Anneaux
(version chantier)

Marc SAGE

<2015

Table des matières

Le mot anneau est issu de annelus, diminutif du latin anus de même sens. Il apparaît en français au Moyen-Âge, d'abord sous la forme anel puis vers 1830 avec l'orthographe actuelle.

Son utilisation en mathématiques date de la fin du XIXème siècle. Son nom, **Ring** en allemand, lui a été donné par David Hilbert em 1894. Il avait hésité avec **Integrität Bereich**, **domaine d'intégrité**. Kronecker avait proposé **Art**, **espèce** et Dedekind **ordre d'un module**. Les mathématiciens allemands introduisent la plupart des axiomatisations de structures algébriques. *Faisant suite au mot groupe, ils utilisèrent des termes relatifs à des groupements organisés. Aussi, plus la strcture est complexe, plus le mot correspond à une structure mathématique riche. Le mot allemand Ring signifie anneau mais désigne aussi un cartel ou un groupement d'entreprises. Le mot corps est choisi par Dedekind en référence aux corps d'armée.* Anneau, traduit en français, n'a plus la connotation allemande et paraît bien orphelin entre le cartel d'entreprises et le corps d'armée.

(extrait de *Les mots et les maths*, de B. Hauchecorne)

Abraham Fraenkel introduisit dans sa thèse de doctorat publiée en 1914 pour la première fois l'axiomatique des ***anneaux*** (motivé par un travail en 1912 pour axiomatiser les nombres p-adiques)

(source Léo Corry p207)

Un élément qui n'est pas un diviseur de zéro est appelé ***régulier*** par Fraenkel 1912

(source Léo Corry p208)

EG

$(Z, +, \times)$

$(N, \min, \max)$? ? ? ?

$(N, \min, +)$

1 Structure annelée

On s'intérese à $\mathbb{Z}$ mais en fait jsute ses propriétés.

1.1 def

Définition : *On appelle* anneau *tout ensemble* A muni de deux lois de composition internes, notées $+$ et $\times$, vérifiant :

- $(A, +)$ est un groupe abélien
- $\times$ est associative
- $\times$ est distributive par rapport à $+$, c'est-à-dire

$$\begin{aligned} \forall x, y, z &\in A,\ x \times (y + z) = x \times y + x \times z \\ \forall x, y, z &\in A,\ (x + y) \times z = x \times z + y \times z \end{aligned}$$

de manière plus concise, un anneau est un groupe additif (abélien) agissant sur lui-même de façon asoc et distributive.

De plus, l'anneau A est dit :

- *commutatif si la loi $\times$ est commutative*
- *unitaire*[1] *si la loi $\times$ admet un élément neutre.*

Rq : Si A unitaire, le $+$ est automatiquement abélien :

$$a + b + a + b = 1\,(a + b) + 1\,(a + b) = (1 + 1)\,(a + b) = (1 + 1)\,a + (1 + 1)\,b = a + a + b + b$$

COmment transformer un groupe en anneau ? Avec une multiplication nulle. (on parle d'anneau *de carré nul*, puisqu'alors $A^2 = AA = \{a\alpha\}_{a,\alpha \in A} = \{0\}$)

[1] On dit parfois *unifère*. Le suffixe -fère (ou -ifère), comme dans "prolifère" et "somnifère", vient de 'ferre'. Ainsi, *unifère* signifie *qui porte une unité*.

D'ailleurs, un groupe non abélien ainsi annelisé ne donne pas d'unité !

Par la suite, tous les anneaux seront unitaires. C'est la convention le plus souvent adoptée, de sorte qu'un ensemble $(A, +, \times)$ est un anneau ssi $(A, +)$ groupe et $(A, \times)$ monoïde.

Lorsque l'unité vient à manquer, comme $2\mathbb{Z}$, on utilise le terme de **pseudo-anneau** : $(A, +)$ est un groupe et $(A, \times)$ un magma. Exemepl : la convolution (le neutre devrait être un dirac, donc une distribution)

Si ce sont les symétriques qui manquent, on rate la moité des éléments : $(A, +, \times)$ est un **semi-anneau** si $(A, +)$ et $(A, \times)$ monoïdes (on pourait donc dire **bioïde**) avec la condition de distributivité.

