Anneaux & corps (12h)

Marc SAGE

lundi 29 septembre, vendredi 3 et lundi 6 octobre 2014

Table des matières

Ce cours présente une introduction aux anneaux par une approche *arithmétique*, la contrainte étant ne pas parler de quotients. Ce fil directeur aboutit à la définition des idéaux en vu d'unifier les deux arithmétiques présentées (entière et polynomiales) et motive l'exploration des corps en caractéristique première (l'étude systématique des extensions algébriques ne sera qu'effleurée).

1 Rappels d'arithmétique

Définition (divisibilité). *Soient d et m dans $\mathbf{N}$. 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*

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

Exemples. 1 divise tout naturel, 0 est divisible par tout naturel, 3 et 7 divisent 42, tout naturel est diviseur et multiple de lui-même.

Propriété (stabilité de l'ensemble des diviseurs). *Soit $n \in \mathbf{N}$. L'ensemble $\mathbf{N}n$ des multiples de n est stable par somme et par multiplication par n'importe quel naturel fixé.*

1.1 L'involution des diviseurs

Remarque. Lorsque $d \mid m$, alors $\frac{m}{d} \mid m$. On dispose ainsi d'une involution de l'ensemble $\mathrm{Div}\,(n)$ des diviseurs d'un naturel n fixé :

$$\left\{ \begin{array}{ccc} \mathrm{Div}\, n & \longrightarrow & \mathrm{Div}\, n \\ d & \longmapsto & \frac{n}{d} \end{array} \right. .$$

Application. *Montrer que la moyenne géométrique des diviseurs de n vaut $\sqrt{n}$.*

Calculons le produit des diviseurs de d, reparamétré par l'involution ci-dessus :

$$\left(\prod_{d|n} d\right)^2 = \prod_{d|n} d \prod_{d|n} d = \prod_{d|n} d \prod_{d|n} \frac{n}{d} = \prod_{d|n} d\frac{n}{d} = n^{\#\,\mathrm{Div}(n)}.$$

Prendre la racine carrée conclut.

1.2 Décomposer en indécomposables

Problème : cherchons à factoriser un naturel n "le plus possible". Un algorithme naturel se présente :

1. ou bien n peut se factoriser (on réapplique alors l'algorithme aux facteurs) ;
2. ou bien il ne peut pas (n est "indécomposable").

Si l'algorithme décrit s'arrête, on aura "décomposé" n en produit d'"indécomposables" (les fameux nombres premiers).

Définition (premier). *Un naturel sera dit **premier** s'il possède exactement deux diviseurs (qui sont alors nécessairement 1 et lui-même).*

Exemples. Les premiers nombres premiers sont (★ les entiers 0 et 1 ne sont pas premiers !)

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37...$$

Théorème (décomposition en facteurs premiers). *Tout naturel non nul est produit de premiers, avec unicité des facteurs à l'ordre près.*

Démonstration. Suivre l'algorithme ci-dessus il termine car $\mathbf{N}$ ne contient aucune suite strictement décroissante pour $|$. Formellement, on raisonne par récurrence, ce qui revient à dire que $\mathbf{N}$ ne contient aucune suite strictement décroissante (pour l'ordre usuel). On admet l'unicité.

Exemple : $3\,628\,800 = 2^8 3^4 5^2 7$.

1.3 Valuations p-adiques, p. g. c. d., p. p. c. m.

Définition (valuations p-adiques). *Soit p un premier. On appelle **valuation p-adique** l'application, notée v_p, qui à un naturel associe l'exposant de p dans sa décomposition en facteurs premiers (on définira $v_p(0) := \infty$).*

On peut ainsi, pour tout entier $n \geq 1$, écrire

$$n = \prod_{p \in \mathbf{P}} p^{v_p(n)} \text{ avec les propriétés (\textbf{exercices !})} \begin{cases} v_p(ab) = v_p(a) + v_p(b) \\ v_p(a+b) \geq \min\{v_p(a), v_b(a)\} \\ d \mid m \iff \forall p \in \mathbf{P},\ v_p(d) \leq v_p(m) \end{cases}.$$

Corollaire-définition (p. g. c. d. & p. p. c. m.). *Soient a et b deux naturels. Alors a et b admettent*

$$\text{un } \textbf{\textit{plus grand commun diviseur}}\ a \wedge b := \prod p^{\min\{v_p(a), v_p(b)\}} \text{ et}$$

$$\text{un } \textbf{\textit{plus petit commun multiple}}\ a \vee b := \prod p^{\max\{v_p(a), v_p(b)\}}$$

(généralisables à plusieurs naturels a, b, c, d...)

Lorsque $a \wedge b = 1$, i. e. *lorsque a et b n'ont pas de diviseurs commun (non trivial), on dit que a et b sont **étrangers** ou **premiers entre eux**.*

Exemple : on a $\wedge \begin{matrix} 1071 \\ 462 \end{matrix} = \wedge \begin{matrix} 2^0 \cdot 3^2 \cdot 7 \cdot 11^0 \cdot 17 \\ 2 \cdot 3 \cdot 7 \cdot 11 \cdot 17^0 \end{matrix} = 2^0 \cdot 3^1 \cdot 7^1 \cdot 11^0 \cdot 17^0 = 21.$

Exercice 0. *Soient x et y deux naturels. Montrer l'égalité $(x \wedge y)(x \vee y) = xy$.*

Il suffit d'utiliser l'identité $\min\{u,v\} + \max\{u,v\} = u + v$.

Exercice 1. *Soient a et b deux naturels. Montrer l'équivalence $a^2 \mid b^2 \iff a \mid b$.*

Seul le sens $\Longrightarrow$ est digne. À la main, on a un problème car $\mathbf{N}$ n'est pas stable par racine carrée : les valuations vont trivialiser la chose. Supposons $a^2 \mid b^2$. Soit $p \in \mathbf{P}$. On a alors $v_p\left(a^2\right) \leq v_p\left(b^2\right)$, *i. e.* $2v_p(a) \leq 2v_p(b)$, d'où $v_p(a) \leq v_p(b)$, ce qui montre $a \mid b$.

Exercice 2. *Soient p un premier, a et k deux naturels non nuls. Montrer l'équivalence $p \mid a^k \iff p \mid a$.*

Comme ci-dessus, si $p \mid a^k$, alors $0 < v_p(p) \leq v\left(a^k\right) = kv_p(a)$, d'où (en simplifiant par k) $v_p(a) > 0$, *i. e.* $v_p(a) \geq 1$.

