Groupe de travail pour élèves de lycée

Choisissez votre corps !

par

Xavier CARUSO

(Texte produit et tapé par Xavier CARUSO)

Le 12 janvier 2004

Table des matières

1 Introduction

1.1 Qu'est-ce qu'un corps ?

Pour casser le mythe dès le début, avouons que dans cet exposé un corps désignera un ensemble de nombres que l'on sait additionner, soustraire, multiplier et diviser. On va donc bien parler encore une fois de mathématiques. Formellement, un corps est donc un ensemble $\mathbb{K}$ dont les éléments sont appelés les nombres. Les opérations, quant à elles, sont incarnées par plusieurs applications. On a tout d'abord $+ : \mathbb{K}^2 \to \mathbb{K}$ et $\times : \mathbb{K}^2 \to \mathbb{K}$. La soustraction est juste donnée par l'application « opposé » : il faut donc en particulier fixer un élément 0 de $\mathbb{K}$. De même avant de parler de division, il faut fixer un élément $1 \in \mathbb{K}$; la division est simplement donnée par une application $\text{inv} : \mathbb{K}^\star \to \mathbb{K}^\star$, $\mathbb{K}^\star$ désignant l'ensemble $\mathbb{K}$ privé de l'élément 0 car évidemment il faut bien faire attention à ne pas diviser par 0.

Bien entendu, on demande à ces données de vérifier certaines propriétés évidentes. La première d'entre elles est l'associativité qui s'écrit ainsi :

$$+(x, +(y, z)) = +(+(x, y), z)$$

ce que l'on notera pas la suite plus lisiblement[1] :

$$x + (y + z) = (x + y) + z$$

En plus de cela, il y a trois autres axiomes naturels sur l'addition et la soustraction qui sont :

$$\begin{aligned} x + y &= y + x \\ x + 0 &= x \\ x - x &= 0 \end{aligned}$$

où $x - x$ désigne bien entendu la somme de x et de son opposé. Ces axiomes doivent être vérifiés pour tous éléments x et y dans $\mathbb{K}$. On a évidemment des axiomes analogues pour la multiplication. Ils sont :

$$\begin{aligned} x(yz) &= (xy)z \\ xy &= yx \\ x \times 1 &= x \\ x \times \frac{1}{x} &= 1 \end{aligned}$$

où $\frac{1}{x}$ désigne l'image de x par l'application inv. Bien évidemment, on ne demande que la dernière propriété ne soit vérifiée que pour $x \neq 0$.

À tout cela, il faut finalement rajouter une condition de compatibilité entre les deux opérations, condition que l'on nomme *distributivité* et qui est :

$$x(y + z) = xy + xz$$

Elle doit, elle aussi, être vérifiée pour tous éléments x, y et z de $\mathbb{K}$.

Voilà pour la définition. Il y a ensuite les exemples évidents : $\mathbb{Q}$, $\mathbb{R}$ ou encore $\mathbb{C}$ sont des corps. Les opérations que l'on définit sur ces ensembles sont les opérations usuelles.

[1] Lorsque l'on omet les parenthèses et que l'on met les signes $+$ et $\times$ à droite, on obtient ce que l'on appelle la *notation polonaise inversée*, notation utilisée sur certaines calculatrices.

Ces opérations vérifient tous les axiomes listés précédemment. Bien sûr, ce ne sont pas les seuls exemples... le but de ce exposé est précisement d'en construire d'autres sans doute un peu plus exotiques.

Avant de passer à cela, faisons plusieurs remarques utiles. Les applications « opposé » et « inverse », si elles existent, sont forcément uniques comme on le vérifie facilement. Ainsi pour définir un corps, on aura simplement besoin de donner les applications $+$ et $\times$ et de vérifier les axiomes. Par ailleurs, ces axiomes impliquent que le produit $0 \times x$ vaut toujours 0. En effet, il suffit pour cela de calculer :

$$0 \times x = (0 + 0) \times x = 0 \times x + 0 \times x$$

et de simplier par $0 \times x$ pour obtenir le résultat. Ainsi l'on voit pourquoi il est illusoire de penser pouvoir calculer l'inverse de 0 : on ne peut pas obtenir 1 en multipliant 0 par quelque chose puisque l'on obtient toujours 0.

1.2 Un exemple trop naïf

On va considérer dans ce paragraphe l'ensemble $\mathbb{R}^+$ des réels positifs, mais on change la façon de multiplier et d'additionner ces nombres. Afin d'éviter les confusions nous allons appeler $\mathbb{K}$ et non plus $\mathbb{R}^+$ ce nouvel ensemble de nombres. Le corps $\mathbb{K}$ que l'on va considérer a encore une subtile différence avec $\mathbb{R}^+$. On sait que dans $\mathbb{R}$ les deux nombres $0,999\ldots$ (donc avec une infinité de 9) et 1 sont égaux. Ce n'est pas une condition que l'on imposera dans $\mathbb{K}$. Une façon correcte de procéder est de définir un élément de $\mathbb{K}$ comme la suite de ses décimales ; ainsi deux éléments de $\mathbb{K}$ sont distincts dès qu'ils ont une décimale qui diffère.