On note usuellement, comme dans l'anneau de référence $\mathbb{Z}$ muni des lois de l'arithmétique usuelle :
- $a - b$ pour $a + (-b)$
- $a \cdot b$ (ou même ab) pour le produit $a \times b$
- 0_A (ou 0) le neutre pour la loi $+$
- 1_A (ou 1) le neutre pour la loi $\times$ si l'anneau A est unitaire
- nx l'itéré n fois de l'élément x pour la loi $+$ ($n \in \mathbb{Z}$), avec la convention $0x = 0_A$
- x^n l'itéré n fois de l'élément x pour la loi $\times$ ($n \in \mathbb{N}$), avec la convention $x^0 = 1_A$
- x^{-n} l'itéré n fois de l'élément x^{-1} (pour la loi $\times$) si x est inversible ($n \in \mathbb{N}$)

$0a = a0 = 0$ (attention pas comm..)

Règle des signes : pourquoi moins par moins fait plus ? le voir comme une symétrique centrale sur la droite entière.

Factorisation : 2bett+3bett=(2+3)bett=5bett

corps : anneau (unitaire) commutatif où $A^\times = A \setminus \{0\}$. (vient de Körper, Field)

Ambiguité de la terminologie –> parler de **corps gauche** si commutativité pas supposée, ou bien d'anneau / **algèbre à division** (division ring en anglais)

1.2 anneau poduit

On parle de ***loi produit*** ainsi que d'***anneau produit***. Les opérations se faisant coordonée par coordonnée, les vérifications d'usage sont triviales.

On peut étendre la définition de l'anneau produit à une famille quelconque d'anneaux $(A_i, +_i, \times_i)_{i \in I}$ indexée par un ensemble I non vide.

rq : dans anneau produit, il y a des élément de produit nul : on dit qu'ils sont ***orthogonaux***

Ainsi, dansun produit, les anneaux sont deux à deux orthogonaux.

Pourquoi autoriser $1 = 0$? Si A est un anneau et X un ensemble, on a envie que l'ensemble A^X des applications de X dans A muni de l'addition et la multiplication point par point soit un anneau, avec ta définition, il faudrait exclure le cas X vide pour s'assurer que A^X reste non nul, c'est grotesque

1.3 Sous anneaux

sous truc : préserve le zéro, la somme, les opposés, l'unité (souvet oublié !) et le produit

!!!EXO les "sous-anneaux" avec autre unité sont les Ai pour i idempotent

B sous anneau ssi contient $0, 1$ stable par somme produit et passage à l'opposé

rq :

B sous anneau ssi $1 \in B$, $B - B \subset B$, $BB \subset B$

B sous anneau ssi $-1 \in B$, $B + B \subset B$, $BB \subset B$

EG : $\mathbb{Z}[i]$, $\mathbb{Q}[\sqrt{2}]$

Généralement, on donne l'exemple pour les anneaux, pour attirer l'attention sur le fait qu'« être un sous-anneau » impose bien d'avoir la même unité : si A et B sont deux anneaux, alors $A \times B$ est un anneau dont le neutre multiplicatif est $(1, 1)$; l'ensemble des couples $A \times \{0\}$ est sous-groupe additif stable par multiplication,

d'ailleurs c'est même un idéal, qui est isomorphe à A en tant que groupe additif muni d'une multiplication, mais qui n'est pas un sous-anneau de $A \times B$ parce que son unité est $(1,0)$ au lieu de $(1,1)$.

Plus petit sous-annéeu de A ? –> **sous-annaeau premier**, Z ou Z/nZ, **caractéristique**. On parle de carac **nulle** ou en carc **positive** (cf anglais)

l'anneau $\mathbb{Z}$ agit sur A par $k \cdot a := \underbrace{a + a + \cdots + a}_{k \text{ fois}}$, de façon distributive sur l'addition et compatible avec la multiplication (au sens où $k \cdot (a \times b) = (k \cdot a) \times b = a \times (k \cdot b)$). Ces propriétés, en plus de celles de l'anneau A, résument le fait que tout anneau est une $\mathbb{Z}$-algèbre.

