusion canonique de S dans M soit un morphismes de trucs.*

SOL On utilise l'exercice analogue sur les monoïdes & groupes.

anneaux & corps. Notons $\left(M, \substack{0\\+}, \substack{1\\\times}\right)$ la structure d'anneau de M et soit $\left(S, \substack{z\\p}, \substack{u\\f}\right)$ une structure d'anneau. L'inclusion canonique $S \hookrightarrow M$ est un morphisme de groupes additifs, donc $\binom{z}{p}$ coïncide avec $\binom{0}{+}$; de même, $S \hookrightarrow M$ est un morphisme de monoïdes multiplicatifs, donc $\binom{u}{f}$ coïncide avec $\binom{1}{\times}$.

espaces vectoriels Notons $\left(M, \substack{0\\+}, \cdot\right)$ la structure d'espace vectoriel de M et soit $\left(S, \substack{z\\p}, \circ\right)$ une structure d'espace vectoriel. Comme ci-dessus, on a $\binom{z}{p} = \binom{0}{+}$. Par ailleurs, l'inclusion canonique $S \overset{i}{\hookrightarrow} M$ étant linéaire, pour chaque $s \in S$ et pour chaque scalaire λ, on a $\lambda \circ s = \lambda \circ i(s) = i(\lambda \cdot s) = \lambda \cdot s$, donc les actions $\circ$ et $\bullet$ coïncident.

algèbres Utiliser les deux paragraphes précédents.

1.1.9 Nombres algébriques

Soit c un complexe annulé par un polynôme rationnel non nul. *Montrer que l'algèbre $\mathbb{Q}[c]$ est un corps.*

SOL Le noyau $\operatorname{Ker}\operatorname{eval}_c$ de l'évaluation en c est un idéal de $\mathbb{Q}[X]$, donc (par principalité) est de la forme (μ) pour un certain $\mu \in \mathbb{Q}[X]$.

Montrons que μ est irréductible. Par hypothèse, l'idéal (μ) est non nul, donc μ est non nul. Puisque c n'est pas annulé par le polynôme 1, l'idéal (μ) n'est pas plein, donc μ n'est pas inversible. Soient enfin $A, B \in \mathbb{Q}[X]$ tels que $\mu = AB$: on a alors $0 = \mu(c) = [AB](c) = A(c)B(c)$, d'où (par intégrité) la nullité de $A(c)$ ou de $B(c)$, disons $A(c) = 0$, çàd $A \in \operatorname{Ker}\operatorname{eval}_c$, çàd $A \in (\mu)$, çàd $\mu \mid A$, çàd $AB \mid A$, çàd (en simplifiant par A qui ne peut être nul sans que μ le soit) $B \mid 1$, ou encore $B \sim 1$.

L'algèbre $\mathbb{Q}[c]$ est non nulle (elle contient $\mathbf{Q}$) et clairement commutative. Soit $a \in \mathbb{Q}[c]^*$, soit $A \in \mathbb{Q}[X]$ tel que $a = A(c)$. Puisque $A(c) \neq 0$, le polynôme A n'est pas dans $\operatorname{Ker}\operatorname{eval}_c = (\mu)$, donc μ ne divise par A, donc (par irréductibilité) est étranger à lui, d'où (par Bézout) deux polynômes U et V tels que $AU + \mu V = 1$. Évaluer en c donne $A(c)U(c) + 0V(c) = 1$, çàd $aU(c) = 1$, d'où l'inversibilité de a.

1.1.10 Algèbre des fractions

Soit A un anneau intègre, soit S une partie de A stable par multiplication (même vide). On définit sur $A \times S$ une relation $\sim$ par

$$\binom{a}{s} \sim \binom{\alpha}{\sigma} \overset{\text{déf.}}{\iff} \sigma a = s\alpha.$$