Comment additionne-t-on deux éléments de $\mathbb{K}$? On fait comme les petits écoliers du primaire. On pose l'addition, mais on ne tient pas compte des retenues. Par exemple, pour additionner 17 et 25, on écrit :

$$\begin{array}{cccc} & & 1 & 7 \\ + & & 2 & 5 \\ \hline & & 3 & 2 \end{array}$$

et le résultat est donc 32 et non 42 comme habituellement. On notera en particulier que pour faire ces opérations, on n'est plus obligé de commencer de la droite comme dans le cas classique : comme il n'y a pas de retenues, elles ne pourront pas influencer les résultats des colonnes plus à gauche.

En particulier, ce n'est pas du tout gênant qu'il y ait une infinité de chiffres après la virgule. Dans $\mathbb{R}$ (avec les opérations classiques donc), ce n'était pas non plus gênant, mais pour faire une telle addition, il fallait procéder par approximations successives... ce n'est plus la peine de procéder ainsi ici[2].

Intéressons-nous maintenant à la recherche d'un opposé. C'est en fait très facile et comme un exemple est souvent bien plus clair que de longues explications, essayons de calculer l'opposé de 1048. Il faut trouver un nombre qui additionné à 1048 fasse 0. On cherche donc à compléter l'opération suivante :

$$\begin{array}{cccccc} & & 1 & 0 & 4 & 8 \\ + & \_ & \_ & \_ & \_ & \\ \hline & 0 & 0 & 0 & 0 & \end{array}$$

[2] D'ailleurs on ne pourrait pas car on ne peut parler ni d'ordre ni d'encadrement sur le corps $\mathbb{K}$: en effet, comme on va le voir l'opposé de 1 est 9 et dans ces conditions, lequel des deux devrait être positif ?

Le premier chiffre doit forcément être un 9, le second un 0, le troisième un 6 et le quatrième un 2. On écrira donc sans vergogne $-1048 = 9062$. De façon générale, pour calculer l'opposé d'un nombre, il suffit de remplacer chaque chiffre (non nul) par son complément à 10.

Passons maintenant à la multiplication. Il n'y a pas de mystère : on fait la multiplication comme au primaire mais sans poser aucune retenue à nouveau. Pour multiplier 17 par 25, on écrit :

$$\begin{array}{rcccc} & & & 1 & 7 \\ & & \times & 2 & 5 \\ \hline & & & 5 & 5 \\ & + & 2 & 4 & \\ \hline & & 2 & 9 & 5 \end{array}$$

et le résultat est donc 295. Là encore, on n'est pas obligé de commencer la multiplication par la droite et de fait, il n'y a aucun problème lorsque l'on veut multiplier des nombres ayant une infinité de chiffres après la virgule. Pour illustrer cela, commençons la multiplication de π par lui-même :

$$\begin{array}{rcccccccccc} & 3, & 1 & 4 & 1 & 5 & \dots & & & & \\ \times & 3, & 1 & 4 & 1 & 5 & \dots & & & & \\ \hline & 9 & 3 & 2 & 3 & 5 & \dots & & & & \\ + & & 3 & 1 & 4 & 1 & 5 & \dots & & & \\ + & & & 2 & 4 & 6 & 4 & 0 & \dots & & \\ + & & & & 3 & 1 & 4 & 1 & 5 & \dots & \\ + & & & & & 5 & 5 & 0 & 5 & 5 & \dots \\ & & & \vdots & & & \vdots & & & & \\ \hline & 9, & 6 & 4 & 4 & 8 & \dots & & & & \end{array}$$

Ainsi le résultat commence par $9,6448$ et on est sûr de ces chiffres. Pour pouvoir accéder aux suivants, il aurait fallu prendre plus de chiffres dans le multiplicande et le multiplicateur lorsque l'on a posé la multiplication.

La division par contre pose problème. Pour exemple, il suffit d'essayer de chercher l'inverse de 2. Il devrait être un nombre qui multiplié par 2 fasse 1. Mais en posant la multiplication :

$$\begin{array}{rccccccc} & a_n & \dots & a_1 & a_0\,, & a_{-1} & a_{-2} & \dots \\ \times & & & & 2 & & & \\ \hline & 2a_n & \dots & 2a_1 & 2a_0\,, & 2a_{-1} & 2a_{-2} & \dots \end{array}$$

on voit que les chiffres du résultat sont tous pairs (car le dernier chiffre d'un nombre pair est toujours pair) et donc que l'on ne pourra jamais obtenir 1.