1.4 morphismes

$f\left(\sum a_i\right) = \sum f\left(a_i\right)$
$f\left(\prod a_i\right) = \prod f\left(a_i\right)$
$f\left(a^n\right) = f\left(a^n\right)$
$f\left(na\right) = nf\left(a\right)$
ker n'est pas un sous-anneaux ! il ne contient pas 1 qui ennvoyé sur 1. Donc sous-anneaux mauvaise notion –> **idéaux**

Eg : A commutatif ssi le carré est morphisme

rq : on a toujours un morphisme $\mathbb{Z} \longrightarrow A$ (d'image le sous-anneau premier) : on dit que Z est un **objet initial** de la catégorie des anneaux.

rq : un morphisme d'anneaux de but intègre est unitaire (ou nul). Plus généralement, on peut remplacer intègre par **indécomposable** (on dit aussi **connexe**). Réciproque : si tout morphisme +x vers B est unitaire, alors B est indéocmposable.
rq : un morphisme d'anneaux entre K-algèbres qui stabile K n'est pas nécessairement d'algèbres (à cause de l'automorphise de K)
rq : mono + épi n'impique pas iso, prendre $Z \hookrightarrow Q$ mono (car inj) épi (soient φ etψ morhisme coinidant sur Z ; puisque $1 = a\varphi\left(\frac{1}{a}\right) = f\left(\frac{1}{a}\right)a$, tous les enteiers $\neq 0$ sont inverbles dans A : soit $\frac{a}{b} \in Q$, on a $\varphi\left(\frac{a}{b}\right) = \frac{\varphi(a)}{b} = \frac{\psi(a)}{b} = \psi\left(\frac{a}{b}\right)$)

1.5 groupes des unités

Le **groupe des inversibles**, ou des **unités**, est $A^\times$.
unité –> penser à ± 1 dans Z.
LASSE : $1 = 0$, 0 inverseible, $A = \{0\}$.
=> interdiction de smplifier par 0 (sauf cas trivial).

rappeler $\left(\prod A_i\right)^\times = \prod A_i^\times$
élément **réguliers**

EXO : *un pseudo-anneau est unifère ssi il y a deux éléments a et b tels que les homothéies $a\cdot$ et $\cdot b$ sont bijectives.*
=> claire (prendre $a = b = 1$, alors les homo sont Id)
<= la composée $a \cdot b$ est bij, donc atteint $ab = aeb$, d'où $a = ae$ puis $ax = aex$ done $x = ex$; idem en partnat de$b = eb$ => $xb = xeb$ => $x = xe$. Donc e neutre

1.6 intégrité

on est habitué à ce que $ab = 0$ ssi a ou $b = 0$ dans un anneau : c'est honnete de leur part, ils sont dits *intègres* (les autrse anneaux sont *fourbes*, ils nous trompent)

diviseurs de zéros, élément **réguliers** : PROP *un élément est régulier ssi il ne divise pas* 0

(Vieux) un **domaine d'intégrité** (en anglais **domain**) est un anneau sans diviesures de zéros. Le caractère unitaire ou commutatif est conventionnel et discutable

intègre = domaine d'intégrité NON NUL.

non nul n'est pas une convention : aussi indispensable que de dire qu'un corps n'est pas nul

EG : $\mathbb{ZQRC}$ sont intègres, un corps est intègre,

CEG : les nilpotents

CEG : l'intégrité ne passe pas au produit : A^X(χ_P et $\chi_{^cP}$ sont de produit nul pour P partie propre de A, ok car A a au moins 2 éléments car $A \neq \{0\}$)

CEG : anneau de produit nul, algèbre de matrices (cf fin de cours)

RQ ce sont les seules obstructions à l'intégrité (nilpotence & décomposabilité) (cf exo sur idéaux radicaux)

EG : si $A = C^\infty(R)$, les div de 0 sont les fonctions s'annulant au moins sur un intervalle infini.

EXO : *inversible d'un côté et régulier de l'autre => inversible tout court* (si $ab = 1$, on a $(1 - ba)\, b = 0 = a\,(1 - ba)$, d'où $1 - ab = 0$ en simplifiant par a ou b)

EXO : *mq un domaine d'intégrité est unifère ssi il y a une homothétie surjective.*

DEM : => clair (prendre Id). <= soit $a\cdot$ un telle homo surj. Elle atteint a, mettons $ae = a$, d'où $(\times x)$ $aex = ax$, puis $(a\div)$ $ex = x$, d'où $(x\times)$ $xex = xx$ et $(\div x)$ $xe = x$.

COR : *tout domaine d'intégrité FINI est un corps gauche*

DEM : tout les homothétie sont injectives, donc surjectives, donc il y a une unité ; alors les homothéties atteignent 1, donc tout le monde est inversibles.

