$\mathbf{Q}$, $\mathbf{R}$, polynômes & achèvements

Marc SAGE

avril 2018

Table des matières

Résumé

Ce texte propose une construction des complexes depuis les ensembles, en passant par les naturels, les rationnels positifs, les réels positifs, puis les réels. L'angle d'approche pour les rationnels et les complexes est polynomial (rajouter des racines manquantes à l'aide de quotients), tandis que celui pour les réels utilise les ordres achevés (où chaque partie admet un *supremum*) en déguisant les coupures de Dedekind.

[1]REF biblio *Stetigkeit und irrationale Zahlen* 1872 (*continuité et nombres irrationnels*)

Belle histoire : *la création des nombres* H. Sinaceur Vrin 2008

1 Intro

prérequis : monoïdes, rég, groupes, anneaux, corps, quotients d'algèbres par idéaux, polynômes à plusieurs indéterminées sur un anneau

1.1 Caractérisation de N, Z, Q, R, C

$\mathbf{N}$; monoide monogène infini ? ? ? (ou peano)
$\mathbf{Z}$ groupe mongène (infini ou $\hookleftarrow \mathbf{N}$)
$\mathbf{Q}$ corps mongène (infini ou $\hookleftarrow \mathbf{N}$)
$\mathbf{R}$ corps ordonné complet

1.2 Deux idées, motivations, résumé

1) rajouter les racines de polynômes (= boucher les trous algébriques). EGs :

1. partant de $\mathbf{R}$, on construit $\mathbf{C}$ en rajoutant une racine à X^2+1, çàd en quotientant $\mathbf{C}[X]$ par l'égalité $X^2+1=0$. Nommer la racine rajoutée i et le tour est joué, la $\mathbf{R}$-algèbre ${}^{\mathbf{C}[i]}\!\diagup_{i^2+1}$ étant un corps vu l'irréductibilité du diviseur X^2+1. Par D'ALEMBERT GAUSS ce corps est algébriquement clos, c'est $\mathbf{C}$.
2. dans $\mathbf{Z}$ rajouter des racines de $nX-1$ où n parcourt[2] $\mathbf{N}^*$(afin d'inverser les non-nuls, d'où $\mathbf{Q}$)
3. dans $\mathbf{N}$ rajouter une racine de $X+1$ (afin d'opposer 1, ce qui livre $\mathbf{N}[-1]=\mathbf{Z}$) ou bien de X^2+1 (pour avoir directement $\mathbf{N}[i]=\mathbf{Z}+i\mathbf{Z}$)

Renvoi à cours quotient dans algèbre poly. Vu le départ $\mathbf{N}$, on devra travailler sans soustraction –> **semi-anneaux**.(*cf.* partie 2.3)
De même, pour inverser des éléments d'un monoïde, la régularité sera essentielle –> **semi-groupes** (*cf.* partie 2.2)

2) rajouter les suprema (=boucher les trous ordinaux) (*cf.* partie 4) :
facile dans un $\mathsf{P}(E)$ en rajoutant les réunions (car sup = $\cup$)
puis plonger chaque odrre $\left\{\begin{array}{ccc} O & \hookrightarrow & \mathsf{P}(O) \\ o & \longmapsto & S_o := \{s\}_{s\leq o}\end{array}\right.$
idéal pour passer de $\mathbf{Q}_+$ à $\mathbf{R}_+$

Restera à voir les compatibiltiés de ces constructions $+\times<$. **En résumé :**

1. on plonge $\mathbf{N}\hookrightarrow {}^{\mathbf{N}[m,i_1,i_2,i_3,\ldots]}\!\diagup_{\substack{m+1\\ ni_n+m}}$ dans semi-anneau $\mathbf{Q}$. Aors , $i_n=\frac{1}{n}$ (car $1=ni_n+m+1=ni_n$)
2. Def $\mathbf{Q}_+ := \mathbf{N}[i_{n\geq 2}] = \left\{\frac{n}{d}\right\}_{d\in\mathbf{N}^*}^{n\in\mathbf{N}}$ semi-corps, def $a<b \iff \exists q\in\mathbf{Q}_+^*,\ b=a+q \iff \exists\frac{n}{d}\in\mathbf{N}^*, da=db+n$, prolonge ordre $\mathbf{N}$, compat $+$, archim. Sur $\mathbf{Q}_+$: ordre EN OUTRE compat $\times$, total, avec différences
3. Achever $\overline{\mathbf{R}_+}$ retirer ∞ et annelliser le reste ? ? ?Check all avec bureacratie

2 Préliminaires

2.1 Monoïdes

PT *Soit $o\mapsto\mathbf{o}$ morphisme pour loi, mq $\langle\mathbf{o}\rangle=\langle\mathbf{m}\rangle_{m\in\langle o\rangle}$ (servira pour achèvement).*
$\subset$ claire car $\langle\mathbf{m}\rangle_{m\in\langle o\rangle}$ contient $\mathbf{o}$ et stable (car psv loi). Soit réciproqement $m\in\langle o\rangle$, soit Σpartie but contenant $\mathbf{o}$ et stable, mq $\mathbf{m}\in\Sigma$ (ce qui conclura $\mathbf{m}\in\cap\Sigma=\langle\mathbf{o}\rangle$) : la préimage de$\Sigma$ contient o et est stable, donc contient $\langle o\rangle\ni m$, d'où $\mathbf{m}\in\Sigma$ QED

[2]on pourrait bien sûr restreindre l'indexation aux *premiers*

2.2 Semi-groupes, grégarisation

On appellera ***semi-groupe*** tout monoïde régulier. EG ; $\mathbf{N}$, $\mathbf{Q}_+$ pour $+$. SiA anneau intègre, alors A^* pour $\times$.

Pour inverser les éléments (non nuls) d'un anneau commutatif, il suffit que ce dernier soit intègre, càd que chaque élément non nul soit régulier pour $\times$ (l'inversion fournit alors le corps des fractions de l'anneau considéré). On peut même choisir de n'inverser qu'une partie des éléments réguliers (par exemple, inverser 10 dans $\mathbf{Z}$ livre les nombres décimaux). Généralisons.