En analysant un peu mieux cet exemple, on voit que l'inverse d'un nombre dont le seul chiffre non nul est celui des unités, doit également être un nombre avec un seul chiffre non nul en position des unités. En particulier, il faut donc, pour que l'objet que l'on souhaite construire soit un corps, que l'ensemble des chiffres soit lui-même muni d'une structure de corps.

C'est donc ce que nous allons étudier par la suite : nous allons essayer de trouver des ensembles finis munis d'une structure de corps. Ces ensembles seront les ensembles de chiffres et on s'intéressera ensuite aux nombres que l'on peut écrire avec ces chiffres.

2 Les chiffres

2.1 Premiers exemples

Comme nous venons de le dire, notre but, ici, est de déterminer des corps qui n'ont qu'un nombre fini d'éléments. Nous notons N le cardinal de notre corps et allons donc essayer de définir des opérations d'addition et de multiplication sur les ensembles $\{0, 1, \ldots, N-1\}$, le 0 et le 1 désigneront comme à l'habitude les éléments neutres respectifs de l'addition et de la multiplication.

Le cas N = 2

Pour ce cas, les tables d'addition et de multiplication sont presque directement imposées. Déjà, il faut que l'on ait :

$+$	**0**	**1**
0	0	1
1	1	

$\times$	**0**	**1**
0	0	0
1	0	1

Il ne reste plus qu'à décider d'une valeur pour $1+1$. Pour cela, nous allons faire une remarque très générale et très importante : si $x+y = x+z$ alors $y+z$, ce que l'on obtient simplement en retranchant x de chaque côté. Cela signifie qu'il ne peut pas apparaître deux fois le même chiffre sur une même ligne ou une même colonne (de la table d'addition).

Ici, on a déjà un 1 sur la deuxième ligne du tableau d'addition, il ne peut donc plus y en avoir. C'est donc que $1+1=0$ et finalement que les tables sont les suivantes :

$+$	**0**	**1**
0	0	1
1	1	0

$\times$	**0**	**1**
0	0	0
1	0	1

Il reste ensuite à vérifier que ceci satisfait bien tous les axiomes donnés au début de l'article. C'est en général un peu pénible et laborieux, mais ça se fait évidemment sans difficulté. La commutativité par exemple est facile à vérifier : il s'agit de voir que les tableaux sont symétriques par rapport à la diagonale principale. Pour l'existence de l'inverse et de l'opposé, il s'agit de vérifier qu'un 0 apparaît sur chaque ligne de la table d'addition et qu'un 1 apparaît sur chaque ligne de la table de multiplication. Mais pour l'associativité et la distributivité, il n'y a pas de façon très claire de s'en sortir : il faut en fait tester tous les cas un par un à la main.

Nous n'allons pas le faire ici, mais les tables que nous avons écrites juste au dessus correspondent bien à des opérations qui définissent une structure de corps sur l'ensemble $\{0, 1\}$. On a donc construit un corps à 2 éléments.

Le cas N = 3

On considère à présent l'ensemble $\{0, 1, 2\}$ et on essaie comme précédemment de définir des lois d'addition et de multiplication sur cet ensemble. Comme précédemment, on a les contraintes évidentes :

$+$	**0**	**1**	**2**
0	0	1	2
1	1		
2	2		

$\times$	**0**	**1**	**2**
0	0	0	0
1	0	1	2
2	0	2	

On commence par finir de remplir la table de multiplication. Pour cela, on fait la même remarque que pour la table d'addition dans le cas $N = 2$: si $xy = xz$ et $x \neq 0$, alors $y = z$, encore simplement en divisant par x des deux côtés. Ainsi comme pour l'addition, il ne peut pas y avoir deux fois le même chiffre sur une ligne dans le tableau de multiplication sauf évidemment dans le cas où cette ligne correspond à la multiplication par 0. On en déduit donc que forcément $2 \times 2 = 1$.

Il reste à déterminer la valeur de $1 + 1$. C'est soit 2 soit 0. Supposons que ce soit 0. Comme il nous faut trois chiffres distincts sur la ligne d'addition par 1, on aurait forcément $1+2 = 2$, mais il aurait alors deux 2 sur la colonne d'addition par 2, ce qui n'est pas possible. Donc on a obligatoirement $1 + 1 = 2$, et on peut alors finir facilement de compléter les tableaux :

+	**0**	**1**	**2**
0	0	1	2
1	1	2	0
2	2	0	1

×	**0**	**1**	**2**
0	0	0	0
1	0	1	2
2	0	2	1

On vérifie ensuite que ces tables sont bien solution du problème et que l'on a ainsi construit un corps à 3 éléments.