Exercice 3. *Soit a et b deux naturels étrangers. Si le produit ab est un carré, alors a et b en sont aussi.*

Exercice 4 (lemme Euclide). *Soient p un premier, a et b deux naturels. Si $p \mid ab$, alors $p \mid a$ ou $p \mid b$.*

Exercice 5 (lemme Gauss). *Si deux naturels étrangers divisent un entier, alors leur produit divise encore cet entier.*

Exercice 6 (formule de Legendre). *Soient p un premier et n un naturel. Montrer que $v_p(n!) = \sum_{k \geq 1} \left\lfloor \frac{n}{p^k} \right\rfloor$.*

Exercice 7 (plus difficile). *Soient a et b dans $\mathbf{N}^*$. Montrer que le coefficient binomial $\binom{a+b}{a}$ divise $\binom{2a}{a}\binom{2b}{b}$.*

1.4 Triplets pythagoriciens

Thème (triplets pythagoriciens). *Trouver tous les triplets $(a,b,c) \in \mathbf{N}^{*3}$ tel que $a^2 + b^2 = c^2$.*

Soit (a,b,c) un tel triplet. Quitte à diviser l'égalité par $a \wedge b \wedge c$, on peut supposer que ce dernier vaut 1.

Idée 1 : factoriser $a^2 = c^2 - b^2 = (c-b)(c+b)$. On a envie de dire que les facteurs (du carré a^2) sont des carrés – mais ce n'est pas vrai en général puisque $6^2 = 2 \cdot 18$. Cependant, si les facteurs sont étrangers, cela sera possible (**exercice !**). Or, il se pourrait, si par malheur a était pair, que chaque facteur soit divisible par 2 : nous allons donc diviser au préalable par $4 = 2 \cdot 2$.

Idée 2 : passer l'égalité *modulo* des entiers bien choisis. Modulo 4, on vérifiera que les seuls carrés sont 0 et 1, donc il est impossible que a et b soient tous deux impairs (sinon $c^2 = 2 \bmod 4$). Par symétrie, on peut toujours supposer a pair. Il vient alors

$$\left(\frac{a}{2}\right)^2 = \frac{c-b}{2}\frac{c+b}{2}.$$

Mise en œuvre. Soit par l'absurde p un diviseur premier de $\frac{c-b}{2} \wedge \frac{c+b}{2}$. Il divise la somme c et la différence b, donc les carrés c^2 et b^2, donc la différence $c^2-b^2=a^2$, donc (étant premier) divise a : finalement p divise $a\wedge b\wedge c = 1$, ce qui est absurde, d'où l'étrangeté des facteurs $\frac{c-b}{2}$ et $\frac{c+b}{2}$. Il y a par conséquent deux naturels u et v (étrangers) tels que $\frac{c-b}{2}=u^2$ et $\frac{c+b}{2}=v^2$, d'où $c=u^2+v^2$, $b=v^2-u^2$ et $a=2uv$. Réciproquement, un tel triplet fonctionne (on peut même imposer u et v de parités distinctes sinon 2 diviserait $a\wedge b\wedge c$). Ci-après quelques exemples :

(u,v)	$(1,2)$	$(1,4)$	$(2,3)$	$(2,5)$	$(3,4)$
(a,b,c)	$(4,3,5)$	$(8,15,17)$	$(12,5,13)$	$(20,21,29)$	$(24,7,25)$

1.5 Algorithme d'Euclide, identité de Bézout

On fixe deux naturels a et b.

Soient d,λ,μ trois naturels. Si $d \mid a$ et $d \mid b$, alors $d \mid \lambda a$ et $d \mid \mu b$, donc $d \mid \lambda a+\mu b$; en particulier, pour $d=a\wedge b$, on obtient l'inclusion $\mathbf{N}a+\mathbf{N}b \subset \mathbf{N}(a\wedge b)$. A-t-on l'inclusion réciproque ? Il suffirait pour cela de montrer que $a\wedge b \in \mathbf{N}a+\mathbf{N}b$, ce qui va être "presque" vrai.

Lemme : *si a,b,c sont trois entiers tels que $a-c\in\mathbf{N}b$, alors un entier divise $a\wedge b$ ssi il divise $b\wedge c$* (**exercice !**). En corollaire, si $a>b$ sont deux naturels, alors le p. g. c. d. de a et b vaut celui de b et du reste de la division de a par b. En itérant ce processus, on obtient le p. g. c. d. de a et b comme dernier reste non nul (en effet, on a $d\wedge 0=d$ pour tout naturel d). Puis remonter les calculs va permettre d'obtenir explicitement $a\wedge b$ comme élément de "presque" $\mathbf{N}a+\mathbf{N}b$.

Exemple : appliquons cet **algorithme** (attribué à **Euclide**) à 1071 et 462 (leur p. g. c. d. vaut 21 d'après un exemple précédent). On a les divisions euclidiennes

$$1071 = 2\cdot 462+147, \qquad 462 = 3\cdot 147+21, \qquad 147 = 7\cdot 21+0.$$

En remontant les calculs, on obtient

$$\begin{aligned} 21 &= 462-3\cdot 147 \\ &= 462-3\,(1071-2\cdot 462) \\ &= 7\cdot 462-3\cdot 1071, \end{aligned}$$

d'où une égalité (presque) comme cherché : les coefficients entiers peuvent être négatifs ! .

Une formalisation de cet exemple conduirait à une preuve du théorème suivant.

Théorème (Bachet-Bézout). *Il y a deux entiers relatifs λ et μ tels que $a\wedge b=\lambda a+\mu b$, ce qui revient à affirmer l'égalité*

$$\mathbf{Z}a+\mathbf{Z}b=\mathbf{Z}(a\wedge b).$$

On montrerait de même l'inclusion $\mathbf{N}(a\vee b)\subset \mathbf{N}a\cap\mathbf{N}b$ (en écrivant $a\vee b=\frac{b}{a\wedge b}a\in\mathbf{N}a$ et de même en échangeant a et b) puis l'inclusion réciproque (par minimalité du p. p. c. m. parmi les multiples communs), d'où les égalités

$$\mathbf{N}a\cap\mathbf{N}b=\mathbf{N}(a\vee b) \text{ puis } \mathbf{Z}a\cap\mathbf{Z}b=\mathbf{Z}(a\vee b).$$

Tout cela ne ressemble qu'à un immonde bricolage : tantôt du $\mathbf{N}$, tantôt du $\mathbf{Z}$, des inclusions montrées à la main à l'aide d'écritures *ad hoc*...

Exercice. *Montrer l'unicité de la décomposition en facteurs premiers.*

Soient deux décompositions $p_1p_2\cdots p_r=q_1q_2\cdots q_s$ en produits de premiers. Si l'on montre le lemme d'Euclide, alors le fait que p_1 divise les deux produits montre que p_1 divise l'un des q_j, donc lui est égal : itérer cette simplification aboutit à l'égalité des familles (p_i) et (q_j) à l'ordre près.