Soit M un semi-groupe abélien noté additivement (typiquement $\mathbf{N}$, $\mathbf{Q}_+$ ou $\mathbf{R}_+$) et soit $P \subset M$. Nous allons montrer que

le semi-groupe M se plonge[3] dans un semi-groupe $M - P$ engendré par (l'image de) M et l'opposé (de l'image) de P.

En particulier, lorsque P est la partie pleine :

le semi-groupe M se plonge dans un $\underline{\underline{\text{groupe}}}$ $^\natural M$ engendré par (l'image de) M.

Un tel groupe $^\natural M$ est appelé le ***symétrisé***[4] ou le ***grégarisé***[5] de M. Intuitivement, grégariser M est rajouter à M les différences d'éléments qui ne seraient pas déjà opposables dans M (et rien d'autre). Le terme « grégarisation » peut désigner autant l'*acte* de grégariser que l'*objet résultant* de cet acte (ici le groupe $M^\natural$, identifié abusivement à l'injection $M \hookrightarrow M^\natural$).

Avec ce résultat[6], on peut définir le groupe $(\mathbf{Z}, +)$ comme le grégarisé du monoïde additif $\mathbf{N}$. De la même façon, nous définirons le groupe $(\mathbf{R}, +)$ comme le grégarisé du monoïde additif $\mathbf{R}_+$. (Il restera ensuite à montrer que l'ordre et la multiplication se transportent bien.)

RQ : on a unicité même si anabélien avec bonne formulation catégorielle (cf feuille exos lois composition)

S'entraîner tout d'abord à établir *l'unicité d'un tel semi-groupe $M - P$ à unique*[7] *isomorphisme près* (unicité traduisant la parenthèse « et rien d'autre »). Au vu de cette unicité, il sufit d'exhiber *un* morphisme $M \hookrightarrow M - P$ qui convienne. Procédons par analyse-synthèse dans le cas simple $M = \mathbf{N} = P$.

[Analyse.] Vu la condition souhaitée d'engendrement de $^\natural\mathbf{N}$, chaque élément de $^\natural\mathbf{N}$ est censé être une somme d'(images de) naturels ou d'opposés de ces dernières ; vu par ailleurs la commutativité de l'addition entière, on peut regrouper d'un côté les naturels et d'un autre les opposés. Chaque élément de $^\natural\mathbf{N}$ peut alors s'écrire comme une différence $m-p$ où chaque lettre dénote (l'image d')un naturel, deux telles différences $m-p$ et $\mu - \pi$ coïncidant si $m + \pi = \mu + p$. [Fin de l'analyse.]

Grégarisation (construction classique). L'analyse nous incite à définir $M - P$ par l'ensemble des couples $\binom{m}{p} \in M \times \langle P \rangle$ *modulo* les égalités précédentes[8], on vérifie que la structure de semi-groupe produit[9] de $M \times \langle P \rangle$ passe au quotient et induit un morphisme injectif[10] $\left\{ \begin{array}{ccc} M & \hookrightarrow & M - P \\ m & \longmapsto & \overline{(m, 0)} \end{array} \right.$ qui est bijectif ssi M est un groupe[11]. Chaque élément de $\in M - P$ pourra alors s'écrire $\overline{\binom{m}{p}} = \overline{\binom{m}{0}} - \overline{\binom{p}{0}}$ comme différence de (l'image d')un élément de M par (l'image d')un élément de P, comme attendu.

VOie de sortie : une fois $\mathbf{N}$ sur pied, on peut construire $\mathbf{R}$ à partir du grégarisé $^\natural\mathbf{N} = \mathbf{Z}$ par la méthode des quasi-morphisme[12]. *Idée* : coder un réel par la pente d'une droite dans un repère. Mais comme on n'a

[3] un ***plongement*** est un morphisme (ici : de monoïdes) injectif

[4] En musique, les altérations $\sharp$ et $\flat$ resp. "aiguisent" (an. : *sharp*) et "applatissent" (an. : *flat*) une note donnée, tandis que $\natural$ supprime ces altérations et recentre ainsi la note par rapport à ces deux dernières. Suivant cette analogie, on pourrait écrire $\binom{\sharp\mathbf{Z}}{\flat\mathbf{Z}} = \binom{\mathbf{N}}{-\mathbf{N}}$ et $\mathbf{Z} = {}^\natural\mathbf{N}$, d'où la notation choisie.

[5] de *grégaire*, adjectif relatif à *groupe* (plus compréhensible mais moins élégant : ***groupifié***)

[6] dont on pourrait lever l'hypothèse de commutativité et que l'on pourrait adapter sans régularité (bien que cela nous soit ici inutile)

[7] Comprendre : si $\begin{array}{c} M \overset{i}{\hookrightarrow} S \\ M \overset{j}{\hookrightarrow} T \end{array}$ sont deux tels plongements, il y a alors un unique isomorphisme $S \overset{\varphi}{\longrightarrow} T$ tel que $\varphi \circ i = j$. Intuitivement : les éléments de M (*modulo* les plongements i et j) sont fixés par φ.

[8] Dans le cas non régulier, la transitivé passe avec l'amendement suivant (qui reste bien sûr valide lorsque l'on interprête les couples comme différences) :

$$\binom{a}{b} \sim \binom{a'}{b'} \overset{\text{déf.}}{\iff} \exists m \in M, \quad \begin{array}{c} a + b' + m \\ = a' + b + m \end{array}.$$

[9] Pour que $M \times P$ soit stable par la loi produit de M^2, il suffit de remplacer P par le semi-groupe $\langle P \rangle$ qu'il engendre.

[10] Sans régularité, ce morphisme est précisément injectif ssi M est régulier.