Le cas N = 4

Comme d'habitude, on commence par compléter les chiffres obligés :

+	**0**	**1**	**2**	**3**
0	0	1	2	3
1	1			
2	2			
3	3			

×	**0**	**1**	**2**	**3**
0	0	0	0	0
1	0	1	2	3
2	0	2		
3	0	3		

Finir de remplir la table de multiplication se fait comme pour la table d'addition dans le cas $N = 3$: 2×2 ne peut pas faire 1 car sinon il y aurait deux fois le chiffre 3 dans la dernière colonne. Ainsi on a $2 \times 2 = 3$ et le reste s'en déduit.

Il faut maintenant déterminer la valeur de $s = 1+1$. C'est soit 0, soit 2, soit 3. Et dans chacun des cas, on peut compléter de façon unique la deuxième ligne du tableau, obtenant respectivement :

+	**0**	**1**	**2**	**3**
1	1	0	3	2

+	**0**	**1**	**2**	**3**
1	1	2	3	0

+	**0**	**1**	**2**	**3**
1	1	3	0	2

On remarque que dans tous les cas on a $1 + 1 + 1 + 1 = 0$. Ce que l'on peut encore réécrire $(1 + 1) \times (1 + 1) = 0$, soit $s^2 = 0$. Et cela implique évidemment que $s = 0$ puisque, si ce n'était pas le cas, on pourrait diviser par s des deux côtés et on obtiendrait $s = 0$.

En définitive, on a prouvé que $1+1 = 0$ et donc on peut compléter nos tables. Il est plus simple pour cela de remarquer une dernière chose : si $1 + 1 = 0$, alors pour tout nombre x, on doit avoir $x + x = x\,(1 + 1) = 0$. Il ne reste alors plus qu'une possibilité :

+	**0**	**1**	**2**	**3**
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

×	**0**	**1**	**2**	**3**
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

Il ne reste plus que la vérification pénible à faire... ce que l'on laisse une fois de plus au lecteur.

Le cas N = 5

Pour le coup, et comme il commence à y avoir beaucoup de chiffres, tentons de faire un raisonnement qui pourra même être réutilisé par la suite. Comme on l'a déjà vu sur les exemples précédents, une question importante à se poser est « que vaut $1+1$? ». En fait, il n'y a que deux possibilités, c'est soit 0, soit 2, 3 ou 4, les trois derniers résultats étant totalement équivalents pour l'instant...

Définissons une suite. On pose $s_1 = 1$, $s_2 = 1+1$, $s_3 = 1+1+1$, et de façon générale $s_n = 1 + \ldots + 1$ (n fois). Comme l'ensemble des nombres est fini (ici en l'occurrence de cardinal 5), il existe des indices n et m distincts tels que $s_n = s_m$. Mais si par exemple $m < n$, on peut simplifier m fois par 1 et de l'égalité précédente résulte $s_{n-m} = 0$. Ainsi il existe forcément un entier $p > 0$ tel que $s_p = 0$. Regardons le plus petit d'entre eux et appelons-le p.

Ce nombre p s'appelle la *caractéristique* du corps. Il sera très important par la suite.

Essayons de la déterminer ici. Dans notre corps, on a les éléments :

$$s_0 \quad ; \quad s_1 \quad ; \quad \ldots \quad ; \quad s_{p-1}$$

ce qui en fait p. Ces nombres sont deux à deux distincts évidemment car si $s_i = s_j$ on aurait $s_{|i-j|} = 0$ et bien sûr $|i-j| < p$. Parmi les nombres écrits, soit on a tous les nombres, soit il en manque encore. S'il en manque, c'est qu'il existe un nombre x qui n'est pas l'un d'entre eux et dans le corps, il y a encore tous les éléments :

$$x + s_0 \quad ; \quad x + s_1 \quad ; \quad \ldots \quad ; \quad x + s_{p-1}$$

Tous ces nombres sont deux à deux distincts. En effet, s'il existait i et j tels que $x + s_i = x + s_j$, on aurait $s_i = s_j$, ce que l'on a déjà prouvé comme étant impossible. De plus, ces nombres sont également différents des premiers écrits, car si on avait $x + s_i = s_j$, on aurait $x = s_i - s_j$ mais il est facile de voir que $s_i - s_j$ est toujours l'un des s_k, ce qui est incompatible avec le fait que x soit choisi comme n'étant pas un des s_k. Ainsi avons-nous trouvé $2p$ éléments dans le corps.

Là encore, soit on les a tous, soit il nous en manque à nouveau. S'il en manque, on considère un nouvel y qui n'est aucun des nombres écrits précédemment et par le fait, on a tous les nombres :

$$y + s_0 \quad ; \quad y + s_1 \quad ; \quad \ldots \quad ; \quad y + s_{p-1}$$

Exactement comme avant, on prouve que ces nombres sont deux à deux distincts et également qu'ils sont distincts des précédents nombres écrits. On a donc trouvé $3p$ nombres. Soit on les a tous, soit il en manque encore. S'il en manque, on prend un z encore nouveau et on considère les éléments :

$$z + s_0 \quad ; \quad z + s_1 \quad ; \quad \ldots \quad ; \quad z + s_{p-1}$$

et ainsi de suite[3]...