Si A intègre de carc positive, car est un premier. Alors Fr est un morphisme

CNS pour qu'un anneau se plonge dans un corps ? intégrité nécesaire, et me^me sufisante –> **corps des frations**

Autre point de vue : quels éléments peut-on inverser ? CEux qui ne divisent pas 0 (afin de ne pas avoir de 0 en dénom) –> **anneau des fractions.**

1.7 idempotents

idempotent : on a toujours 0 et 1, appelés idempotents triviaux. EXo : *il y en a d'auttre ssi A produit.*

compléter à 1 est une involution des idempotents, sans point fixe (sauf dans anneau nul) (si $i = 1 - i$, on a $2i = 1$, d'où $i = 2i^2 = 2i$ et $i = 0$ puis $i = 1 - i = 1$)

EXO : *mq idéal engendré par un idepotent est un anneau pour les loi induites (attention à l'unité !)*

Mq $i + j = 1$ => $A \approx iA \times jA$.

Généraliser à idempotents orthogonaux maximal. ($1 - \sum a_i$ idempotent orthogonal à tous les autres, donc vaut un a_i, mais lu étant orthognaol il estnul). On a donc $A \approx \prod(a_j)$).

EXO : *un anneau où tout le monde est idempotent est commutatif.*

$ab + ba = (a + b)^2 - a^2 + b^2 = 0$, puis $2 = 2^2 - 2 = 0$, d'où $ba = -ab = ba$.

se généralise avec 2 remplcé par 3 (cf feuille exo), par un entier qcq, et même dépendant de l'élément a (Jacobson).

Anneau dit **booléen** ou **de Boule** -> cf exo pour classification dans le cas fini.

1.8 Idéaux

Intro : dans $\mathbb{Z}$, on a la DFI (factoriel). Fructueux pour étudier somme de deux carés d'introduire $\mathbb{Z}[i]$ (entiers de Gauss, $i^2 = -1$) qui véirie aussi cela (on a même une division euclidienne). Pour résoudre FLT, on a commencé par essayer pareil, avec $\mathbb{Z}\left[i\sqrt{3}\right]$ pour $x^3+y^3 = z^3$: pb, la DFI n'est plus unique : $2\times 2 = 4 = \left(1+i\sqrt{3}\right)\left(1-i\sqrt{3}\right)$ avec que des irréductibles.

Plus générament, Lamé introduit $\mathbb{Q}(\zeta)$ où ζ racine de l'unité, et regarde l'annaux des entiers sur ce corps. Encore un échec : pas factoriel. Kummer exhibe un ceg pour racine 23e.

Une manière d'interpréter cette difficulté consiste à considérer qu'il manque des nombres pour assurer l'unicité de la décomposition en facteurs premiers. Kummer définit des nombres **idéaux** palliant les manques et permettant d'exprimer une nouvelle forme de théorème fondamental de l'arithmétique. L'idée est de plonger A dans $\mathfrak{P}(A)$ via $a \mapsto aA$, lequel est un sous-groupe additif stable par toute homothétie de A. Il pourrait y en avor d'autres !

Dedeking reprend et esaie de montrer que tout idéal est produit d'idéaux premiers, ce qui conduit à la défiiton des anneaux de Dedekind (hors sujet).

Déf : **idéal** = sous groupa additif stable par homothétie : $0 \in I,\ I - I \subset I,\ AI \subset I$.
idéal **princpal** est un aA (pas si idéal que ça !)

Rq : si I idéeal, on a équivalences
I contient 1 ssi I contient une unité ssi I vaut tout l'anneau
Rq : idéal et sous-anneau sont notions orthogonal, au sens où idéal + sous-anneau => tout l'anneau.
Rq : Cependant, idéal + "sous-anneau" sans me^me unité => principal idempotent

introduire $(a) = Aa$, $(a_1, ..., a_n) = Aa_1 + ... + Aa_n$, $(a_i) = \sum Aa_i$, puis $\sum I_i = (\bigcup I_i)$
EG : nZ, $R \times \{0\}$ dans R^2, fonctino s'annulant en un point (-> exos sur idéaux maximaux)
Noyau sont idéeaux.
COR (def de la carac) : unique entier n tel que $\mathrm{Ker}(Z \longrightarrow A) = nZ$.