[11] Chaque groupe abélien vaut donc son propre grégarisé, ce qui est rassurant : rien besoin de rajouter pour obtenir un groupe !

[12] *cf.* par exemple la présentation par Xavier Caruso sur sa page http ://xavier.toonywood.org/papers/publis/R.pdf

pas encore les réels on remplace les application linéaires par des applications $Z \longrightarrow Z$ dont le graphe est "bien" encadré pour ressembler à une droite.w

2.3 Semi-anneaux, annellisation

Appelons ***semi-anneau***.tout semi-groupe A (lettre "A" gothique) muni d'une seconde loi pour laquelle A est un monoïde distributif[13] sur $+$ (cela force $+$abélien). Informellement, un semi-anneau est un anneau sans soustraction[14], à l'instar de $\mathbf{N}$ ou $\mathbf{R}_+$ munis des $+$ et $\times$ usuels. De fait, chaque anneau est un semi-anneau et, réciproquement, si A dénote un semi-anneau, alors A est un anneau ssi A un *groupe* additif. À retenir (et établir) :

un semi-anneau est un anneau ssi -1 est opposable.

sous-semi-anneau $\left(\iff \begin{cases} \text{stablepar } + \times \\ \text{contient } 0\ 1 \end{cases} \iff \text{sous-mono pour } +\times\right)$

semi-ev (semi-gpe & acvtion semianno), ***sous-semi-ev*** (<=>stable par CL <=> $\begin{array}{c}\text{sousmono}\\ \text{stable par homothie}\end{array}$),

notion stable par produit

d'où ***semi-algèbres*** classiques, en particulier celles polynomiales :

$\mathsf{A}[X] = \mathsf{A}^{(\mathbf{N})}$ semi-A-algèbre (sous-semi-ev de $\mathsf{A}^{\mathbf{N}}$) muni de multipication de Cacuhy $\binom{a}{b} \mapsto \left(\sum_{p+q=n}^{p,q\in\mathbf{N}} a_p a_q\right)_{n\in\mathbf{N}}$,

de même avec plusieurs indétermindées $\mathsf{A}\left[(X_i)_{i\in I}\right] := \mathsf{A}^{\left(\mathbf{N}^{(I)}\right)}$.

Annellisation (construction classique). Soit A semi-anneau, reprenons construction du grégarisé $^\natural\mathsf{A}$ où différences codées par couples. Vu le développement $(a-b)(\lambda-\mu) = (a\lambda+b\mu)-(a\mu+b\lambda)$ valide dans chaque anneau, on vérifie que la loi $\left(\binom{a}{b},\binom{\lambda}{\mu}\right) \mapsto \binom{a\lambda+b\mu}{a\mu+b\lambda}$ de A^2 passe au quotient $^\natural\mathsf{A}$ et se distribue sur l'addition quotient, ce qui enrichit le grégarisé $^\natural\mathsf{A}$ d'une structure d'anneau dans lequel se plonge notre semi-anneau A. Nous avons ainsi "annellisé" notre semi-anneau :

le semi-anneau A se plonge dans un anneau $^\natural\mathsf{A}$ engendré par (l'image de) A.

RQ : comme pour la grégarisation, l'***annelisation*** d'un semi-ano A (au sens d'un plongement $\mathsf{A} \hookrightarrow A$ dans un anneau engendré par (l'image de) A) est unique à unique iso près[15]

2.4 Quotients & semi-idéaux

Soit Mmono et soit $S \subset M$ stable non vide ***distinguée*** (au sens où $\forall m \in M,\ Sm = mS$)

Alors $a \sim b \overset{\text{déf.}}{\iff} \exists s,t \in S,\ as = bt$ est une relation d'équivalence compatible[16] et **le quotient préserve la régualirté**. Ainsi :

quotienter un semi-groupe par un sous-monoïde distingué livre un semi-groupe.

(RQ : on ne peut pas retrouver S à partir de la re. CEG : dans $\mathbf{N}$, chq $[n,\infty[$ engendre la relation grossière car $\forall a \leq b,\ a + \underline{(b-a)+n} = 0 + \underline{b+n}$. Question ouverte : étudier $S \mapsto$re ? ? ?)

Le cours sur les polynômes à plusieurs indéterminées se fait souvent sur un corps, voire un anneau. Il peut en fait s'effectuer sur un *semi*-anneau, ce qui permettra de parler de polynômes à coefficients dans $\mathbf{N}$ ou $\mathbf{Q}_+$ ainsi que des quotients associés.

Il convient toutefois de remplacer ce par quoi l'on quotiente, les idéaux (d'un anneau), par les ***semi-idéaux*** du sous-anneau A considéré (tout sous-monoïde additif stable par multiplication par chaque élément du semi-ano). EG : semi-idéal engendré par a est $(a) := \sum AaA$ (si a central, alors (a) devient $aA = Aa$). L'***égalité*** *modulo* I définie par $a \overset{I}{=} b \iff \exists i,j \in I,\ a+i = b+j$ est alors compatible avec les lois de A, le quotient est semi-anneau[17] et annule chaque élément de I (ainsi que leurs "différences").

quotienter un semi-ano par un semi-idéal livre un semi-ano.

[13] Ceci force la commutativité de l'addition (développer $(a+b)(1+1)$ de deux façons et utiliser la régularité). CEG sans reg : ω^2 semiano pas rég (où $+$ non com)

[14] Il manque *a priori* "la moitié des éléments" (leurs opposés), d'où la terminologie.

[15] Deux telles annellisations étant isomorphes en tant que groupes additifs (unicité de la grégarisation), il reste à vérifier que l'isomorphisme entre les deux préserve la multiplication et le 1).

[16] Quand M est un groupe, on retrouve (en inversant s ou t) l'égalité *modulo* S.