Soit donc p un premier divisant un produit ab. Si p ne divise pas a, il lui est étranger (car $a\wedge p$, divisant p, vaut ou bien 1 ou bien p), d'où deux entiers λ et μ tels que $\lambda p+\mu a=1$. Multiplier par b donne $b=\lambda pb+\mu ab = p\left(\lambda b+\mu\frac{ab}{p}\right)$, ce qui montre que p divise b.

★ C'est le théorème de Bézout qui permet de montrer le lemme d'Euclide et l'unicité de la décomposition, d'où la bonne définition des valuations p-adiques. Ce serait donc tricher que de montrer (comme proposé plus haut en exercices) le lemme Euclide à l'aide des valuations !

1.6 Un peu d'arithmétique polynomiale

Comme dans $\mathbf{N}$, on dira qu'un polynôme D ***divise*** un polynôme M si

$$D \mid M \overset{\text{déf.}}{\iff} \exists D' \in \mathbf{K}[X],\ M = DD'.$$

Notation-propriété : on abrégera l'ensemble des multiples d'un polynôme A par

$$(A) := \mathbf{K}[X]\, A,$$

lequel est stable par somme et par multiplication par n'importe quel polynôme fixé. On a ainsi l'équivalence

$$A \mid B \iff (B) \subset (A).$$

Propriété-définition (relation "être associé") : il est possible d'avoir l'égalité $(A) = (B)$, *i. e.* d'avoir les deux divisibilités $\begin{cases} A \mid B \\ B \mid A \end{cases}$. Cela équivaut à ce que $B = \lambda A$ pour un certain scalaire (=polynôme inversible) λ. On dit alors que A et B sont ***associés*** et on note

$$A \sim B \overset{\text{déf.}}{\iff} (A) = (B) \iff \begin{cases} A \mid B \\ B \mid A \end{cases} \overset{\text{prop.}}{\iff} \exists \lambda \in \mathbf{K}^*,\ B = \lambda A.$$

Définition (irréductible). *Un polynôme est dit* ***irréductible*** *si : 1) il n'est pas constant, 2) tous ses diviseurs sont associés à* 1 *ou à lui-même.*

Par exemple, $X - \lambda$ est irréductible pour tout scalaire λ et $X^2 + 1$ est irréductible dans $\mathbf{R}[X]$ mais pas dans $\mathbf{C}[X]$.

Question : peut-on "réduire" un polynôme en irréductibles ? Comme pour les entiers naturels, la réponse est oui :

tout polynôme non nul est produit d'irréductibles par un scalaire.

Une démonstration s'obtient par récurrence sur le degré, récurrence permise par l'implication

$$A \mid B \Longrightarrow (A \sim B \text{ ou } \deg A < \deg B),$$

argument clef que l'on peut reformuler en disant

"*Il n'y a pas de suite strictement décroissante pour* $\mid$ *modulo* $\sim$ ".

Toutefois, l'unicité des facteurs à l'ordre près ne s'obtient que *modulo* la relation $\sim$. Elle se démontre comme dans $\mathbf{N}$: division euclidienne, algorithme d'Euclide, identité de Bézout, lemme d'Euclide. Bézout nous donne au passage les égalités

$$(A) + (B) = (A \wedge B) \text{ et } (A) \cap (B) = (A \vee B).$$

Comme pour $\mathbf{N}$, on déduit de cette décomposition unique la construction des valuations P-adiques pour tout polynôme P irréductible (observer que la valuation usuelle n'est autre que la valuation X-adique), l'existence de p. g. c. d. et p. p. c. m. (★ il n'y a plus unicité ! à moins, par exemple, de normaliser le coefficient dominant) et le lemme de Gauss.

Même commentaire que pour $\mathbf{N}$: impression de bricolage malhabile. En particulier, la relation $\sim$ semble tout compliquer en ruinant des unicités.

Comment unir ces deux arithmétiques aux propriétés pourtant semblables ?

2 Anneaux

2.1 Exemples

Définition. *On appelle* ***anneau***[1] *tout groupe additif* $(A, +)$ *muni d'une multiplication* $\times$ *distributive sur* $+$.

[1] 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 structure 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)

Lorsque $\times$ admet un neutre, on note ce dernier 1_A ou 1 et on dit que l'anneau est ***unifère***[2]*.*
Lorsque $\times$ est commutative (resp. associative), on dit que A est ***commutatif*** *(resp.* ***associatif****).*

Exercice. *Montrer que l'addition d'un anneau unifère est commutative.*
Soient a et b deux éléments d'un anneau unifère. On écrit

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

puis on simplifie par a à gauche et par b à droite.

Tous les anneaux de ce cours seront associatifs et unifères.

Exemples classiques. L'anneau initial $\mathbf{Z}$ (pas $\mathbf{N}$!), l'anneau nul $\{0\}$, les $\mathbf{Z}/n$, $\mathbf{Q}$, $\mathbf{R}$, $\mathbf{C}$, $\mathbf{K}[X]$, $\mathbf{K}^{\mathbf{N}}$, les $\mathbf{K}^I$ et les $C^k(I,\mathbf{K})$ (où I est un intervalle réel et où $k\in\mathbf{N}\cup\{\infty\}$), $\mathbf{Z}[i]:=\mathbf{Z}+\mathbf{Z}i$, $\mathbf{Q}\left[\sqrt{2}\right]:=\mathbf{Q}+\mathbf{Q}\sqrt{2}$.

Exemples exotiques.

1. $\mathbf{Z}+X\mathbf{Q}[X]$: les polynômes rationnels à termes constants entiers. Plus généralement $\mathbf{Z}_n[X]+X^{n+1}\mathbf{Q}[X]$ pour tout naturel n.
2. Soit M un monoïde. On rappelle que le ***support*** d'un $f\in\mathbf{K}^M$ est défini par

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

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

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

   Exercices : *montrer que* $\operatorname{Supp}(f*g)\subset\operatorname{Supp}f\operatorname{Supp}g$ *et trouver un neutre pour* $*$. (Lorsque $M=\mathbf{N}$, on retrouve l'anneau des polynômes $\mathbf{K}[X]=\mathbf{K}^{(\mathbf{N})}$.)
3. **Version continue** : on dira qu'une fonction $f\in\mathbf{K}^{\mathbf{R}}$ est ***à support compact*** si elle s'annule en-dehors d'un segment. Notons $C_c^\infty(\mathbf{R},\mathbf{K})$ le s.-e. v. de $C^\infty(\mathbf{R},\mathbf{K})$ formé des fonctions de $\mathbf{K}^{\mathbf{R}}$ à support compact. On défini alors le ***produit de convolution*** sur $C_c^\infty(\mathbf{R},\mathbf{K})$ par