Tout le vocab de divisibilité –> cf cours PLM

idéaux **premiers** => rend intègre
idéaux **maximaux** => rend corps, d'où preuve qui passent mieux (sans tensoriser)

EXO : $\mathfrak{p}$ premier ssi $\forall n,\ I_1 \cdots I_n \subset \mathfrak{p} \Rightarrow \exists k,\ I_k \subset \mathfrak{p}$ (c'est la def où on remplacer les éléméent par des idéaux et les $\in$ par des $\subset$)
DEM : => OPS $n = 2$. Si $\exists i \in I \setminus \mathfrak{p}$, alors $iJ \subset \mathfrak{p}$ implique par primalité $J \subset \mathfrak{p}$.
<= soit $ab \in \mathfrak{p}$. Alors $(a)(b) = (ab) \subset \mathfrak{p}$ car $\mathfrak{p}$ idéal, dnc p contient (a) (donc a) ou (b) (donc b
EXO : $\mathfrak{i}$ non premier => $\exists I, J$ tq $IJ \subset \mathfrak{i} \subset I \cap J$
DEM : soient $ab \in \mathfrak{i}$ mais $a, b \notin \mathfrak{i}$. Alors $\mathfrak{i} + (a)$ et $\mathfrak{i} + (b)$ conviennent

2 Divers

factoriel : dans $\mathbb{Z}\left[i\sqrt{3}\right]$, pas unicité $4 = 2 \times 2 = \left(1+i\sqrt{3}\right)\left(1-i\sqrt{3}\right)$.
dans $\mathbb{Z}\left[i\sqrt{5}\right]$, mq les éléments 3 et $2+i\sqrt{5}$ n'ont pas de ppcm et que 9 et $3\left(2+i\sqrt{5}\right)$ n'ont pas de pgcd. Il n'y a pas unicité car $3 \times 3 = 9 = \left(2+i\sqrt{5}\right)\left(2-i\sqrt{5}\right)$.

Parler des **localisé** (sans ce terme topologique) –> **algèbre des fractions**.
Comment inverser le plus possible d'éléméent dans un anneau ? localisé par rapport aux non divisuers de 0.
attention aux anneau pas intègres, la localisation n'est pas injective...

p **irréductible** ssi $\forall a, b,\ p = ab \implies a \sim 1$ ou $b \sim 1$
IE ssi p minimal (pour divise) dans $A \setminus \{1\}$ (et si A corps ? ? ?)

anneau sans unité : on plonge en rajoutant une unité :-)
EXO : *C'est fonctoriel, et on peut même inposer la caractérisutique.*

Si G gpe anéblien ,CNS pour que $\left(G^G,+,\circ\right)$ soit un anneau ?
$\left(G^G,+\right)$ est bien un gpe abélien, $\left(G^G,\circ\right)$ un monoide.
Pour la distrib, $(f+g)\circ h$ ok par déf de $\circ$ et $+$, mais $f\circ(g+h)$ ok ssi tous les f sont additives (appliquer à fonctions constantes)

3 Vocabulaire

Stathme : Ce mot est utilisé depuis peu pour désigner la valuation dans un anneau euclidien. Il est formé sur le grec stathmê qui signifie cordeau, règle, mesure. Par la suite, il désigne aussi le niveau. Le mot stathme est entré dans le vocabulaire mathématique avec l'idée d'un classement par niveau des éléments de l'anneau étudié. Dans l'anneau des polynômes, par exemple, le stathme euclidien correspond au degré.

a et b commutent / a **commute à** b
a **centralise** B
A et B **se centralisent**

anneau **de Bézout** : tout idéal dtf est principal, ie $(a)+(b)$ s'écit toutjours(c). Alors c est un pgcd de a et b, et l'on a le **th de Bézout** $a\wedge b=1 => \exists\lambda,\mu,\lambda a+\mu b=1$.

4 Calcul dans les anneaux

triangle Pascal : connu des chinois pour la prop addtive.
La nouveauté de Pascal est une prop multiplicative : les quotients succesifs d'une même ligne sont les $\frac{n-k}{k}$, d'où la formule explicite $\frac{n^{\downarrow k}}{k^{\downarrow k}}$ (sans toute la récursion additive)

dessin pour développer, donc pour les identités remarquable $(a+b)^2=a^2$...

Calcul de $\prod_{i=1}^{n}\left(1+a^{2^i}\right)$

identité de lagrange et sophie germain et bramagupta
calcul somme somme, partion différentes du dmaine, exemple du produit de polynômes, de l'exponentiels de nilpotents.