[17] cf quotients par sous-mono distingué pour $+$, le faire à la main pour $\times$

2.5 Annellisation bis

Soit A un semi-anneau. On rajoute des opposés à la main en opposant 1 : le plonger

$$\mathsf{A} \hookrightarrow {}^{\mathsf{A}[X]} \diagup_{X+1}$$

(comme $X+1$ commute à chq poly, le semi-idéal $(X+1)$ est principal). C'est un anneau (semiano où 1 opposable) où A se plonge et engendré par l'image de A : Done!

vive les quotients de polynômes :-)

Plgt bij ssi A ano (importation de la grégarisation).

(**gaffe** : le fait d'être un corps ne passe pas forcéement)

2.6 Grégarisation bis

Rappel[18] : pour chaque corps K, le monoïde M se plonge *via* KRONECKER dans la K-algèbre $K[M] = K^{(M)}$ muni de $\times$ convolution.

Soit $M \hookrightarrow \mathbf{Q}[M]$ algèbre engendrée par monoïde M, soit $m \in M$. On l'inverse à la main en quotientant par les égalités $mX = 1 = Xm$:

$$M \hookrightarrow \mathbf{Q}[M] \hookrightarrow {}^{\mathbf{Q}[M][X]} \diagup_{mX=1=Xm} \supset \langle M, X \rangle .$$

Alors $M \hookrightarrow \langle M, X \rangle$ ssi m régulier ? ? ?. Donc on peut *rajouter* les inverse des réguliers mais inverser un non-reg va "fusionner" des élémets. Plus précisémenet, si a non-reg est inversé, les classe mod $\overset{a\cdot}{\underset{\cdot a}{}}$ deviennent triviales, d'où morphdimes ${}^{M}\diagup_{a} \longrightarrow \langle M, a^{-1} \rangle$ (QQ ouverte : noyau ? ? ? c'est tout si abélien[19], sinon...)

Cette utilisation des polynôme livre une *autre* construction de la grégarisation "relative" $M - P$ lorsque P est inclus dans les réguliers de P (et sans hypothèse de commutativté !). Comme $\mathbf{Q}$ pas encore construit, on adapte la construction de $K[M]$ en remplaçant le corps K par un *semi*-anneau, ce qui permet par exemple de donner sens à la semi-algèbre $\mathbf{N}[M]$. On y plonge M, on rajoute des indéterminées X_0 et $(X_p)_{p \in P}$, on quotiente par le semi-idéal engedré par $X_0 + 1$ et les $X_0 + pX_p$ lorsque p parcourt P (ajouter 1 à droite donne alors $1 = pX_p$) et on considère le sous-monoïde engendré $\langle M, X_p \rangle_{p \in P}$. C'est bien une grégarisation de P dans M !

vive les quotients de polynômes :-)

2.7 Monoïdes ordonnés

t

Les réels possédant une structure tant algébrique (corps) qu'ordonnée (topologie des intervalles), il convient d'étudier la compatibilité entre lois et ordre. Peu heureux d'étudier les deux sans compatibilité !

Principe de base : un ***magma ordonné*** est un magma muni d'un ordre compatible avec sa loi. çàd *on peut composer les comparaisons.*

EG : si M monoïde, alors $\mathsf{P}(M)$ muni de loi "parties" est mono ordonné.

Dans un monoïde ordonné, les majorants du neutre forment une partie stable et sont ainsi qualifiés ***positifs***. Si $\exists d \geq 0,\ b = a + d$, alors $b \geq a$, réciproque fausse ($2 < 3$ dans $\mathbf{N} \backslash \{1\}$). Mais ok dans *groupe* ordonné.

COmparons $\leq$ avec $a \precsim b \overset{def}{\Longleftrightarrow} \exists d \geq 0,\ b = a + d$. On a tjs $\precsim \subset \leq$

DIsons qu'***il y a des différences*** si $\forall a \leq b,\ \exists d,\ b = a + d$ (pas tjs le cas, eg dans $\{0, 2, 3, 4, ..\}$), çàd si $\leq \subset \precsim$

RQ : on peut tjs rajouter à M un min absorbatn depuis lequel pas de dufférence ! (eg $-\infty < 0 \cdots$) C'est pourquoi on trouvera l'hypothèse avec la restriction $a$non minimal (le cas des minimaux, svt peu intérssant et facile à traiter, étant laissé au contexte)

Ordonner un groupe abélien (disons additif) revient à se donner une partie stable (dont les éléments sont dits ***positifs***) telle que chaque élément est positif ou d'opposé positif, 0 étant le seul à être les deux à la foi

tranfère ordre à l'annellisé ? ? ?

PT :*soit monoide ordonné. Si régulier, alors ajouter $<$ et $\leq$ donne $<$.*

[18] *cf.* cours sur les invariants dans l'algèbre d'un monoïde

[19] cf feuille exos lois composition

Récipque ok si ordre total, faux en général sinon (CEG $\begin{smallmatrix}0\\0'\end{smallmatrix}$ 1 2 3... où $0'$ "neutre" sauf pour 0)

Reprenons grégarisation classique dans semi-groupe M abélien

La relation $a \leq b \overset{\text{déf.}}{\iff} \exists m, b = a + m$ définit un ordre sur M ssi 0 en est le seul opposable (ce qui est le cas des semi-groupes[20] $\mathbf{N}$ et $\mathbf{R}_+$), auquel cas la relation $\binom{a}{b} \leq \binom{a'}{b'} \overset{\text{déf.}}{\iff} a + b' \leq a' + b$ passe au quotient.

Lorque cet ordre est de plus total, on montre que chaque élément du grégarisé $^\natural M$ est dans M ou est l'opposé d'un élément de M, la terminologie *symétrisé* prenant alors tout son sens.

[? ? ? inutile ? ? ?]