1. *Montrer que $\sim$ est une relation d'équivalence.* Le quotient ${}^{A\times S}\diagup_{\sim}$ sera noté $A\left[\frac{1}{S}\right]$, la classe d'un (a,s) sera notée $\frac{a}{s}$.
2. *Montrer que le quotient $A\left[\frac{1}{S}\right]$ est trivial si S contient* 0. On impose désormais $0 \notin S$.
3. *Montrer l'égalité $\frac{\sigma a}{\sigma s} = \frac{a}{s}$ pour chaque $(a,s,\sigma) \in A \times S^2$.*
4. *Montrer que les lois $\left(\frac{a}{s}, \frac{\alpha}{\sigma}\right) \overset{+}{\mapsto} \frac{a\sigma + s\alpha}{s\sigma}$ et $\left(\frac{a}{s}, \frac{\alpha}{\sigma}\right) \overset{\times}{\mapsto} \frac{a\alpha}{s\sigma}$ munissent $A\left[\frac{1}{S}\right]$ d'une structure d'anneau.*
5. *Montrer que l'anneau A se plonge dans $A\left[\frac{1}{S}\right]$ via $a \mapsto \frac{a}{1}$ et que les éléments de la partie S (vue à travers ce plongement) sont inversibles*[3] *dans $A\left[\frac{1}{S}\right]$. Exemple ?*

SOL

1. La réflexivité de $\sim$ découle de la commutativité de A, la symétricité de $\sim$ vient de celle de $=$, reste la transitivité. Soient $a, \alpha, \mathfrak{a} \in A$ et $s, \sigma, \mathfrak{s} \in S$ tels que $\begin{cases} \binom{a}{s} \sim \binom{\alpha}{\sigma} \\ \binom{\alpha}{\sigma} \sim \binom{\mathfrak{a}}{\mathfrak{s}} \end{cases}$. On a alors $\begin{cases} \sigma a = s\alpha \\ \mathfrak{s}\alpha = \sigma\mathfrak{a} \end{cases}$, multiplier donne $\sigma a \mathfrak{s} \alpha = s\alpha\sigma\mathfrak{a}$, d'où (en simplifiant par $\sigma\alpha$ par intégrité) $a\mathfrak{s} = \mathfrak{a}s$, çàd $\binom{a}{s} \sim \binom{\mathfrak{a}}{\mathfrak{s}}$.

[3] On rajoute ainsi formellement à A l'inverse de chaque élément de S et l'on considère l'algèbre engendrée suite à ce rajout : il s'agit bien de l'A-algèbre engendré par les "inverses" des éléments de S, d'où la notation.

2. Si S contient 0, alors chaque couple de $A \times S$ est équivalent à $(0,0)$ vu l'égalité $0=0$.
3. Soit $(a,s,\sigma) \in A \times S \times S$. Puisque σ est non nul, il est régulier, d'où les équivalences

$$\binom{\sigma a}{\sigma s} \sim \binom{a}{s} \iff s\sigma a = \sigma s a \iff sa = sa, \text{ ce qu'on a.}$$

4. Soient $\binom{a}{s} \sim \binom{a'}{s'}$ et $\binom{\alpha}{\sigma} \sim \binom{\alpha'}{\sigma'}$ dans $A \times S$. En réécrivant

$$\begin{cases} \frac{a\alpha}{s\sigma} = \frac{(s'\sigma')a\alpha}{(s'\sigma')s\sigma} = \frac{(as')(\alpha\sigma')}{ss'\sigma\sigma'} \\ \frac{a'\alpha'}{s'\sigma'} = \frac{(s\sigma)a'\alpha'}{(s\sigma)s'\sigma'} = \frac{(a's)(\alpha'\sigma)}{ss'\sigma\sigma'} \end{cases} \text{ et } \begin{cases} \frac{a\sigma+s\alpha}{s\sigma} = \frac{(s'\sigma')(a\sigma+s\alpha)}{(s'\sigma')s\sigma} = \frac{(as')\sigma\sigma'+(\alpha\sigma')ss'}{ss'\sigma\sigma} \\ \frac{a'\sigma'+s'\alpha'}{s'\sigma'} = \frac{(s\sigma)(a'\sigma'+s'\alpha')}{(s\sigma)s'\sigma'} = \frac{(a's)\sigma\sigma'+(\alpha'\sigma)ss'}{ss'\sigma\sigma} \end{cases},$$

on voit que les hypothèses $\begin{cases} as' = a's \\ \alpha\sigma' = \alpha'\sigma \end{cases}$ donnent les égalités $\begin{cases} \frac{a\alpha}{s\sigma} = \frac{a'\alpha'}{s'\sigma'} \\ \frac{a\sigma+s\alpha}{s\sigma} = \frac{a'\sigma'+s'\alpha'}{s'\sigma'} \end{cases}$; les dénominateurs restant par ailleurs dans S (ce dernier étant stable par multiplication), les "lois" proposées font sens. Les axiomes d'un anneau s'établissent aisément par le calcul, le zéro valant $\frac{0}{1}$ et l'unité $\frac{1}{1}$ (cela fait sens car S contient le produit vide 1).
5. Notons $i : a \mapsto \frac{a}{1}$. Cette application conserve clairement l'addition et la multiplication (simple calcul) et est injective vu les à $a \in A$ fixé les équivalences

$$a \in \operatorname{Ker} i \iff \frac{a}{1} = \frac{0}{1} \iff a1 = 1 \cdot 0 \iff a = 0.$$