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

   Exercice : *montrer que* $*$ *est commutatif, associatif et n'a pas de neutre. (Le neutre serait un* ***Dirac*** *centré en* 0*.)*
4. Soit I un ensemble. On muni l'ensemble $\mathbf{K}^{(I^2)}$ des ***matrices*** indexées par I du produit

$$AB:(x,y)\mapsto\sum_{i\in I}A(x,i)\,B(i,y).$$

   Exercice : *montrer que ce produit est associatif, n'est pas commutatif ssi* $|I|>1$ *et admet un neutre ssi* $|I|<\infty$*.*

Exercice. *Soit A un anneau (peut-être pas unifère). Montrer qu'il est unifère ssi il y a deux éléments a et b tels que les homothéties $a\,\mathrm{Id}$ et $\mathrm{Id}\,b$ soient bijectives.*
Le sens $\Longrightarrow$ est trivial (prendre $a=b=1$). Soient réciproquement a et b comme ci-dessus. La composée $a\,\mathrm{Id}\,b=(a\,\mathrm{Id})\circ(\mathrm{Id}\,b)$ est alors bijective, donc atteint ab en un e. Par injectivité, de $aeb=ab$ on déduit $eb=b$, d'où (à $x\in A$ fixé) $xeb=xb$ et $xe=x$, ce qui montre que e est un neutre à droite. On montrerait de même qu'il est neutre à gauche.

Définition. *Soit A un anneau. Un* ***sous-anneau*** *de A est une partie de A qui est un anneau pour les lois induites (par celles de A).*

On montre (comme pour les e. v. et les groupes) que cela équivaut à ce que la partie considérée soit un sous-groupe stable par produit et contenant 1. On montre ainsi que $C^k([0,1],\mathbf{K})$ est un anneau en tant que sous-anneau de $\mathbf{K}^{[0,1]}$ (idem pour le s.-e. v. des fonctions k fois dérivables.)

[2] littéralement "qui porte une unité"

2.2 Anneaux produits, isomorphismes, lemme chinois, inversibles, indicatrice d'Euler, petit théorème de Fermat

Soit A et B deux anneaux. Alors le produit $A \times B$ est un anneau pour les lois "coordonnées à coordonnées" (appelées lois ***produits***)

$$\begin{pmatrix} a \\ b \end{pmatrix} + \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \times \begin{pmatrix} f \\ g \end{pmatrix} := \begin{pmatrix} a + \alpha f \\ b + \beta g \end{pmatrix}.$$

Plus généralement, si (A_i) est une famille d'anneaux, alors le produit $\prod A_i$ est un anneau pour les lois "produits". En particulier, quand tous les A_i valent un même A, on trouve l'anneau A^I des applications de I dans A. Ainsi $\mathbf{K}^{42}$ et $\mathbf{K}^{[0,1]}$ sont-ils des anneaux.

Définition (morphisme d'anneaux). Soit $f : A \longrightarrow B$ une application entre deux anneaux.
*On dit que f est un **morphisme d'anneaux** si f préserve l'addition, la multiplication et l'unité (souvent oubliée !).*
*Lorsque f est de plus bijective, on dit que c'est un **isomorphisme d'anneaux**.*

Exercice : *montrer que la réciproque d'un isomorphisme d'anneaux est un isomorphisme.*
Comme pour les groupes, un morphisme d'anneaux sera injectif ssi son noyau est réduit à $\{0\}$.

Exercice. *Soient p un premier et A un anneau commutatif où $p = 0$. Montrer que $a \mapsto a^p$ est un endomorphisme de l'anneau A.*
(rappel : p désigne le p-ième itéré de 1_A pour $+$). Seule l'additivité est non triviale. Développons $(a+b)^p - a^p - b^p = \sum_{k=1}^{p-1} \binom{p}{k} a^k b^{p-k}$. Or l'égalité $k\binom{p}{k} = p\binom{p-1}{k-1}$ montre que les binomiaux $\binom{p}{k}$ pour $k \wedge p = 1$ sont nuls *modulo p*.

Exemple de transfert de structure. Soit E un ensemble. On rappelle que son ensemble des parties $\mathfrak{P}(E)$ est en bijection avec $\left(\mathbf{Z}/_2\right)^E$ *via* les fonctions caractéristiques :

$$\left\{ \begin{array}{ccc} \mathfrak{P}(E) & \longrightarrow & \left(\mathbf{Z}/_2\right)^E \\ P & \longmapsto & \chi_P : \left\{ \begin{array}{ccc} E & \longrightarrow & \mathbf{Z}/_2 \\ x & \longmapsto & \left\{ \begin{array}{l} 1 \text{ si } x \in P \\ 0 \text{ si } x \notin P \end{array} \right. \end{array} \right. \\ \{x \in E \ ; \ f(x) = 1\} & \longleftarrow & f \end{array} \right. .$$

On vérifiera par ailleurs aisément pour toute parties P et Q de E les égalités $\left\{ \begin{array}{c} \chi_{P \cap Q} = \chi_P \chi_Q \\ \chi_{P \Delta Q} = \chi_P + \chi_Q \end{array} \right.$. Puisque $\left(\left(\mathbf{Z}/_2\right)^E, +, \times\right)$ est un anneau, on en déduit que $(\mathfrak{P}(E), \Delta, \cap)$ est un anneau ! Par exemple, l'associativité de Δ s'obtiendra en écrivant (à $A, B, C, \subset E$ fixées)

$$\chi_{A\Delta(B\Delta C)} = \chi_A + \chi_{B\Delta C} = \chi_A + (\chi_B + \chi_C) = (\chi_A + \chi_B) + \chi_C = \chi_{(A\Delta B)\Delta C}.$$

Utilisation en arithmétique. Comment résoudre un système de congruences, à l'instar de $\left\{ \begin{array}{ll} x = 2 & [3] \\ x = 1 & [5] \end{array} \right.$?
L'existence d'une solution serait assurée par la surjectivité de l'application $\left\{ \begin{array}{ccc} \mathbf{Z} & \longrightarrow & \mathbf{Z}/_3 \times \mathbf{Z}/_5 \\ n & \longmapsto & (\overline{n}, \widehat{n}) \end{array} \right.$ (dans l'exemple, 11 et -4 sont solutions).
Montrons plus généralement le **lemme chinois** : *si a et b sont deux naturels étrangers, est alors un isomorphisme d'anneaux l'application* $\left\{ \begin{array}{ccc} \mathbf{Z}/_{ab} & \longrightarrow & \mathbf{Z}/_a \times \mathbf{Z}/_b \\ \widetilde{n} & \longmapsto & (\overline{n}, \widehat{n}) \end{array} \right.$.
On laisse vérifier que cette application est bien définie. Il est alors immédiat que c'est un morphisme d'anneaux. Vu l'égalité des cardinaux, sa surjectivité revient à son injectivité. Soit $n \in \mathbf{Z}$ nul *modulo a* et *modulo b*. Alors a et b divisent n, donc (Gauss) leur produit divise n, donc n est nul *modulo n*, *c. q. f. d.*.