[3] N'allons pas trop loin pour ne pas épuiser les lettres dans l'alphabet.

Cela prouve que la caractéristique d'un corps fini est toujours un diviseur du cardinal dudit corps. Ici, la caractéristique est forcément 5 puisque c'est le seul diviseur de N strictement plus grand que 1.

En particulier, on ne peut pas avoir $1+1=0$. On pose donc tout naturellement $1+1=2$ puis $1+2=3$ par exemple. On a en fait le choix entre 3 et 4, choix totalement équivalents, restons donc dans la simplicité. La somme $1+3$ vaut alors forcément 4 et finalement on a $1+4=0$.

Avec tout cela, il n'y a plus qu'une seule possibilité pour remplir. En effet si on a des nombres x et y, on peut toujours avec les conventions précédentes écrire $x=1+\ldots+1$ (x fois) et $y=1+\ldots+1$ (y fois). Ainsi $x+y$ vaut s_{x+y} et le produit xy vaut s_{xy} comme on le voit en développant.

Ainsi nos tables sont les suivantes :

$+$	**0**	**1**	**2**	**3**	**4**
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\times$	**0**	**1**	**2**	**3**	**4**
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Si on ne l'a pas encore remarqué, il s'agit simplement de l'addition et de la multiplication modulo 5. Il reste encore à vérifier que ces lois définissent bien un corps, mais comme nous ne l'avons encore jamais fait jusqu'à présent, nous n'allons pas commencer maintenant.

Le cas N premier

Oui, avant de passer à $N=6$, il faut noter que la démarche précédente se généralise directement au cas où N est premier. On note de même p la caractéristique d'un corps fini à N éléments. C'est forcément un diviseur strictement supérieur à 1 de N, et donc comme N est premier, on a $p=N$.

On voit ensuite que quitte à renuméroter les éléments du corps, on peut poser $1+1=2$, $1+2=3$, et ce jusqu'à $1+(p-2)=p-1$ et puis finalement $1+(p-1)=0$. De même encore, ces simples remarques suffisent à impliquer que partout l'addition et la multiplication sont forcément l'addition et la multiplication modulo p (*i.e.* pour additionner ou multiplier deux nombres, on les additionne ou les multiplie classiquement, mais on ne donne au final que le reste de la division euclidienne du résultat par p qui est bien un nombre de notre corps).

Ainsi, on vient que prouver, que quitte à renuméroter les éléments, il ne peut exister au plus qu'un corps fini de cardinal N si N est un nombre premier.

Nous allons voir maintenant en fait que ce corps existe bien, c'est-à-dire que les tables d'addition et de multiplication que l'on vient de décrire vérifient les axiomes listés au tout début de ce texte.

L'associativité et la commutativité de l'addition et de la multiplication sont immédiates. Il en est d'ailleurs de même de la distributivité. Voir que tout nombre admet un opposé est également simple : l'opposé de l'entier x compris entre 0 et $p-1$ est $p-x$, puisque modulo p, on a bien $x+(p-x)=0$.

Le seul point délicat en fait est l'existence de l'inverse. Soit x un entier compris entre 1 et $p-1$, montrons qu'il existe un entier y tel que $xy=1$ modulo p. Et pour cela, on

utilise le théorème de Bézout qui stipule que si a et b sont des entiers premiers entre eux, alors on peut trouver des entiers u et v tels que :

$$au + bv = 1$$

Les entiers x et p sont premiers entre eux, puisque p est premier et d'après l'encadrement fait, x n'est pas divisible par p. On peut donc trouver des entiers u et v tels que $xu+pv = 1$. On appelle alors y le reste de la division euclidienne de u par p et on vérifie alors très facilement que modulo p, on a $xy = 1$. Cela conclut la preuve.

En résumé, si $N = p$ est un nombre premier, à renumérotation près des nombres, il existe un unique corps de cardinal N. On le note $\mathbb{F}_p$.

Le cas N = 6

Le nombre 6 n'est hélas pas premier. Il va donc falloir refaire l'étude ici. Mais encore une fois, plutôt que d'essayer de remplir à tatons des tableaux, essayons de raisonner de façon un peu plus générale et conceptuelle.

Introduisons une fois de plus la caractéristique et appelons-la p comme à l'habitude. Elle doit diviser 6, donc elle ne peut valoir que 2, 3 ou 6.

Déjà dans un premier temps, on peut éliminer 6 car sinon on aurait en développant :

$$(1+1)(1+1+1) = 1+1+1+1+1+1 = 0$$

et on reconnaît un produit de deux termes non nuls qui est nul, ce qui n'est pas possible dans un corps (en effet, si $xy = 0$ et si $x \neq 0$, on peut diviser par x pour obtenir $y = 0$). On a donc abouti à une absurdité et la caractéristique est forcément 2 ou 3.