Soit M mono, soit $P \subset M$, def $a \succ b \iff a \in bP$, noter $P \lhd M$ pour $\forall m \in P,\ Pm \subset mP$ et $^{-1}P := \{m \in M\ ;\ 1 \in mP\}$. Alors

réf ssi $1 \in P$ ref & $\lhd \Longrightarrow$ compat compat$\Longrightarrow$stable$\Longrightarrow$trans trans & $\lhd \Longrightarrow$ compa antisym si $P \cap\ ^{-1}P = \{1\}$ total $\Longrightarrow P \cup\ ^{-1}P = M$ (réc fausse : mono$1 < \begin{smallmatrix}a\\b\end{smallmatrix} < \begin{smallmatrix}a^2 & b^2\\ab & ba\end{smallmatrix}$ avec $P = M \lhd$)

Pstable$\Longrightarrow$ $P \succ\ ^{-1}P$ Pstable&$\lhd\Longrightarrow$ $^{-1}P \lhd$

[? ? ? inutile ? ? ?]

PT *soit M mono abélien. On relie $^\natural M = M - M$ par $\exists d \in M,\ b = a + m$. Alors*
** rel comptabil avec loi $^\natural M$*
** prolonge ordre de M ssi 0 en est le seul opposable*
** préserve carac total*
** préserve achèvement* (2démos si partie$\not\subset M$: par oppositio, par translation)

grégar commute à achevet ? ? ?

Un monoïde ordonné est dit ***archimédien*** quand chaque élément strictement positif engendre un monoïde non majoré.

RQ : on peut tjs rajouter à M un max absorbatn qui majore ainsi chaque monoïde engendré, bloquant ainsi artificiellement l'archéimédianté (eg $\overline{\mathbf{N}}$) C'est pourquoi on trouvera l'hypothèse restreinte à M privé de son éventuel max.

PT *Soit $o \mapsto \mathbf{o}$ croissant : mq source archi si but archi*
(on verra <= avec hypo en plus)
Suppo $\mathbf{O}$ archi, soient $p > 0$ et $o \in O$. Alors $\exists \mu \in \langle \mathbf{p} \rangle = \langle \mathbf{m} \rangle_{m \in \langle p \rangle}$ tq $\mu > \mathbf{o}$, çàd $\exists m \in \langle p \rangle$ tq $\mathbf{m} \not\leq \mathbf{o}$, çàd tq $m \not\leq o$
<= *ok si* $\leq$*tot et si $o \mapsto \mathbf{o}$ morphisme +*
Suppos O archim. Soient $\begin{matrix}\pi > \mathbf{0}\\ \alpha \in \overline{O} \setminus \max\end{matrix}$, soit (*tot*) $\begin{matrix}\mathbf{0} < \mathbf{p} \leq \pi\\ \mathbf{q} > \alpha\end{matrix}$. (QQ**??**) Soit $m \in \langle p \rangle$ tq $m > q$. Alors $\{m\ ;\ \exists \mu \in \langle \pi \rangle,\ \mu \geq \mathbf{m}\}$ contient p (prendre $\mu := \pi$) et est stable (*compat*), donc contient $\langle p \rangle$, d'où un $\mu \in \langle \pi \rangle$ tq $\mu \geq \mathbf{m} > \mathbf{q} > \alpha$
? ? ? où mettre cela ? ? ?

2.8 Anneaux ordonnés

Un ***anneau ordonné*** est un anneau A muni d'une partie stable par somme et produit (dont les éléments sont dits ***positifs***) telle que chaque élément est positif ou d'opposé positif, 0 étant le seul à être les deux à la fois. Une telle partie positive définit un ordre *total* par « a vient avant b quand $b - a$ est positif » compatible avec l'addition et (si restreint aux *positifs*) la multiplication, ainsi qu'une valeur absolue valant l'identité sur les positifs et l'opposition sur les négatifs. Un anneau ordonné est dit ***archimédien*** quand chaque élément strictement positif engendre un semi-groupe additif non majoré.

En symboles : les positifs de A forment une partie $P \subset A$ telle que $\begin{cases} P + P \subset P \\ P \cdot P \subset P \end{cases}$ et $\begin{cases} A = P \cup -P \\ \{0\} = P \cap -P \end{cases}$, laquelle induit un ordre total par « $a \leq b \overset{\text{déf.}}{\iff} b - a \in P$ » permettant l'ajout des comparaisons dans A et la multiplication des comparaisons dans P, ainsi qu'une valeur absolue $|a| \mapsto \max\{a, -a\}$, l'archimédianité s'écrivant[21] $\begin{matrix}\forall p \in P^*\\ \forall a \in A\end{matrix}$, $\exists m \in \langle a \rangle,\ m > a$.

Montrons *l'archimédianité des anneaux ordonnés dont chaque partie (non vide majorée) possède un supremum*[22].

[20] littéralement des **semi**-groupes au sens de **moitiés** de groupes
[21] m comme **m**ultiple (en effet, lorsque A est muni d'un prédicat "être un naturel", on peut expliciter $\langle p \rangle = \{np\}_{n \in \mathbf{N}}$)
[22] Il est donc *inutile* d'imposer le caractère archimédien dans les hypothèses d'unicité du corps des réels !

Dans un tel anneau, soit a par lequel le semi-groupe additif engendré $\langle a \rangle$ est majoré. Fait alors sens son *supremum* $B := \sup \langle a \rangle$. Pour chaque multiple $m \in \langle a \rangle$, on peut majorer $B \geq \langle a \rangle \geq m + a$, d'où $B - a \geq m$; faire varier m donne alors $B - a \geq \sup \langle a \rangle = B$, d'où $a \leq 0$.

EG de corps ordonné non arichmédien : pour chaque k corps ordonné, $k(X)$ ordonné par "rapport coefs dom est positif" (alors X majore les multiples de 1)

Soit A ano ordonné non nul. 1 ou bien -1 étant positif, leur carré 1 le reste, d'où $1 > 0$. L'addition étant compatible avec l'ordre et régulière, on peut ajouter des comparaison strictes, d'où $n > 0$ pour chaque naturel n, ce qui montre que

chaque anneau ordonné est (nul ou) de caractéristiqe nulle

En particulier, dans chaque *corps* ordonné on peut plonger $\mathbf{Q}$ et découper les ε en morceaux comme d'habitude. Dans un tel corps, il équivaut de dire :

1. chaque partie (non vide majorée) possède un *supremum* ;
2. chaque suite de Cauchy converge ;
3. chaque suite bornée admet une valeur d'adhérence.