Alors un élément $s \in S$ est envoyé sur $\frac{s}{1}$ qui est inverse de $\frac{1}{s}$. Un exemple est d'imposer $S = A^\times$: l'anneau $A\left[\frac{1}{A^\times}\right]$ sera alors un corps[4].

1.1.11 De l'intuition pour inverser $1+a$

1. *Soient dans un anneau un inversible i et un nilpotent n qui commutent. Montrer que $i+n$ est aussi inversible. Contre-exemple sans la commutativité ?*
2. *Soient a et b deux éléments d'un anneau A tel que $1-ab$ soit inversible. Montrer que $1-ba$ est aussi inversible.*

Solution proposée.

1. Vu que[5] $i+n = i\left(1+\frac{n}{i}\right)$ et que $\frac{n}{i}$ est nilpotent (si $n^k=0$, alors on a $\left(\frac{n}{i}\right)^k = \frac{n^k}{i^k} = \frac{0}{i^k} = 0$), il suffit de traiter le cas $i=1$.

   On intuite alors l'inverse à l'aide de la formule « physicienne »

$$\frac{1}{1-x} = 1 + x + x^2 + x^3 + \cdots$$

[4] En "inversant" chaque élément non nul, il est naturel d'obtenir un corps.

[5] la commutativité de u et n légitime la notation $\frac{n}{u}$ pouvant signifier nu^{-1} ou $u^{-1}n$

dont le membre de droite a le bon goût de faire sens pour x nilpotent. On vérifie alors que $1-n+n^2-n^3+...+(-1)^k n^k$ est bien l'inverse de $1+n$:

$$(1+n)\sum_{i=0}^{k}(-1)^i n^i=\sum_{i=0}^{k}(-1)^i n^i+\sum_{i=0}^{k}(-1)^i n^{i+1}.$$

En décalant l'indice de la seconde somme (on a mis le premier terme de côté) $\sum_{i=0}^{k}(-1)^i n^{i+1}\overset{j:=i+1}{=}1+\sum_{j=0}^{k-1}(-1)^{j-1}n^j$, on trouve 1 moins l'opposé de la première somme (le facteur d'indice k ne contribue pas à la somme), ce qui conclut.

(Attention, nous n'avons montré l'inversibilité que d'un seul côté : pour nous dispenser de l'autre côté, on peut dire que, notre inverse étant un polynôme en n, il commute trivialement avec $1+n$.)

Pour un contre-exemple, en cherchant dans les matrices 2×2, on trouve que l'inversible $\begin{pmatrix}1&1\\ \cdot&1\end{pmatrix}$ plus le nilpotent $\begin{pmatrix}\cdot&\cdot\\ 1&\cdot\end{pmatrix}$ n'est pas inversible (sanity check : ils ne commutent pas).

2. On va intuiter l'inverse toujours à l'aide de la formule

$$\frac{1}{1-x}=1+x+x^2+x^3+\cdots.$$

On l'applique de façon complètement non rigoureuse à $x=ba$ et on fait apparaître l'inverse i de $1-ab$:

$$\begin{aligned}\frac{1}{1-ba}&=1+ba+baba+bababa+...\\&=1+b(1+ab+abab+ababab+...)a\\&=1+b\frac{1}{1-ab}a\\&=1+bia.\end{aligned}$$