Supposons maintenant que ce soit 2. Et reprenons la démonstration faite dans le cas $N = 5$ en essayant d'être un peu plus précis. Si la caractéristique est 2, le corps contient au moins les éléments :

$$0 \quad ; \quad 1$$

Évidemment comme ici, il a 6 éléments, ce n'est pas tout et donc il y a un autre nombre x dans notre corps. Mais alors on a les quatre éléments :

$$0 \quad ; \quad 1 \quad ; \quad x \quad ; \quad x+1$$

qui sont deux à deux distincts. Là encore ce n'est pas tout, il y a un nouvel élément y. Mais avec cet y, on peut construire huit éléments dans notre corps qui sont :

$$0 \quad ; \quad 1 \quad ; \quad x \quad ; \quad x+1 \quad ; \quad y \quad ; \quad y+1 \quad ; \quad x+y \quad ; \quad x+y+1$$

et qui sont bien deux à deux distincts. Par exemple, si $x + y$ était égal à 0, cela voudrait dire que $y = -x$ puis $y = x$ puisque $x = -x$. Comme cela est supposé faux, on a bien $x + y \neq 0$. De même, on prouve que tous les éléments sont bien différents. Mais cela fait huit éléments dans notre corps, et on n'en a que six par hypothèse. La caractéristique ne peut donc pas être 2.

Essayons de voir si elle peut être 3. Dans ce cas, on aurait dans un premier temps les éléments :

$$0 \quad ; \quad 1 \quad ; \quad 2$$

où par définition $2 = 1 + 1$. Il y aurait alors un autre nombre x qui donnerait naissance à tous les éléments suivants :

$$0 \quad ; \quad 1 \quad ; \quad 2 \quad ; \quad x \quad ; \quad x+1 \quad ; \quad x+2 \quad ; \quad 2x \quad ; \quad 2x+1 \quad ; \quad 2x+2$$

ce qui en fait neuf. On vérifie une fois de plus qu'ils sont deux à deux distincts. Le cas le plus délicat est de prouver que par exemple $2x + 2 \neq 0$. S'il y avait égalité, on aurait $2x = -2 = 1$ et il faut alors penser à multiplier par l'inverse de 2 dans le corps qui est 2 puisque $2 \times 2 = (1 + 1) \times (1 + 1) = 1 + 1 + 1 + 1 = 1$. On obtient alors $x = 2$, ce qui n'est pas possible.

Tout cela prouve donc qu'un corps à 6 éléments ne peut exister. Il était donc bien inutile de commencer à remplir plein de tables...

Leçons à tirer des exemples

Il faut principalement retenir que la notion de caractéristique est importante et même cruciale. On a vu que si N est un entier, la caractéristique d'un corps à N éléments est un diviseur de N. En fait, on a bien mieux : les démonstrations faites dans le cas $N = 6$ s'adaptent presque directement pour prouver que la caractérisque d'un corps est toujours un nombre premier et le cardinal du corps est toujours une puissance de la caractéristique.

En particulier, le cardinal d'un corps fini est toujours une puissance d'un nombre premier. Ainsi, il n'existe pas de corps de cardinal 10 ou de cardinal 12 281 047 simplement parce que la décomposition en facteurs premiers de ce nombre est $743 \times 16\,529$.

Reste donc maintenant à se poser la question pour les puissances de nombres premiers. C'est l'objet de toute la suite du chapitre.

2.2 Rajouter des racines carrées

Avant de continuer, fixons une notation. Appelons $\mathbb{F}_q$ un corps fini à q éléments. D'après ce qui précède, pour que cette notation prenne sens, il faut au moins que q soit une puissance d'un nombre premier.

Regardons le cas $N = 9$ et essayons donc de construire $\mathbb{F}_9$. Une idée consisterait à rajouter au corps fini $\mathbb{F}_3$ éléments que l'on a déjà construit une racine carrée d'un nombre qui n'en aurait pas, un peu comme l'on passe de $\mathbb{R}$ à $\mathbb{C}$. On obtiendrait ainsi probablement une structure de corps sur les couples d'éléments de $\mathbb{F}_3$ ce qui fournirait bien un ensemble de cardinal 9.

On remarque, d'après la table de multiplication que l'on a dressée, que dans $\mathbb{F}_3$, le nombre $2 = -1$ n'est pas un carré. On aimerait donc lui rajouter une racine carrée que l'on va traditionnellement noter i. On regarde donc l'ensemble de $x + iy$ pour x et y variant dans $\mathbb{F}_3$. Il est facile à décrire, c'est simplement :

$$\mathbb{F}_9 = \{0, 1, 2, i, i + 1, i + 2, 2i, 2i + 1, 2i + 2\}$$

Il est bien de cardinal 9. Il ne faut pas croire que la mystérieuse lettre i renferme un secret inavouable, il s'agit au contraire simplement d'une notation pratique : fondamentalement, les éléments de $\mathbb{F}_9$ sont simplement des couples (x, y), mais que l'on préfère noter $x + iy$ car la description des opérations sera alors plus intuitive.