Un corps vérifiant ces conditions est unique[23] *à (unique) isomorphisme près – et est archimédien.*

3 De Q à R (*via* Leray, "classique")

Partons maintenant de $\mathbf{Q}$ et donnons un peu de terminologie.

Soit E un espace métrique (par exemple $\mathbf{Q}$ muni de sa distance usuelle).

L'espace E est dit ***complet*** si chaque suite de Cauchy à valeur dans E converge. Par exemple, sont complets l'espace $\mathbf{R}$ ainsi que l'espace $\mathcal{B}(E, \mathbf{R})$ des fonctions réelles *bornées*.

On appelle ***complétion*** de E toute isométrie[24] $E \hookrightarrow \overline{E}$ vers un métrique complet $\overline{E}$ dans lequel l'image de E est dense[25]. Intuitivement, compléter E est rajouter à E les limites de suites qui ne convergeraient pas déjà dans E (et rien d'autre). S'entraîner d'ailleurs à montrer qu'une complétion de E est unique à isomorphisme près[26]. Le terme « complétion » peut désigner autant l'*acte* de compléter que l'*objet résultant* de cet acte (ici l'espace complet $\overline{E}$, identifié abusivement au plongement $E \hookrightarrow \overline{E}$).

Pour compléter un espace métrique au sens ci-dessus, une idée attribuée à Leray (1869) et indépendamment à Cantor (1870) consiste à coder chaque "limite ℓ éventuellement pas déjà dans E" par une de ses approximations, çàd par une suite tendant vers ℓ (par exemple, chaque point de E s'approche (parfaitement !) par la suite constante valant partout le point considéré). Bien sûr, rajouter à une telle approximation une suite tendant vers 0 ne change pas la limite approchée. La tendance pouvant ne pas faire sens dans E (justement quand la limite visée n'y est pas), on remplacera la tendance vers ℓ par le caractère de Cauchy. Certes, on perd alors trace de la limite ℓ explicite mais la complétude de l'espace d'arrivée conserve *implicitement* cette limite, le tout bien sûr *modulo* l'ajoute des suites tendant vers 0.

Formellement, on en vient finalement à quotienter l'ensemble des suites de Cauchy à valeurs dans E par la relation « la différence tend vers 0 » et à y plonger E en associant à chaque point la suite constant valant partout ce point.

Ainsi $\mathbf{R}$ peut-il se définir comme la complétion[27] de $\mathbf{Q}$. Un des avantages de cette idée est que la structure d'anneau de $\mathbf{Q}$ se transfère bien à ses suites de Cauchy et passe au quotient. Il est cependant moins immédiat de tranférer l'ordre et de montrer la complétude.

Bonus. Une fois contruit $\mathbf{R}$, on peut compléter chaque espace métrique E non vide (soit ε dedans) à l'aide de l'isométrie[28] $\Delta := \left\{ \begin{array}{ccc} E & \hookrightarrow & \mathcal{B}(E, \mathbf{R}) \\ e & \longmapsto & d(e, \cdot) - d(\varepsilon, \cdot) \end{array} \right.$ corestreinte à l'adhérence de son image. En

[23] Les deux hypothèses sont indispensables : $\mathbf{Q}$ est un corps ordonné non complet, $\mathbf{C}$ est un corps complet non-ordonnable.

[24] les structures étant ici métriques, les morphismes sont les isométries, lesquelles sont toujours injectives

[25] la densité lève l'ambigüité de la barre coiffante

[26] Si i et j dénotent deux complétions, on a même *unicité* d'un isomorphisme φ faisant commuter le diagramme $\begin{tikzcd} & \overline{E} \arrow[d, "\varphi"] \\ E \arrow[ur, hook, "i"] \arrow[r, hook, "j"'] & \widetilde{E} \end{tikzcd}$ (çàd fixant E *modulo* plongements)

[27] La distance d'un espace métrique est usuellement imposée à valeurs *réelles*. Concernant l'espace $\mathbf{Q}$, sa distance est évidemment entendue *rationnelle*.

[28] Δ comme « **d**ifférence de **d**istances »

effet, d'une part l'espace E se plonge bien (isométriquement) dans $\overline{\Delta(E)}$, d'autre part le fermé $\overline{\Delta(E)}$ du complet $\mathcal{B}(E,\mathbf{R})$ est complet, *QED* !

Rq (de N à C sans passer par R) Partant de $\mathbf{N}$, simultanément rajouter i et inverser les naturel livre une construction de $\mathbf{Q}(i)=\mathbf{Q}+i\mathbf{Q}$ par $\mathbf{N}\left[(I_n)_{n\in\mathbf{N}^*}\right]$ où l'on quotiente par les égalités I_1^2+1 et $nI_n+I_1^2$ pour chaque naturel $n\geq 2$. On peut alors contruire $\mathbf{C}$ à partir de $\mathbf{Q}(i)$ par complétion à la LERAY, sans passer par $\mathbf{R}$ et donc sans préoccupation d'ordre[29].

Le bonus ci-dessus évite de répéter la construction précédente dont les quotients peuvent rebuter, en s'appuyant toutefois sur la complétude de $\mathbf{R}$. Or voici à présent une complétion de $\mathbf{R}$ qui évite les quotients de suites.

4 De $\mathbf{Q}_+$ à $\overline{\mathbf{R}_+}$ (*via* Dedekind[30])

Un autre point de vue pour compléter $\mathbf{Q}$ (et même un peu plus) est de se souvenir de l'origine *ordonnée* de sa topologie (ses ouverts étant les réunions au-plus-dénombrables d'intervalles ouverts) et de s'intéresser plutôt à la propriété de la borne supérieure. On abrégera $\vee:=\sup$.