On pose donc $j:=1+bia$ et on vérifie à la main que ça marche :

$$\begin{aligned}(1-ba)j&=(1-ba)(1+bia)=1+bia-ba-babia=1-ba+b1ia-babia\\&=1-ba+b\underbrace{(1-ab)i}_{=1}a=1-ba+ba=1\end{aligned}$$

et pareil de l'autre côté :

$$j(1-ba)=(1+bia)(1-ba)=1-ba+bia-biaba=1-ba+b[i(1-ab)]a=1.$$

Remarque. L'erreur est classique de ne vérifier qu'un sens pour les inverses car l'on raisonne trop souvent sur l'anneau $M_n(K)$ où cela est suffisant. On pourra méditer sur les tapis roulants de $\mathbb{R}^{\mathbb{N}}$

$$\left\{\begin{array}{l}\gamma:(a_0,a_1,...)\mapsto(a_1,a_2,...)\\ \delta:(a_0,a_1,...)\mapsto(0,a_0,a_1,...)\end{array}\right.,$$

lesquels vérifient $\gamma\delta = 1 \neq \delta\gamma$.

Remarque. Le même énoncé tient en remplaçant inversible par inversible à droite/gauche.

1.1.12 Idempotents et factorisations d'anneaux

Le cadre est celui d'un anneau commutatif appelé A. On dit qu'un anneau est ***décomposable*** s'il est isomorphe au produit de deux anneaux non nuls, ***indécomposable***[6] sinon

1. *Montrer qu'un idéal est un anneau pour les lois induites ssi il est engendré par un idempotent.*
2. *Montrer que l'application « compléménter à* 1 *» est une involution sans point fixe des idempotents de* A *(* modulo *un cas pathologique à préciser).*
3. *Soient* i *et* j *deux idempotents de somme* 1*. Montrer que* A *est isomorphe à l'anneau produit* $iA \times jA$*.*
4. *Montrer que* A *est indécomposable ssi ses seuls idempotents sont triviaux (*0 *et* 1*). Exemples ?*

   On dit qu'une famille (a_i) d'éléments de A est ***orthogonale*** si le produit $a_x a_y$ est nul pour chaques $x \neq y$.
5. *Soient* i_x *des idempotents orthogonaux en nombre fini. Montrer que la somme des* i_x *est idempotente. En déduire un idempotent orthogonal à chaque* i_x*.*
6. *Soient* $i_1, ..., i_n$ *des idempotents orthogonaux en nombre maximal. Montrer que* A *est isomorphe au produit* $\prod_{x=1}^{n} i_x A$*.*

Solution proposée.

1. Soit i un idempotent. L'idéal (i) est un sous-groupe additif (c'est immédiat) stable par multiplication (grâce à l'idempotence de i) et possède i pour neutre (pour la même raison). Attention à dire que ce n'est pas un sous-anneau de l'anneau de départ car ils n'ont pas la même unité[7].

   Soit réciproquement I un idéal qui soit un anneau. Notons i son unité et montrons (comme suggéré par ce qui précède) que $I = (i)$. D'une part l'idéal $(i) = iA$ est inclus dans I (car I est stable par $i\cdot$), d'autre part chaque élément $x \in I$ vaut son produit par l'unité i, d'où l'inclusion réciproque $I \subset iA$.
2. Soit i idempotent. L'idempotence de $1 - i$ est immédiate :

$$(1-i)^2 = 1^2 - 2i + i^2 = 1 - 2i + i = 1 - i.$$

[6] Cela revient à dire que toute factorisation (isomorphisme) $A \simeq A_1 \times \cdots \times A_n$ est triviale, au sens où les A_i sont alors tous nuls sauf un qui vaut A (à isomorphisme près).

[7] à moins bien sûr que $i = 1$

Si i et $1-i$ devaient coïncider, multiplier par i donnerait $i^2 = i(1-i) = 0$, donc $i = i^2$ serait nul et l'on aurait $1 - i = 1 \overset{?}{\neq} 0 = i$, ce qui est une contradiction dans un anneau non nul[8].

3. Comment envoyer A sur $iA \times jA$? Il est facile d'envoyer A sur iA (prendre l'homothétie de rapport i), donc il est naturel d'essayer le produit $\pi : a \mapsto (ia, ja)$ des homothéties de rapport i et j. C'est clairement un morphisme d'anneaux (grâce aux idempotences de i et j). Montrons qu'il est bijectif : si a est un antécédent d'un $(ix, iy) \in iA \times jA$, alors sommer les coordonnées de $(ia, ja) = \pi(a) = (ix, jy)$ donne $a = ix + jy$, ce qui d'une part montre l'injectivité de π et d'autre part donne l'antécédent de chaque élément de $iA \times jA$ (c'est immédiat à vérifier une fois observée la nullité du produit $ij = i(1-i) = i - i^2$).