Définition (groupe des unités). *Soit A un anneau. On appelle **unité** tout élément inversible. Leur ensemble est noté $A^\times$ (à ne pas confondre avec $A^* := A \setminus \{0\}$). C'est un groupe, appelé **groupe des unités** (ou des inversibles) de A.*

Par exemple, on a les égalités $\mathbf{Z}^\times = \{-1, 1\}$, $\mathbf{Q}^\times = \mathbf{Q}^*$, $\mathbf{R}^\times = \mathbf{R}^*$, $\mathbf{C}[X]^\times = \mathbf{C}^*$.

Il est aisé de vérifier que deux anneaux isomorphes ont leurs groupes des inversibles isomorphes.

On vérifiera que le groupe des unités d'un produit d'anneaux est le produit des groupes des unités : $(\prod A_i)^\times = \prod A_i^\times$.

Exercice (unités de $\mathbf{Z}/n$). *Soient $n \in \mathbf{N}$ et $a \in \{1, 2, ..., n\}$. Donner une CNS pour que a soit une unité de $\mathbf{Z}/n$.*

Supposons a inversible dans $\mathbf{Z}/n$. Notons b son inverse. On a donc $ab = 1 \bmod n$; soit $\lambda \in \mathbf{Z}$ tel que $ab = 1 + \lambda n$. On en déduit $\lambda n + ba = 1$, ce qui montre que a et n sont étrangers. Réciproquement, si $\lambda n + \mu a = 1$, alors μ est l'inverse de a modulo n.

On note $\varphi(n)$ le nombre d'entiers de $[1, n]$ étrangers avec n (l'application φ est appelée ***indicatrice d'Euler***). D'après ce qui précède, $\varphi(n)$ est le cardinal de $\left(\mathbf{Z}/n\right)^\times$. Vu le lemme chinois, on en déduit pour tous naturels a et b étrangers (on abrégera par commodité $\mathbf{Z}_n := \mathbf{Z}/n$)

$$\varphi(ab) = \operatorname{Card} \mathbf{Z}_{ab}^\times = \operatorname{Card}\ (\mathbf{Z}_a \times \mathbf{Z}_b)^\times = \operatorname{Card}\left(\mathbf{Z}_a^\times \times \mathbf{Z}_b^\times\right) = \operatorname{Card} \mathbf{Z}_a^\times\ \operatorname{Card} \mathbf{Z}_b^\times = \varphi(a)\,\varphi(b)$$

(bon courage pour montrer cela à la main). Il est par ailleurs aisé de montrer (à la main) l'égalité $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$ pour tout premier p, ce qui permet de calculer $\varphi(n)$ connaissant la décomposition de n en facteurs premiers. Par exemple, on trouvera

$$\varphi(120) = \varphi\left(2^3 \cdot 3 \cdot 5\right) = \left(2^3 - 2^2\right)\left(3 - 3^0\right)\left(5 - 5^0\right) = 4 \cdot 2 \cdot 4 = 32.$$

Remarque : le théorème de Lagrange appliqué au groupe $\left(\mathbf{Z}/n\right)^\times$ permet d'affirmer $a^{\varphi(n)} = 1\ [n]$ pour tout naturel a étrangers avec n. En particulier quand n est un premier p, on retrouve le **petit théorème de Fermat** : $a^{p-1} = 1\ [p]$ pour tout naturel a non multiple de p.

Exercice. *Montrer que $\sum_{d|n} \varphi(d) = n$.* On regroupe les n fractions $\frac{1}{n}, \frac{2}{n}, ..., \frac{n}{n}$ selon leur dénominateur minimal, lequel peut être tout diviseur de n (penser à $\frac{1}{d}$ pour tout $d \mid n$). À $d \mid n$ fixé, les fractions irréductibles de dénominateur d sont celles de la forme $\frac{k}{d}$ pour k étranger avec d (la fraction est irréductible) et tel que $k \in [1, d]$ (puisque $0 < \frac{k}{d} \leq 1$), donc sont en nombre $\varphi(d)$.

On pourra regarder l'exemple du cas $n = 12$: il y a

$$\begin{aligned}
\varphi(12) &= \left(2^2 - 2^1\right)\left(3^1 - 3^0\right) = 4 \text{ fractions de dénominateur réduit } 12 : \frac{1}{12}, \frac{5}{12}, \frac{7}{12} \text{ et } \frac{11}{12} ; \\
\varphi(6) &= \left(2^1 - 2^0\right)\left(3^1 - 3^0\right) = 2 \text{ fractions de dénominateur réduit } 6 : \frac{2}{12} = \frac{1}{6} \text{ et } \frac{10}{12} = \frac{5}{6} ; \\
\varphi(4) &= \left(2^2 - 2^1\right) = 2 \text{ fractions de dénominateur réduit } 4 : \frac{3}{12} = \frac{1}{4} \text{ et } \frac{9}{12} = \frac{3}{4} ; \\
\varphi(3) &= \left(3^1 - 3^0\right) = 2 \text{ fractions de dénominateur réduit } 3 : \frac{4}{12} = \frac{1}{3} \text{ et } \frac{8}{12} = \frac{2}{3} ; \\
\varphi(2) &= \left(2^1 - 2^0\right) = 1 \text{ fraction de dénominateur réduit } 2 : \frac{6}{12} = \frac{1}{2} ; \\
\varphi(1) &= 1 \text{ fraction de dénominateur réduit } 1 : \frac{12}{12} = \frac{1}{1}.
\end{aligned}$$

2.3 Arithmétique idéale

Soit A un anneau *commutatif*. On abrégera $(a) := Aa$ pour tout $a \in A$.