Soit O un ensemble ordonné (par exemple $\mathbf{Q}_+$ muni de son ordre usuel).

Pour chaque $o\in O$, on notera $C_o:=\{e\in O\ ;\ e<o\}$ la ***coupure initiale***[31] associée.

L'ordre O est dit ***achevé*** si chaque partie de O admet un *supremum*[32]. Par exemple, chaque ensemble $\mathcal{E}$ induit avec l'inclusion un ordre $\mathsf{P}(\mathcal{E})$ achevé, les *supremum* et *infimum* correspondant resp. aux réunion et intersection.

Une application f est dite ***achevée*** si chq égalité $f(\vee S)=\vee f(S)$ tient dès qu'elle fait sens. (CP : entre ordres achevés, être achevée <=> préserver $\vee$). RQ : achevée => croissante (regarder les paires)

Nous montrerons que (lorsque O est total) l'application $c:=\begin{cases} O & \longrightarrow & \mathsf{P}(O) \\ o & \longmapsto & C_o \end{cases}$ est injective et achevé : il s'agit alors d'un *plongement d'ordres achevés* (les morphismes étant les applications achevées).

Pour chaque partie $P\subset O$, on appelle $\vee$***adhérece*** de P l'ensemble $\overline{P}$ des éventuels *suprema* des parties de P et on dit que P est $\vee$***dense*** si $\overline{P}=O$ (çàd si chaque point de O est le *supremum* d'une partie de P). On vérifiera qu'est achevée chaque $\vee$adhérence dans chaque ordre achevé[33].

Trois analogies donc avec la vision métrique :

1. les achevés $\mathsf{P}(O)$ correspondent aux complets $\mathcal{B}(E,\mathbf{R})$ (exemples génériques) ;
2. chaque ordre (resp. métrique) se plonge dans un achevé *via* c (resp. un complet *via* Δ) ;
3. l'adhérence (avec "$\vee$" ou sans) attribue le caractère désiré ("achevé" ou "complet") quand la structure ambiante le possède (à l'instar des exemples génériques précédents).

Appelons ***achèvement*** de O toute injection achevée $O\hookrightarrow\overline{O}$ vers un ordre achevé $\overline{O}$ dans lequel l'image de O est $\vee$dense[34]. Intuitivement, achever O est rajouter à O les *suprema* qui ne seraient pas déjà dans O (*plgt* d'ordres à *but achevé*) et rien d'autre (plgt *achevé*)[35], sans toucher aux *suprema* en place[36]. Comme pour la complétion, le terme « achèvement » peut désigner autant l'*acte* d'achever que l'*objet résultant* de cet acte (ici l'ordre achevé $\overline{O}$, identifié abusivement au plongement $O\hookrightarrow\overline{O}$).

On peut achever l'ordre O (si total) à l'aide du plongement c corestreint à l'adhérence de son image. En effet, d'une part l'ordre O se plonge bien dans $\overline{c(O)}$ en respectant $\vee$, d'autre part l'$\vee$adhérence $\overline{c(O)}$ dans l'achevé $\mathsf{P}(O)$ est achevée, *QED*.

Ainsi $\overline{\mathbf{R}_+}$ peut-il se définir comme l'achèvement de l'ordre total $\mathbf{Q}_+$, l'infini ∞ apparaissant alors comme son plus grand élément. Par ailleurs, en munissant $\mathsf{P}(\mathbf{Q}_+)$ des addition et multiplication "parties" (chacune

[29] Cependant, montrer le carc alg clos utilise habtiluellement des fonction *réelles* atteignant leur minimum sur un compact : si la compacité locale de $\mathbf{C}$ est livrée avec la complétion à la LERAY, il semble toutefois difficile de se passer complètement de $\mathbf{R}$.

[30] REF biblio *Stetigkeit und irrationale Zahlen* 1872 (*continuité et nombres irrationnels*)

[31] La lettre C réfère aux **c**oupures de DEDEKIND. Observer l'identification de chaque élément de O à sa coupure initiale associée (identification ne gardant que la moitié d'une coupure-au-sens-originel-de-DEDEKIND).

[32] Cela équivaut à l'existence de l'*infimum* de chaque partie. Chaque ordre achevé admet un maximum $\sup O=\inf\emptyset$ et un minimum $\inf O=\sup\emptyset$.

[33] Utiliser l'associativité du *supremum* sous la forme $\sup_{i\in I}\sup A_i=\sup\bigcup_{i\in I}A_i$ (pour chaque famille (A_i) de parties d'un ordre achevé).

[34] la densité lève l'ambigüité de la barre coiffante

[35] Si l'ordre O est *total*, on peut montrer l'unicité des achèvements de O à unique isomorphisme achevé près.

[36] Dans le cas métrique, les limites déjà existantes étaient préservées par *continuité* du plongement. Dans le cas ordonné, c'est le caractère *achevé* du plongement qui préservera les *suprema* déjà existant.

unifère, associative et compatible avec l'ordre[37]), le plongement $\left\{\begin{array}{ccc}\mathbf{Q}_+ & \hookrightarrow & \mathsf{P}(\mathbf{Q}_+)\\ q & \longmapsto & C_q\end{array}\right.$ préserve les deux lois[38] (tout l'intérêt pour $\times$ de rester dans le positif !), ce qui transporte *ipso facto* la structure de semi-anneau ordonné de $\mathbf{Q}_+$ vers $c(\mathbf{Q}_+)$

Reste à établir l'ordre total $\overline{c(\mathbf{Q}_+)}$, la distrib et la régularité de $+$. Relevons les manches.