4. Si on peut « casser » $A \simeq B \times C$ avec B et C non nuls (*i. e.* $1 \neq 0$ dans chacun), alors les éléments $(1, 0)$ et $(0, 1)$ sont des idempotents non triviaux. Observer alors les isomorphismes $B \simeq (1, 0)A$ et $C \simeq (0, 1)A$.

   Réciproquement, si i est un idempotent non trivial, alors la synthèse suggère de considérer l'idempotent $j := 1 - i$ (il est non trivial sinon i serait trivial) ainsi qu'un éventuel isomorphisme $A \overset{?}{\simeq} iA \times jA$ (les deux facteurs sont non nuls car contiennent chacun d'une part 0 et d'autre part i ou j) ; or la question 3 de l'exercice précédent nous donne une telle factorisation, ce qui conclut.

   Vu qu'un idempotent i est caractérisé par la relation $i^2 = i$, chaque anneau *intègre* est indécomposable, par exemple $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}[X]$. Par ailleurs, chaque produit $A \times B$ admet deux idéaux maximaux distincts $\mathfrak{m}_A \times B$ et $A \times \mathfrak{m}_B$ (où $\mathfrak{m}_R$ est un idéal maximal de l'anneau non nul R), donc ne peut être local[9] : par contraposée, chaque anneau *local* est indécomposable.

5. Le calcul est immédiat (dans le carré de la somme, les termes croisés disparaissent par orthogonalité) :

$$\left(\sum_x i_x\right)^2 = \sum_x i_x^2 + \sum_{x \neq y} i_x i_y = \sum_x i_x + 0.$$

   Étant donné un seul idempotent i, la question 2 nous suggère $1 - i$. Avec plusieurs idempotents i_x orthogonaux, l'analogue serait $1 - \sum i_x$. C'est bien un idempotent en tant que complément à 1 de l'idempotent $\sum i_x$. Montrons qu'il est orthogonal à chaque i_x : cela résulte de l'égalité $i_\xi \sum_x i_x = \sum_x \delta_x^\xi i_x = i_\xi$ pour chaque ξ.

6. Tentons le même raisonnement qu'à la question 3. Il est déjà clair que le produit des homothéties de rapport i_x est un morphisme d'anneaux surjectif (grâce à l'orthogonalité des i_x). Son injectivité viendrait de ce que la somme des i_x fasse 1 (même argument : un élément $a \in A$ vaut la somme des coordonnées de son image). Il s'agit donc de montrer que la différence $\delta := 1 - \sum i_x$ est nulle. D'après la question précédente, δ est un idempotent orthogonal à chaque

[8] Dans l'anneau nul $\{0\}$, l'unique élément est idempotent et fixe par toute les applications de $\{0\}$ dans $\{0\}$.

[9] Un anneau commutatif est dit ***local*** lorsqu'il admet un unique idéal maximal. Le quotient par cet idéal est alors appelé ***corps résiduel***.

i_x, donc par maximalité doit valoir l'un d'eux, disons $\delta = i_\xi$; mais alors δi_ξ est nul par orthogonalité et vaut i_ξ par idempotence, d'où $0 = \delta = i_\xi$, *CQFD*

1.2 Arithmétique

1.2.1 RSA

1.2.2 $(\mathbf{Z}/2^n)^\times$ cyclique ?

non ssi n≥ 3 et si 2<–p ?

1.2.3 Divisibilité "additive"

Décrire la relation de divisibilité dans le monoïde $(\mathbb{N}, +)$.

SOL Dans ce monoïde, un élément a "divise" un élément b ssi $\exists n \in \mathbb{N},\ b = a + n$, çàd ssi $b \geq a$. On retrouve ainsi l'ordre usuel.

1.2.4 Polynômes positifs

1. *Soit P un polynôme à coefficients réels qui est partout positif. Montrer que P s'écrit comme la somme $A^2 + B^2$ de deux carrés de polynômes.*
2. *Montrer que chaque polynôme réel positif sur $\mathbb{R}_+$ est de la forme $A^2 + XB^2$ pour certains polynômes A et B.*

Solution proposée.