Définition (divisibilité, "être associé", irréductible). *Soient a et b dans A. On dit que a **divise** b si $\exists \lambda \in A,\ b = \lambda a$. On note alors $a \mid b$, ce qui revient à l'inclusion $(b) \subset (a)$.*

*Lorsque $(a) = (b)$, on dit que a et b sont **associés** (ce qui revient à pouvoir écrire $b = ua$ où u est une unité) et on note $a \sim b$.*

*On dit que a est **irréductible** s'il n'est pas inversible et si ses diviseurs sont associés à 1 ou à a.*

Qu'en est-il du théorème de décomposition ? Il suffirait d'une hypothèse "pas de suite strictement décroissante pour |" : mais cela est faux en général. Par exemple, dans $C^0(I, \mathbf{K})$, on a les divisibilités $\cdots \mid \sqrt[4]{\mathrm{Id}} \mid \sqrt[3]{\mathrm{Id}} \mid \sqrt{\mathrm{Id}} \mid \mathrm{Id}$ et aucune fonction $\sqrt[n]{\mathrm{Id}}$ n'est inversible si $0 \in I$ puisque s'annule. De plus, même si l'on a existence, l'unicité n'est plus assurée, comme dans $\mathbf{Z}\left[i\sqrt{3}\right]$ où 4 se décompose $2 \cdot 2 = \left(1 + i\sqrt{3}\right)\left(1 - i\sqrt{3}\right)$ (**exercice** : vérifier que les quatre facteurs sont irréductibles et que $2 \not\sim 1 \pm i\sqrt{3}$).

Définition (idéal). *On appelle **idéal** de A tout sous-groupe de A stable par multiplication par n'importe quel élément de A.*

$$I \text{ idéal de } A \Longleftrightarrow \begin{cases} 0 \in I \\ I \pm I \subset I \\ AI \subset I \end{cases} \quad \text{(un peu comme les s.-e. v.).}$$

Remarquer de suite que $(1) = A$ et qu'un idéal contient une unité ssi il vaut tout l'anneau : un idéal n'est donc (presque) jamais un sous-anneau !

Les (a) sont des idéaux, appelés ***principaux***. Vu l'équivalence $a \mid b \Longleftrightarrow (b) \subset (a)$, les propriétés arithmétiques des éléments de A (*modulo* $\sim$) se trouvent codées par leurs "éléments idéaux" associés (origine historique pour espérer sauver le théorème de décomposition), ce qui motive l'étude générale des idéaux.

Souvenir : dans $\mathbf{Z}$ et dans $\mathbf{K}[X]$, on avait les égalités $\begin{cases} (a) + (b) = (a \wedge b) \\ (a) \cap (b) = (a \vee b) \end{cases}$. Qu'en reste-t-il ?

Exercice : *la somme et l'intersection d'idéaux sont des idéaux.*

Peut-on espérer que tout idéal est principal ? Non : dans $\mathbf{K}[X, Y]$, les polynômes s'annulant en $(0, 0)$ sont ceux de $(X) + (Y)$ et ce dernier n'est pas principal (**exercice !**). En revanche, c'est le cas de $\mathbf{Z}$ et de $\mathbf{K}[X]$ (**exercice** : utiliser la division euclidienne).

Corollaire : si tout idéal de A est principal, alors on peut définir un p. g. c. d. $a \wedge b$ comme tout générateur de $(a) + (b)$ et de même un p. p. c. m. $a \vee b$ comme tout générateur de $(a) \cap (b)$.

Remarque. Dans $\mathbf{Z}$, on peut calculer *modulo* (n). En fait, dans un anneau (commutatif), on peut calculer *modulo* n'importe quel idéal (mais cela nous emmènerait trop loin vers les anneaux quotients).

3 Corps

Dans toute cette section, tous les anneaux considérés seront *commutatifs*[3].

3.1 Intégrité, corps des fractions

Définition (corps). *Un **corps** (en anglais "**field**") est un anneau K tel que $K^\times = K^*$, autrement dit un triplet $(K, +, \times)$ où $\times$ se distribue sur $+$ tel que $(K, +)$ et $(K^*, \times)$ soient des groupes abéliens.*

Exemples : $\mathbf{Q}$, $\mathbf{R}$, $\mathbf{C}$, $\mathbf{Q}\left[\sqrt{2}\right]$ (observer $\frac{1}{a+b\sqrt{2}} = \frac{a-b\sqrt{2}}{a^2+2b^2}$ pour tout $(a, b) \neq (0, 0)$).

Remarque ($1 \neq 0$). Dans un corps K, on a $1 \in K^\times = K^* = K \setminus \{0\}$, donc[4] $1 \neq 0$:

un corps possède au moins deux éléments !

Exercice (idéaux d'un corps). *Montrer qu'un anneau est un corps ssi ses idéaux sont triviaux ((0) ou (1)).*

Preuve. Un idéal non nul contient un élément non nul, donc une unité, donc vaut tout le corps. Réciproquement, si a un élément non nul, l'idéal (a) est non nul, donc vaut tout le corps, donc contient 1, d'où un inverse pour a

Soit K un corps. Puisque K^* est un groupe, on peut toujours simplifier des produits par un élément non nul.

Question : peut-on en général simplifier dans un anneau par un élément non nul ?

[3] Nous conseillons à nos lecteurs d'appeler *algèbre à division* ce que d'autres appelleraient *corps gauche* ou *corps non nécessairement commutatif*.

[4] Cette convention permet de conserver la classification des espaces vectoriels selon la dimension.

Proposition-définition (diviseurs de 0, anneau intègre) *Soit A un anneau. On peut simplifier dans A par tout élément non nul ssi 0 n'est pas produit d'élément non nuls (appelés **diviseurs**[5] **de** 0).*

$\boxed{\Longrightarrow}$ si $0 = ab$ avec $a \neq 0$, alors $a0 = 0 = ab$, d'où (en simplifiant par a) $0 = b$.

$\boxed{\Longleftarrow}$ supposons $ax = ay$ avec $a \neq 0$. Alors $0 = a(x - y)$, donc $x - y$ ne peut être non nul, d'où $x = y$.

Dans ce cas, si de plus A n'est pas l'anneau nul[6]*, on dit qu'il est **intègre*** (il n'est pas fourbe, il ne nous trompe pas sur les produits nuls).

Contre-exemples : un produit d'anneaux $A \times B$ n'est pas intègre, des nilpotents non nuls empêchent l'intégrité. Ces contre-exemples sont génériques, au sens de l'**exercice** suivant : *un anneau est intègre ssi il ne possède pas de nilpotents non nuls et si aucun idéal n'est "isomorphe" à un produit d'idéaux tous non nuls.*

On vient de voir qu'un corps est intègre, donc tous ses sous-anneaux le sont également. Réciproquement, est-ce qu'un anneau intègre est sous-anneau d'un corps ? Autrement dit, peut-on inverser formellement les éléments non nuls d'un anneau intègre ? La réponse est OUI. Deux exemples connus : inverser des entiers donne des rationnels ($\mathbf{Z} \subset \mathbf{Q}$), inverser des polynômes donne des "fractions rationnelles" ($\mathbf{R}[X] \subset \mathbf{R}(X)$).