Effectivement, il est possible de définir une addition et une multiplication sur $\mathbb{F}_9$, *via* les formules :

$$\begin{aligned}(x+iy)+\left(x'+iy'\right) &= \left(x+x'\right)+i\left(y+y'\right)\\ (x+iy)\left(x'+iy'\right) &= \left(xx'-yy'\right)+i\left(x'y+xy'\right)\end{aligned}$$

où les opérations sur les x, y, x' et y' se font dans le corps fini $\mathbb{F}_3$. On reconnaît les mêmes formules que pour les nombres complexes.

La commutativité, l'associativité et la distributivité résultent des propriétés analogues sur le corps $\mathbb{F}_3$ comme on le vérifie directement. L'opposé de $(x+iy)$ est évidemment $(-x-iy)$ et le calcul de l'inverse se fait en utilisant l'astuce de la quantité conjuguée :

$$\frac{1}{x+iy}=\frac{x-iy}{(x-iy)(x+iy)}=\frac{x-iy}{x^2+y^2}=\frac{x}{x^2+y^2}-\frac{y}{x^2+y^2}i$$

Il faut voir que x^2+y^2 n'est jamais nul et évidemment cela ne résulte pas ici de considérations de positivité puisque cela n'a aucun sens de dire qu'un élément de $\mathbb{F}_3$ est positif ou négatif. Toutefois, si on avait $x^2+y^2=0$ avec disons $y\neq 0$, on aurait $\left(\frac{x}{y}\right)^2=-1$, ce qui est impossible puisque (-1) n'est pas un carré dans $\mathbb{F}_3$. C'est donc que $y=0$ puis que $x^2=0$ qui donne $x=0$. Ainsi le seul élément non inversible est 0 comme on pouvait s'y attendre.

On a donc bien construit un corps à 9 éléments, et donc il en existe.

La construction précédente s'étend *illico* à une situation beaucoup plus générale. Supposons donné un corps fini à q éléments, donc $\mathbb{F}_q$. Supposons donné également un élément $a\in\mathbb{F}_q$ qui n'est le carré d'aucun élément de $\mathbb{F}_q$. On veut alors ajouter une racine carrée de a que l'on va noter sans surprise $\sqrt{a}$. Pour cela, on considère l'ensemble produit cartésien $\mathbb{F}_q\times\mathbb{F}_q$ qui est de cardinal q^2. Un élément de ce produit est un couple (x,y) que l'on préfère noter $x+y\sqrt{a}$ par la suite. On définit alors sur cet ensemble une addition et une multiplication *via* les formules naturelles :

$$\begin{aligned}\left(x+y\sqrt{a}\right)+\left(x'+y'\sqrt{a}\right) &= \left(x+x'\right)+\left(y+y'\right)\sqrt{a}\\ \left(x+y\sqrt{a}\right)\left(x'+y'\sqrt{a}\right) &= \left(xx'+ayy'\right)+\left(x'y+xy'\right)\sqrt{a}\end{aligned}$$

Encore une fois, les propriétés de commutativité, d'associativité, de distributivité et d'existence d'un opposé sont conséquences immédiates des propriétés équivalentes sur les éléments de $\mathbb{F}_q$. Encore une fois, pour l'existence de l'inverse, on utilise la quantité conjuguée :

$$\frac{1}{x+y\sqrt{a}}=\frac{x-y\sqrt{a}}{(x-y\sqrt{a})(x+y\sqrt{a})}=\frac{x-y\sqrt{a}}{x^2-ay^2}=\frac{x}{x^2-ay^2}-\frac{y}{x^2-ay^2}\sqrt{a}$$

et il faut voir cette fois-ci que x^2-ay^2 ne peut être nul que si $x=y=0$. Supposons donc que $x^2-ay^2=0$ et par exemple que $y\neq 0$. On peut alors diviser par y^2 pour obtenir $\left(\frac{x}{y}\right)^2=a$, ce qui est impossible par hypothèse. Ainsi $y=0$ et directement $x=0$, ce qui est bien ce que l'on voulait.

Résumons : si on sait construire un corps fini à q éléments dans lequel il existe un élément a qui n'a pas de racine carrée, alors on sait, par la méthode que l'on vient de voir, construire un corps fini à q^2 éléments.

Or dans un corps on a toujours $(-1)^2 = 1^2 = 1$ et donc si $-1 \neq 1$, c'est-à-dire si le corps n'est pas de caractéristique 2, on en déduit que l'application $x \mapsto x^2$ prend deux fois la même valeur et donc ne peut pas atteindre tous les éléments du corps. Cette remarque suffit donc à prouver l'existence de corps finis à p^2, p^4, p^8, p^{16}, etc. éléments si p est un nombre premier impair.