1. L'idée est que, P ne changeant pas de signe, chaque facteur $X - \lambda$ le divisant doit apparaître un nombre pair de fois (sinon P change de signe autour de λ). ? ? ?détailler ? ? ? Quant aux racines complexes, elles sont deux à deux conjuguées car P est à coefficients réels. On peut donc casser P dans $\mathbb{C}$ sous la forme
$$P = \prod (X - \lambda_i)^2 \prod \left(X - \xi_j\right)\left(X - \overline{\xi_j}\right).$$
Un œil aguerri réécrira cela sous la forme
$$P = Q\overline{Q} \text{ avec } Q := \prod (X - \lambda_i) \prod \left(X - \xi_j\right).$$
Il suffit de faire apparaître les parties réelle et imaginaire de $Q = A + Bi$ pour conclure :
$$P = Q\overline{Q} = (A + iB)(A - iB) = A^2 + B^2.$$

Autre idée : une fois noté que l'ordre de chaque racine réelle de P est pair (sinon P changerait de signe), on peut factoriser P dans $\mathbb{R}$ sous la forme

$$\prod_{\lambda}(X-\lambda)^2\prod_{(a,b)}\left((X-a)^2+b^2\right)=\prod_{(A,B)}\left(A^2+B^2\right).$$

Or, les sommes de deux carrés sont stables par multiplication d'après l'identité de Lagrange $\left(a^2+b^2\right)\left(c^2+d^2\right)=(ac+bd)^2+(ad-bc)^2$, ce qui conclut. Signalons que cette dernière n'est qu'une réécriture de la multiplicativité du module complexe $|a+ib|^2\,|c+id|^2=|(a+ib)(c+id)|^2$, ce qui montre que les deux solutions sont fondamentalement les mêmes.

2. Même idée : on scinde $P=\prod_{\lambda}(X-\lambda)\prod_{(a,b)}\left((X-a)^2+b^2\right)$. Les racines positives sont d'ordre pair, donc on peut écrire P comme un carré par un $\prod_c\left(X+c^2\right)$ par un $\prod_{(a,b)}\left((X-a)^2+b^2\right)$. Or, les A^2+XB^2 sont stables par multiplication d'après Bramaguptha (qui généralise Lagrange) : $\left(a^2+\lambda b^2\right)\left(c^2+\lambda d^2\right)=(ac+\lambda bd)^2+\lambda(ad-bc)^2$.

Remarque. *Quid* du résultat pour *plusieurs* indéterminées ? Hilbert a observé que ce n'est toujours pas le cas. Par exemple, le polynôme $X^2Y^2\left(X^2+Y^2-1\right)+1$ est positif mais n'est pas somme de deux carrés.

1.2.5 Déterminants arithmétiques

Pour chaques naturels i,j, on note $d_{i,j}$ le nombre de diviseurs communs à i et j. *Calculer pour chaque naturel n les déterminants des matrices* $(d_{i,j})_{1\leq i,j\leq n}$ *et* $(i\wedge j)_{1\leq i,j\leq n}$

Solution proposée.

L'idée est d'écrire la matrice concernée comme un produit de deux matrices dont le déterminant est plus ou moins trivial à calculer.

Définir une matrice $A:\binom{p}{q}\mapsto\begin{cases}1\text{ si }q\mid p\\0\text{ sinon}\end{cases}$ permet d'écrire (à i,j fixés)

$$d_{i,j}=\sum_{\substack{k|i\\k|j}}1=\sum_{k=1}^{n}a_{i,k}a_{j,k}=\sum_{k=1}^{n}[A]_{i,k}\left[{}^tA\right]_{k,j}=\left[A\,{}^tA\right]_{i,j}.$$

La matrice A étant triangulaire, son déterminant est le produit de ses coefficients diagonaux, d'où $\det A=1$, qui est du coup la valeur du déterminant cherché.

De même, définir une matrice $\Phi:\binom{p}{q}\mapsto\begin{cases}\varphi(q)\text{ si }q\mid p\\0\text{ sinon}\end{cases}$ permet d'écrire (à i,j fixés)

$$i\wedge j=\sum_{k|i\wedge j}\varphi(k)=\sum_{\substack{k|i\\k|j}}\varphi(k)=\sum_{k|i}\varphi(k)\,a_{j,k}=\sum_{k=1}^{n}[\Phi]_{i,k}\left[{}^tA\right]_{k,j}=\left[\Phi\,{}^tA\right]_{i,j}.$$

La matrice Φ étant triangulaire, le déterminant cherché vaut $\prod_{k=1}^{n} \varphi(k)$.