5 Bureaucratie

On vérifiera que $\mathbf{Q}_+$ (muni de $\leq +\times$ standards) vérifie toutes les hypothèses suivantes :

1. $\times$ se distibue sur $+$
2. l'ordre $\leq$ est total et compatible avec les lois $+$ et $\times$
3. l'application $c := \left\{\begin{array}{ccc}\mathbf{Q}_+ & \hookrightarrow & \mathsf{P}(\mathbf{Q}_+)\\ q\neq 0 & \longmapsto & C_q\\ 0 & \longmapsto & \{0\}\end{array}\right.$ est injective, achevée, préserve $+$ et $\times$
4. (Archimède) chaque élément non maximal engendre un monoïde additif non majoré
5. chaque éléemnt non extrémal est régulier pour $+$
6. chaque paire $a<b$ où a non minimal admet des "différences" $\begin{smallmatrix}\acute{d}\\ \grave{d}\end{smallmatrix}$ tq $b=\begin{smallmatrix}a+\acute{d}\\ \grave{d}+a\end{smallmatrix}$.

Soit O un ordre muni de deux lois $\begin{smallmatrix}+\\ \times\end{smallmatrix}$ vérifant les conditions ci-dessus. Abrégeons $\mathbf{o}:=c(o)$, $\mathbf{O}:=\{\mathbf{o}\}_{o\in O}$, $\overline{O}$ l'achèvement de $\mathbf{O}$ dans$\mathsf{P}(O)$. Nous allons alors montrer que l'achèvement de $\overline{O}$ régi par les lois parties $+$ et $\times$ est un ordre total, un monoïde additif régulier surlequel $\times$ se distribue.

? ? ?cf fuille exo relation d'ordre "6relOrd" (en tirer un DM ? ? ?).

insrérer alors fin vérif avec symétrisisation

6 Création de N : itération et axiomes ensembliste

La théorie des ensembles est munie d'un unique symbole de relation (binaire), l'appartenance $\in$. à partir duquel on définit l'inclusion $\subset$ puis l'égalité $=$ (par double-inclusion $\begin{smallmatrix}\subset\\ \supset\end{smallmatrix}$). Afin de vérifier le principe de Leibniz (deux objets égaux ne peuvent être distingués par aucune propriété), on décrète axiomatiquement que

deux ensembles ayant même éléments appartiennent aux mêmes ensembles,

ce qui livre les équivalences usuelles[39]

$$\forall A,B,\ [A=B]\Longleftrightarrow[\forall e,\ e\in A\Longleftrightarrow e\in B].$$

Pour construire les naturels, l'axiome qui nous intéresse est[40], étant donné un objet de départ et une relation fonctionnelle, l'existence d'un ensemble contenant l'objet donné et stable par la "fonction" considérée. En bref,

les itérés de chaque objet par chaque "application" forment un ensemble.

En notant o l'objet de départ et f la "fonction" itérante, un tel ensemble se décrirait "par extension" sous la forme

$$\{o,\ f(o),\ f(f(o)),\ f(f(f(o))),\ f^4(o),\ f^5(o),\ ...\}$$

où les points de suspension cachent précisément l'essence de $\mathbf{N}$.

Lorsque la "fonction" est "injective" et n'atteint par l'objet de départ[41] (informellement : évite les boucles), chaque ensemble d'itérés (existant par l'axiome d'itération correspondant) ne saurait être fini ; le plus petit tel ensemble (formellement : leur intersection) peut alors s'appeler $\mathbf{N}$ et vérifiera les axiomes de

[37] même strict à deux exceptions évidentes près (multiplier par 0 ou ajouter ∞).

[38] En fait, pour $+$, il faudra remplacer l'inconvenant absorbant $C_0=\emptyset$ par le bien plus sage neutre $\{0\}$ (le nouveau c reste injectif et achevé). Nous voulons croire que ce bricolage est moins artificiel que la définition dedekinienne de la multiplication des coupures.

[39] De manière équivalente, on aurait pu prendre ces équivalences comme un axiome (l'***axiome d'extensionalité***), ce qui aurait supposé de disposer *au préalable* d'un symbole d'égalité.

[40] Il s'agit en fait d'un *schéma* d'axiomes (un par couple (objet, fonction) donné), que l'on pourrait appeler appeler ***axiomes d'itération***.

[41] prendre par exemple pour objet de départ l'ensemble vide $\emptyset$ et pour "application itérante" *Successeur* $a\mapsto a\cup\{a\}$ ou *Partie* $a\mapsto\mathsf{P}(a)$

Peano-Dedekind (où l'application itérante définit l'incrémentation $n \mapsto n+1$), lesquels reviennent à[42] vérifier le principe de bonne-définition-par-récurrence-des-suites :

$$\forall A, \left\{ \begin{array}{c} \forall f \in A^A \\ \forall @ \in A \end{array} \right., \exists ! a \in A^{\mathbf{N}}, \left\{ \begin{array}{c} a_0 = \alpha \\ \forall n \in \mathbf{N},\ a_{n+1} = f(a) \end{array} \right. .$$

Culture : si l'on part d'*un seul* axiome d'itération "sans boucle", on dispose alors d'un $\mathbf{N}$ et l'on déduit immédiatement *chaque* axiome d'itération – en notant o l'objet de départ et f la "fonction" itérante, envoyer chaque $n \in \mathbf{N}$ sur le n-ième itéré[43] $f^{\circ n}(o)$. Par conséquent, les axiomes d'itérations "sans boucle" sont deux à deux équivalents[44] et aucun $\mathbf{N}$ n'est à cet égard plus légitime qu'un autre ![45]

[42] cette équivalence n'est pas immédiate mais ne comporte aucune difficulté de fond

[43] Faute d'un ensemble d'arrivée pré-existant, il est usuel de faire appel aux ***axiomes de remplacement*** pour former l'ensemble image par cette "fonctionnelle".

[44] *modulo* remplacement

[45] L'***axiome de l'infini*** (usuellement énoncé) est l'axiome d'itération avec pour départ $\emptyset$ et pour itérante *Successeur* $a \mapsto a \cup \{a\}$. Techniquement, il a l'avatange de préparer la théorie ordinale où les opérations limites (qui transcendent l'itération au sens précédent) se décrivent de façon particulièrement compatible avec *Successeur*.