Construction (corps des fractions). Soit A un anneau intègre. On va coder une fraction "$\frac{a}{b}$" (qui n'a pas encore de sens) par un couple $(a, b) \in A \times A^*$ *modulo* simplification. Définissons cette dernière sur $A \times A^*$ en notant $\begin{pmatrix} a \\ b \end{pmatrix} \sim \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \overset{\text{déf.}}{\Longleftrightarrow} a\beta = \alpha b$. On vérifiera qu'il s'agit d'une relation d'équivalence. La classe d'un couple $\begin{pmatrix} a \\ b \end{pmatrix}$ sera noté $\widetilde{\begin{pmatrix} a \\ b \end{pmatrix}}$ (ce que l'on veut être "$\frac{a}{b}$"). On vérifie alors que les lois (motivées par le calcul fractionnaire connu)

$$\widetilde{\begin{pmatrix} a \\ b \end{pmatrix}} \times \widetilde{\begin{pmatrix} \alpha \\ \beta \end{pmatrix}} = \widetilde{\begin{pmatrix} a\alpha \\ b\beta \end{pmatrix}} \text{ et } \widetilde{\begin{pmatrix} a \\ b \end{pmatrix}} + \widetilde{\begin{pmatrix} \alpha \\ \beta \end{pmatrix}} = \widetilde{\begin{pmatrix} a\beta + \alpha b \\ b\beta \end{pmatrix}}$$

sont bien définies et munissent l'ensemble quotient ${}^{A \times A^*}\!/_{\sim} =: \operatorname{Frac} A$ d'une structure d'anneau de neutre $\widetilde{\begin{pmatrix} 1 \\ 1 \end{pmatrix}}$. Observer pour tout $a \neq 0$ les égalités $\widetilde{\begin{pmatrix} a \\ b \end{pmatrix}}\widetilde{\begin{pmatrix} b \\ a \end{pmatrix}} = \widetilde{\begin{pmatrix} ab \\ ab \end{pmatrix}} = \widetilde{\begin{pmatrix} 1 \\ 1 \end{pmatrix}}$, ce qui montre que $\operatorname{Frac} A$ est en fait un corps. Observer ensuite que l'injection

$$i : \begin{cases} A & \hookrightarrow & \operatorname{Frac} A \\ a & \longmapsto & \widetilde{\begin{pmatrix} a \\ 1 \end{pmatrix}} \end{cases}$$

est un morphisme d'anneaux, ce qui permet de "plonger" A dans $\operatorname{Frac} A$, *i. e.* de "voir" A comme sous-anneau de $\operatorname{Frac} A$. Alors toute "fraction" s'écrit

$$\widetilde{\begin{pmatrix} a \\ b \end{pmatrix}} = \widetilde{\begin{pmatrix} a \\ 1 \end{pmatrix}}\widetilde{\begin{pmatrix} 1 \\ b \end{pmatrix}} = \widetilde{\begin{pmatrix} a \\ 1 \end{pmatrix}}\widetilde{\begin{pmatrix} b \\ 1 \end{pmatrix}}^{-1} = \frac{i(a)}{i(b)},$$

donc est bien une fraction et correspond bien (grâce à l'identification de A à $i(A)$) à ce que l'on voudrait être "$\frac{a}{b}$" : on la notera $\frac{a}{b}$ sans scrupules .

Insistons lourdement sur cette idée de plongement qu'il *faut* penser comme une inclusion. Personne (espérons-le) ne vous a dit quand vous étiez petits que $\mathbf{Z}$ s'injectait dans $\mathbf{Q}$ à l'aide un morphisme d'anneaux : vous avez appris que $\mathbf{Z}$ était tout simplement inclus dans $\mathbf{Q}$ – et il faut continuer à le penser. On oubliera donc volontiers l'injection i et l'on notera a au lieu de $i(a)$ sans aucune autre forme de procès[7].

3.2 Sous-anneau premier, caractéristique, corps finis

Soit A un anneau. À quoi ressemble le plus petit sous-anneau de A ? Il doit contenir 1, donc ses itérés, donc l'image du morphisme $\begin{cases} \mathbf{Z} & \longrightarrow & A \\ k & \longmapsto & k \cdot 1_A \end{cases}$. Réciproquement cette image est un sous-anneau de A, appelé

[5] un [diviseur de 0] est donc un [diviseur] de 0 non nul (on écarte ce cas trivial puisque 0 divise trivialement 0 !)

[6] on verra que les anneaux intègres sont les sous-anneaux de corps ; selon ce point de vue, on souhaite $1 \neq 0$ dans les deux structures

[7] Une mise en garde cependant : une fois donné un certain plongement, on identifie tout élément de départ à son image. Mais cette identification peut conduire à des confusions si l'on change de plongement. Il faut donc toujours clairement garder en tête quel plongement est sous-entendu.

sous-anneau premier de A. Le noyau de ce morphisme est un idéal de $\mathbf{Z}$, donc de la forme $n\mathbf{Z}$ pour un certain naturel n appelé la ***caractéristique*** *de* A et notée $\operatorname{car} A$. Deux cas se distinguent alors :

1. Si $\operatorname{car} A = 0$, alors le morphisme ci-dessus est injectif, donc $\mathbf{Z}$ se plonge dans A.
2. Si $\operatorname{car} A > 0$, le sous-anneau premier est de la forme $\mathbf{Z}/n$: on dit alors que A a de la ***torsion*** car itérer un élément un certain nombre de fois (ici n) le fait "boucler" sur 0.

Propriété (caractéristique d'un corps). *La caractéristique d'un corps est ou bien* 0 *ou bien un premier.*

Preuve. Soit K un corps de caractéristique $c > 0$. Si $ab = c$, alors cette égalité vue dans K devient $ab = 0$, d'où (par intégrité), la nullité de a ou b, *i. e.* l'appartenance de l'un au noyau $c\mathbf{Z}$, *i. e.* l'une des divisibilités $c \mid a$ ou $c \mid b$, d'où l'une des égalités $c = a$ ou $c = b$.

Propriété (les corps $\mathbf{Z}/n$). *L'anneau* $\mathbf{Z}/n$ *est un corps ssi* n *est premier.*

Preuve. L'anneau $A := \mathbf{Z}/n$ est un corps ssi $A^\times = A^*$, *i. e.* ssi $|A^\times| = |A^*|$, *i. e.* ssi $\varphi(n) = n - 1$, *i. e.* ssi tout entier de $[1, n[$ est étranger avec n, *i. e.* ssi n est premier. (Ou démo directe par Bézout caché dans $|A^\times| = \varphi(n)$.)