La formule $\sum a_i\sum b_j=\sum_{I\times J}$ est trivial une fois vu l'asso : voir les sommes comme des constantes, et supprimer les arenthèses inutiles.
retrouver la formule du produit matriciel = très bon exo de calcul sur les anneaux

identitiés remarquables !
sommes arihtmétiques, géométriques, polynoùes de Bernouilli
Face à un $\sum a_{i,j}$, on peut chercher à séparer les variables i et j, çàd écrire $a_{i,j}=x_iy_j$, ce qui permet de factoriser $\sum a_{i,j}=\sum x_i\sum y_j$
eg : $\sum\frac{a_ia_j}{i+j+1}=\sum a_ia_j\int x^{i+j}=\int\sum a_ix^i\sum a_jx^j\geq 0$

4.1 Une formule générale

Soit A un anneau[2] unitaire, $a_1, ..., a_n, b_1, ..., b_n \in A^n$ des éléments qui commutent. Notre but est de développer le produit $(a_1 + b_1)(a_2 + b_2)...(a_n + b_n)$.

Rappel du cours sur les loi binaires. Que se passe-t-il si l'on développe naïvement ? On pioche dans chaque facteur $a_i + b_i$ un terme a_i ou b_i, on fait le produit des n termes ainsi trouvés, ce qui donne un terme de la forme $\prod_{i\in I} a_i \prod_{j\in J} b_j$ avec $I \sqcup J = \{1, ..., n\}$: en effet, I correspond aux places des facteurs dans lesquels on a pioché un a_i, et J aux places des facteurs où l'on a pioché un b_j, ils forment donc une réunion disjointe de $\{1, ..., n\}$; noter que I ou J pourrait très bien être vide (cas où l'on ne pioche que des a_i ou que des b_j), puis on somme sur toutes les manières de piocher des a_i et des b_j, çàd sur toutes les façons d'écrire $\{1, ..., n\}$ comme réunion disjointe de deux partie $I \sqcup J$. On devrait donc trouver

$$\prod_{i=1}^{n}(a_i + b_i) = \sum_{I,J\subset\{1,.,n\}}^{I\sqcup J=\{1,.,n\}} \prod_{i\in I} a_i \prod_{j\in J} b_j.$$

Il serait aisé de montrer la généralisation suivante : si a_i^j sont np éléments qui commutent, où i décrit $\{1, ..., n\}$ et j décrit $\{1, ..., p\}$, alors

$$\prod_{i=1}^{n}(a_i^1 + a_i^2 + \cdots + a_i^p) = \sum_{\substack{I_1,...,I_p\subset\{1,...,n\}\\ I_1\sqcup\cdots\sqcup I_p=\{1,...,n\}}} \prod_{i\in I_1} a_i^1 \prod_{i\in I_2} a_i^2 ... \prod_{i\in I_p} a_i^p.$$

Ceci résoud le problème du développement dans un anneau, à savoir comment transformer un produit de sommes en une somme de produits.

4.2 Vers le multinôme de Newton

Corollaire (formule du binôme de Newton).
Si a et b sont deux éléments qui commutent, alors

$$\begin{aligned}(a+b)^n &= \sum_{p+q=n}\binom{n}{p}a^pb^q \\ &= a^n + na^{n-1}b + \frac{n(n-1)}{2}a^{n-2}b^2 + ... + \frac{n(n-1)}{2}a^2b^{n-2} + nab^{n-1} + b^n.\end{aligned}$$

Démonstration.
Il suffit de prendre tous les a_i égaux à a et tous les b_i égaux à b. On trouve alors

$$(a+b)^n = \sum_{I\sqcup J=\{1,.,n\}} \prod_{i\in I} a_i \prod_{j\in J} b_j = \sum_{I\sqcup J=\{1,.,n\}} a^{|I|}b^{|J|}.$$

On somme alors à $|I|$ fixé (donc à $|J| = n-|I|$ fixé) afin de factoriser les termes $a^{|I|}b^{|J|}$ qui apparaissent plusieurs fois :

$$= \sum_{\substack{p,q\geq 0\\ p+q=n}} \sum_{\substack{I\sqcup J=\{1,.,n\}\\ |I|=p,\ |J|=q}} a^{|I|}b^{|J|} = \sum_{\substack{p,q\geq 0\\ p+q=n}} a^pb^q \sum_{\substack{I\sqcup J=\{1,.,n\}\\ |I|=p,\ |J|=q}} 1.$$

Il reste à compter de nombre de façon d'écrire $\{1, ., n\}$ comme réunion disjointe de deux parties de cardinaux p et q. Cela revient à choisir une partie de cardinal p dans $\{1, ..., n\}$ (car la seconde partie doit le complémentaire de la première), ce qui se fait en $\binom{n}{p}$ choix. On trouve donc

$$= \sum_{\substack{p,q\geq 0\\ p+q=n}} a^pb^q\binom{n}{p} = \sum_{p+q=n}\binom{n}{p}a^pb^q,\ CQFD.$$

[2] en fait, ici, un semi-anneau suffirait

C'est quand même plus joli que la démonstration par le calcul habituel, non ?