Remarque. Recourir à l'identité $n = \sum_{d|n} \varphi(d)$ n'est pas si astucieux que ça. En effet, ce qui compte était d'exprimer $i \wedge j$ comme une somme sur plusieurs conditions (dans notre cas $k \mid i$ et $k \mid j$) et d'introduire les matrices correspondantes à ces conditions en priant pour qu'elles soient « gentilles ». En ce sens, l'indicatrice d'Euler ne joue aucun rôle particulier.

1.2.6 Cyclicité du groupe multiplicatif d'un corps fini

Soit k un corps, soit G un sous-groupe fini de k^*. *En classifiant les éléments de G selon leur ordre, montrer que G est cyclique.*

Solution proposée.

Notons n l'ordre du groupe G. Chaque élément de G a un ordre (fini) divisant n. Pour chaque $d \mid n$, on notera Ω_d l'ensemble des éléments de G d'ordre d. On a alors une partition $G = \coprod_{d|n} \Omega_d$.

Fixons un diviseur $d \mid n$ et un élément $g \in \Omega_d$. Les d itérés $1, g, g^2, ..., g^{d-1}$ sont distincts et racines du polynôme $X^d - 1$, donc l'ensemble des racines $X^d - 1$ est ? ? ?corps=>d racines ? ? ? exactement l'engendré $\langle g \rangle$, ce qui montre que ces engendrés (lorsque g décrit Ω_d) sont les mêmes :

$$\forall a \in \Omega_d,\ \langle a \rangle = \left\{ \text{racines de } X^d - 1 \right\}.$$

Soit de plus $\gamma \in \Omega_d$. Alors γ appartient à $\langle \gamma \rangle = \langle g \rangle$, donc s'écrit g^k pour un certain naturel k. En introduisant le p. g. c. d. $\delta := d \wedge k$, les égalités $\gamma^{\frac{d}{\delta}} = \left(g^k\right)^{\frac{d}{\delta}} = \left(g^d\right)^{\frac{k}{\delta}} = 1$ montrent que l'ordre d de γ divise $\frac{d}{\delta}$, d'où $\delta = 1$. Chaque élément de Ω_d s'écrit donc comme une puissance de g première avec d, d'où l'inclusion

$$\Omega_d \subset \left\{ g^k \ ;\ d \wedge k = 1 \right\}.$$

En prenant les cardinaux, on obtient la majoration $|\Omega_d| \leq \varphi(d)$. (? ? ?en fait les éléments d'ordre n sont les générateurs de $Z\left(X^d - 1\right)$)

Or, les Ω_d partitionnant G, on doit avoir

$$n = |G| = \sum_{d|n} |\Omega_d| \leq \sum_{d|n} \varphi(n) = n,$$

ce qui force l'égalité partout : en particulier, $|\Omega_n| = \varphi(n) > 0$, d'où l'existence d'un élément d'ordre n et la cyclicité de G.

Remarque. Un corollaire immédiat est la cyclicité de k^* pour chaque corps fini k.

RQ : utiliser l'exposant $G \subset Z\left(X^M - 1\right)$? ? ?

1.2.7 Incompatibilité de $\sim$ et $+$

Soit A un anneau intègre. *Montrer que son association est compatible avec son addition ssi son groupe des unités est trivial. Donner un exemple de tel anneau qui ne soit pas un corps.*

SOL

Lorsque $A^\times$ est trivial, l'association $\sim$ devient l'égalité $=$ qui est compatible avec n'importe quelle loi.

Supposons $\sim$ et $+$ compatibles. Soit $a \in A^\times$: les trois éléments $1, -1, a$ étant inversibles, on a les associations $\left\{ \begin{array}{c} 1 \sim a \\ -1 \sim 1 \end{array} \right.$, d'où (par compatibilité) $1 - 1 \sim a + 1$, d'où $0 \mid a + 1$, ied $a + 1 = 0$, ied $a = -1$, d'où l'inclusion $A^\times \subset \{-1\}$ et la trivialité attendue.

L'inclusion précédente impliquant l'égalité $2 = 0$, il faut chercher dans les anneaux de caractéristique 2, par exemple $\mathbf{F}_2[X]$. Son groupe des inversible étant $\mathbf{F}_2[X]^\times = \mathbf{F}_2^\times = \{1\}$, on a fini.