Propriété (cardinal d'un corps fini). *Tout corps fini a pour cardinal une puissance d'un premier.*

Preuve. Soit K un corps fini. Sa caractéristique n'est pas nulle sinon K contiendrait $\mathbf{Z}$ (qui est infini), donc est un premier p. Alors K contient le corps $k := \mathbf{Z}/p$, donc est un k-e. v. ; étant fini, il est de dimension finie d, donc isomorphe (comme k-e. v.) à k^d, donc est de cardinal $\left|k^d\right| = |k|^d = p^d$.

Théorème-définition (corps finis). Pour tout premier p et tout entier $n > 0$, on admettra qu'*il existe à isomorphisme près*[8] *un unique corps de cardinal* p^d : on note $\mathbf{F}_{p^d}$ l'un d'entre eux. Par exemple, $\mathbf{F}_p = \mathbf{Z}/p$. **Attention** : si $d \geq 2$, le corps $\mathbf{F}_{p^d}$ *n'est pas* $\mathbf{Z}/p^d$ car $p = 0$ dans $\mathbf{F}_{p^d}$ mais pas dans $\mathbf{Z}/p^d$!

Ce qui précède montre que :

1. en caractéristique nulle, un corps contient $\mathbf{Q}$ (et est donc un $\mathbf{Q}$-e. v.) ;
2. en caractéristique première p, un corps contient $\mathbf{F}_p$ (et est donc un $\mathbf{F}_p$-e. v.).

Exercice. *Soit* K *un corps fini de caractéristique* $p > 0$*, Montrer que l'application* $x \mapsto x^p$ *est un monomorphisme du corps, appelé* ***automorphisme de Frobenius****.*

3.3 Extensions algébriques

[non traité en cours]

On a vu que l'anneau $\mathbf{Q}[\sqrt{2}]$ était un corps. Étudions un peu ces anneaux obtenus en rajoutant une racine d'un polynôme.

Définition (extension). *Une* ***extension*** *d'un anneau* A *est un morphisme d'anneaux de source* A*, souvent identifiée à son anneau but.*

Exemples. $\mathbf{R} \hookrightarrow \mathbf{C}$, $\mathbf{Q} \hookrightarrow \mathbf{Q}[\sqrt{2}]$, $\mathbf{Z} \hookrightarrow \mathbf{Z}[i]$, $\mathbf{Z} \twoheadrightarrow \mathbf{Z}/n$ (plus généralement, le morphisme d'itération permet de réaliser tout anneau comme une extension de $\mathbf{Z}$). Ce dernier cas (non injectif) n'arrive jamais avec les corps.

Propriété (extension de corps). *Une extension d'un corps est toujours injective, donc* doit *être pensée comme une inclusion.*

Preuve. Soit $k \longrightarrow K$ une extension de corps. Son noyau est un idéal de k, donc ou bien k (mais alors l'unité n'est pas préservée) ou bien (0) (ce qui correspond à l'injectivité demandée).

Soit $k \hookrightarrow K$ une extension de corps. Soit $a \in K$. Regardons le morphisme $\left\{ \begin{array}{ccc} k[X] & \longrightarrow & K \\ P & \longmapsto & P(a) \end{array} \right.$. S'il est injectif, on dit que a est ***transcendant*** sur k (exemples *durs* : les réels π et e sont transcendants sur $\mathbf{Q}$) ; sinon on dit que a est ***algébrique*** sur k (*i. e.* solution d'une équation algébrique, *i. e.*[9] polynomiale). Dans ce dernier cas, le noyau (qui est un idéal de $k[X]$, donc principal) est engendré par un unique polynôme unitaire μ_a appelé le ***polynôme minimal*** de a sur k. Par exemple, $\sqrt{2}$ est algébrique sur $\mathbf{Q}$ et y a pour polynôme minimal $X^2 - 2$.

Proposition (les corps $k[a]$). *L'image* $k[a]$ *est un corps ssi* μ_a *est irréductible. Dans ce cas, l'extension* $k \hookrightarrow k[a]$ *est de dimension finie* $\deg \mu_a$*.*

[8] mais il y a plusieurs isomorphismes entre deux tels corps, comme le montre l'exercice suivant

[9] le calcul dans les algèbres ($\mathbf{R}$, $\mathbf{C}$, $\mathbf{Q}[X]$, $M_n(\mathbf{R})$, $L(E)$...) *est* le calcul polynomial

Preuve. C'est l'analogue de "$\mathbf{Z}/_n$ *est un corps ssi* n *est premier*" (il faut les quotients pour le voir...) : mais on n'a plus ici la combinatoire des $\varphi(n)$, donc on fait à la main.

$\boxed{\Longrightarrow}$ Reprendre exactement la même preuve que pour décrire la caractéristique d'un corps en remplaçant le morphisme d'itération $\left\{\begin{array}{ccc}\mathbf{Z} & \longrightarrow & A \\ k & \longmapsto & k\cdot 1_A\end{array}\right.$ par le morphisme d'évaluation $\left\{\begin{array}{ccc}k[X] & \longrightarrow & K \\ P & \longmapsto & P(a)\end{array}\right.$.

$\boxed{\Longleftarrow}$ Soit $P(a)\neq 0$. Alors $P\notin(\mu_a)$, *i. e.* $\mu_a\not|P$, *i. e.* $\mu_a\wedge P=1$, d'où par Bézout $U\mu_a+VP=1$. Évaluer en a donne $U(a)P(a)+0=1$, d'où un inverse $U(a)$ pour $P(a)$.

Passons à la deuxième affirmation. Notons $d:=\deg\mu_a$ et montrons que $\left(1,a,a^2,...,a^{d-1}\right)$ est une base de $k[a]$. Soit $P(a)\in k[a]$: une division euclidienne $P=Q\mu_a+R$ montre que $P(a)=R(a)$ avec $\deg R<\deg P$, d'où le caractère générateur. Par ailleurs, une relation de liaison $\sum_{i=0}^{d-1}\lambda_i a^i=0$ s'écrit $P(a)=0$ (*i. e.* $P\in(\mu_a)$) où $P:=\sum_{i=0}^{d-1}\lambda_i X^i$ est de degré $<d$, d'où $P=0$ à cause des degrés, ce qui montre la liberté.

Définition (degré d'une extension finie). *Soit $k\hookrightarrow K$ une extension de corps. La dimension de K, vu comme k-e. v., s'appelle le* ***degré*** *de l'extension* (par analogie avec les extensions $k\hookrightarrow k[a]$) *et sera notée $[K:k]:=\dim_k K$. Une extension est dit* ***finie*** *si son degré est fini.*

Exercice (degré d'une extension composée). *Montrer que la composée d'extensions finies reste finie et que son degré vaut le produit des degrés :*

$$k\hookrightarrow K\hookrightarrow L\Longrightarrow[L:k]=[L:K][K:k].$$