Attention, noter bien que l'hypothèse de commutativité : si elle n'est pas vérifiée (par exemple sur un anneau de matrices), il faut différencier les termes croisés, à l'instar de

$$(a+b)^2 = a^2 + \underline{ab+ba} + b^2.$$

On pourrait tout aussi bien montrer la formule du multinôme de Newton à l'aide de la généralisation précédente :

$$(a_1 + a_2 + ... + a_p)^n = \sum_{n_1+...+n_p=n} \binom{n}{n_1, ...n_p} a_1^{n_1} a_2^{n_2} ... a_p^{n_p}$$

où le terme $\binom{n}{n_1, ...n_p}$ compte le nombre de façons de choisir p parties de $\{1, ..., n\}$ dont la réunion disjointe[3] fait $\{1, ..., n\}$.

Pour calculer $\binom{n}{n_1, ...n_p}$, on choisit d'abord la partie de cardinal n_1, ce qui se fait en $\binom{n}{n_1}$ choix, puis on choisit une partie à n_2 éléments parmi les $n - n_1$ éléments restants, ce qui se fait en $\binom{n-n_1}{n_2}$ choix, et ainsi de suite, ce qui donne la formule

$$\begin{aligned}\binom{n}{n_1, ...n_p} &= \binom{n}{n_1}\binom{n-n_1}{n_2}\binom{n-n_1-n_2}{n_3}...\binom{n-n_1-n_2-...n_{p-1}}{n_p} \\ &= \frac{n!}{n_1!\,(n-n_1)!}\frac{(n-n_1)!}{n_2!\,(n-n_1-n_2)!}...\frac{(n-n_1-...-n_{p-1})!}{n_p!\,(n-n_1-...-n_p)!}.\end{aligned}$$

Tout se simplifie en diagonale $\diagup$, le dernier terme en bas vaut $(n - n_1 - ... - n_p)! = 0! = 1$, il reste donc

$$\binom{n}{n_1, ...n_p} = \frac{n!}{n_1! n_2! ... n_p!}.$$

4.3 Fonctions symétriques élémentaires

Revenons à la formule

$$\prod_{i=1}^{n}(a_i + b_i) = \sum_{\substack{I,J\subset\{1,..,n\} \\ I\sqcup J=\{1,..,n\}}} \prod_{i\in I} a_i \prod_{j\in J} b_j.$$

Lorsque tous les b_j sont égaux à 1, les produits se simplifient : il reste alors

$$\prod_{i=1}^{n}(1 + a_i) = \sum_{I\subset\{1,..,n\}} \prod_{i\in I} a_i.$$

En regroupant les parties I selon leur cardinal, on fait apparaître les sommes $e_k(\overrightarrow{a})$ de tous les produits formés de k facteurs a_i distincts lorsque k décrit $\{0, ..., n\}$:

$$\prod_{i=1}^{n}(1 + a_i) = \sum_{k=0}^{n}\sum_{|I|=k}\prod_{i\in I} a_i = \sum_{k=0}^{n} e_k(\overrightarrow{a}).$$

Définition.

[3] Attention à ne pas parler de partitions car les parts d'une partition sont par définition non vides !

Le terme $e_k\left(\overrightarrow{a}\right)$ est appelé k-ième fonction symétrique élémentaire[4] *des a_i. On peut l'écrire indifféremment sous l'une des deux formes suivantes*

$$e_k\left(\overrightarrow{a}\right) = \sum_{\substack{I\subset\{1,\ldots,n\}\\|I|=k}} \prod_{i\in I} a_i = \sum_{1\leq i_1<\cdots<i_k\leq n} a_{i_1}\cdots a_{i_k}.$$

Voyons des exemples (en oubliant la dépendance en $\overrightarrow{a}$ pour alléger les notations).

Pour $k=n$, il n'y a qu'un seul produit formé de k facteurs a_i distincts :

$$e_n = a_1\cdots a_n.$$

De même, pour $k=0$, il n'y a que le produit vide 1 :

$$e_0 = 1.$$

Concernant e_1, on trouve la somme des a_i :

$$e_1 = a_1 + \cdots + a_n.$$

Par ailleurs, à k fixé, il y a $\binom{n}{k}$ parties de $\{1,...,n\}$ de cardinal k, de sorte que e_k comporte $\binom{n}{k}$ termes.

Pour comprendre ce qui se passe, rien de mieux qu'un bon exemple :

$$\begin{aligned}(1+a)(1+b)(1+c) &= \underbrace{1.1.1}_{k=0} + \underbrace{a.1.1+1.b.1+1.1.c}_{k=1} + \underbrace{a.b.1+a.1.c+1.b.c}_{k=2} + \underbrace{a.b.c}_{k=3}\\ &= \underline{1} + \underline{a+b+c} + \underline{ab+ac+bc} + \underline{abc}\\ &= 1+e_1+e_2+e_3.\end{aligned}$$

Voyons comment apparaissent naturellement les fonctions symétriques élémentaires dans les polynômes. Soit $\lambda_1,...,\lambda_n$ des scalaires d'un corps (donc qui commutent entre eux et avec l'indéterminée X). On peut applique la formule générale pour développer

$$\begin{aligned}\prod_{i=1}^{n}(X-\lambda_i) &= \sum_{I\sqcup J=\{1,\ldots,n\}} \prod_{i\in I} X \prod_{j\in J}(-\lambda_j) = \sum_{J\subset\{1,\ldots,n\}} X^{n-|I|}(-1)^{|J|}\prod_{j\in J}\lambda_j = \sum_{k=0}^{n} X^{n-k}(-1)^k \sum_{|J|=k}\prod\lambda_j\\ &= \sum_{k=0}^{n}(-1)^k e_k X^{n-k}\\ &= X^n - e_1X^{n-1} + e_2X^{n-2} - ... + (-1)^{n-1}e_{n-1}X + (-1)^n e_n.\end{aligned}$$

Les relations ainsi trouvées entre les coefficients du polynôme et ses racines sont appelées *relations de Viète*.

Pour un polynôme de degré 2, on retrouve la formule connue

$$(X-\lambda)(X-\mu) = X^2 - (\lambda+\mu)X + \lambda\mu$$

où apparaissent **moins** la somme des racines devant le X et le produit des racines en terme constant.

On retrouve par exemple la somme et le produit des racines n-ièmes de l'unité :

$$X^n - 1 = \prod_{\lambda\in\mathbb{U}_n}(X-\lambda) = X^n - e_1X + ... + (-1)^n e_n.$$

Par identification, on trouve $e_1 = 0$ et $e_n = (-1)^{n-1}$. On a même que tous les autre e_k (pour $1<k<n$) sont nuls !

Exo sur le coniques : très bon exemples, car les polynômes ne sont plus unitaires.

[4] Pourquoi fonction *symétriques* ? Et bien il s'agit de voir que les σ_k sont inchangés par permutation des a_i ; ils sont donc symétriques en ces derniers. Réciproquement, il est un résultat non trivial que tout polynôme symétrique en les a_i est un polynôme en les $\sigma_k\left(\overrightarrow{a}\right)$; les σ_k sont donc, en ce sens, *élémentaires*.

5 $M_2(A)$ et les propriétés du det

définiton, c'est un aneau non commutatif avec divisuers de zéro : $AB = 0 \not\Longrightarrow A = 0$ ou $B = 0$, $A^k = 0 \not\Longrightarrow A = 0$, $AM = BM \not\Longrightarrow A = B$.

groupe des invesrbiles : **groupe linéaire**.

def du **det**, mq $\det(AB) = \det A \det B$, dire $\in GL_2 \iff \det \in A^\times$ et expliiter inverse.

cor : dans un corps, inv ssi det non nul

rq : dans Z, inv ssi det $= \pm 1$.

rq : si $AB = I$, alors A inversible, d'ù $BA = A^{-1}ABA = I$: donc un inverse à droite/gauche est un inverse bilatère.

th CayleyHamilton : $A^2 - (\operatorname{tr} A)\, A + |A| = 0$.

cor : mq $(ab - ba)^2\, c - c\,(ab - ba)^2 = 0$ pour toutes matrices a, b, c. DEM : par CH, $(ab - ba)^2$ est scalaire, donc commute avec cs.