2.3 De l'importance des polynômes irréductibles

Nous avons jusqu'à présent rajouté des racines carrées, mais ne serait-il pas possible également de rajouter des racines cubiques ou des racines quatrièmes, voire même sans pitié des racines cinquièmes ? Supposons donc que a soit un élément d'un certain $\mathbb{F}_q$ qui n'admet pas de racine cubique disons. On aimerait adjoindre à cet $\mathbb{F}_q$ un nouvel élément que l'on notera $\sqrt[3]{a}$ pour faire un corps plus gros. Seulement comme précédemment si on ajoute $\sqrt[3]{a}$, il faudra rajouter tous les $x + y\sqrt[3]{a}$, x et y parcourant $\mathbb{F}_q$, comme on l'avait fait avant... mais il faudra aussi rajouter $\sqrt[3]{a} \times \sqrt[3]{a} = \sqrt[3]{a^2}$.

On considère alors non plus les couples d'éléments mais plutôt les triplets, le triplet (x, y, z) correspond à $x + y\sqrt[3]{a} + z\sqrt[3]{a^2}$. On définit encore une fois l'addition et la multiplication comme on le pense. Et on vérifie les axiomes qu'il faut vérifier, la difficulté revenant encore principalement à l'expression de l'inverse d'un nombre.

Mais voyons directement un cas plus général. On se donne $\mathbb{F}_q$ un corps fini à q éléments et un polynôme P à coefficients dans $\mathbb{F}_q$ de degré n et irréductible. On écrit :

$$P(X) = a_n X^n + a_{n-1} X^{n-1} + \ldots + a_0$$

le fait que P soit *irréductible* signifie que l'on ne peut pas écrire P comme produit de deux polynômes de degré supérieur ou égal à 1. En particulier P n'a pas de racine, car s'il avait une racine x il serait divisible par $(X - x)$. Jusqu'à la fin de cet exposé, même si on oublie de le préciser, tous les polynômes irréductibles seront supposés *unitaires*, c'est-à-dire de coefficient dominant égal à 1. En particulier, ici, $a_n = 1$.

Ce que l'on veut, c'est ajouter à $\mathbb{F}_q$ une racine, disons x, de ce polynôme P. On considère pour cela l'ensemble $\mathbb{F}_q^n$ des n-uplets formés d'éléments de $\mathbb{F}_q$, un tel n-uplet $(x_0, \ldots, x_{n-1})$ représentant le nombre que l'on aimerait écrire $x_0 + x_1 x + \ldots + x_{n-1} x^{n-1}$. On voit alors comment additionner et multiplier ces n-uplets : on fait l'addition ou la multiplication en développant et en regroupant, et si l'on obtient des termes en x^i avec $i \geqslant n$, on les remplace en tenant compte de l'égalité :

$$P(x) = x^n + a_{n-1} x^{n-1} + \ldots + a_0 = 0$$

Ainsi on remplace selon les égalités suivantes :

$$\begin{aligned} x^n &= -a_{n-1} x^{n-1} - a_{n-2} x^{n-2} - \ldots - a_0 \\ x^{n+1} &= -a_{n-1} x^n - a_{n-2} x^{n-1} - \ldots - a_0 x \\ &= -a_{n-1} \left(-a_{n-1} x^{n-1} - a_{n-2} x^{n-2} - \ldots - a_0\right) - a_{n-2} x^{n-1} - \ldots - a_0 x \end{aligned}$$

et ainsi de suite.

Plus prosaïquement, on peut dire que les éléments de notre nouveau corps sont les $A(x)$ où A est un polynôme de degré strictement inférieur à n et que pour additionner

ou multiplier ces polynômes, on les additionne et les multiplie comme on sait le faire puis on prend le reste de la division euclidienne du résultat obtenu par le polynôme P. Cette dernière étape permet de tenir compte du fait que $P(x) = 0$ comme on veut l'imposer. On remarque en particulier que si le polynôme $P(X)$ est $X^2 - a$ on retrouve bien les constructions faites dans le paragraphe précédent. Tout ceci est bien rassurant.

Là encore, la commutativité, l'associativité, la distributivité et l'existence d'un opposé sont des conséquences immédiates des propriétés analogues sur le corps $\mathbb{F}_q$. On veut maintenant calculer l'inverse de l'élément $A(x)$ où A est un certain polynôme non nul à coefficients dans $\mathbb{F}_q$ et de degré strictement inférieur à n. Pour cela, il s'agit de trouver un polynôme B tel que $A(x)B(x) = 1$. Ainsi si formellement on arrive à écrire :

$$A(X)B(X) = 1 + P(X)Q(X)$$

pour certains polynômes B et Q à coefficients dans $\mathbb{F}_q$, l'élément $B(x)$ sera l'inverse recherché. Et ceci est simplement le théorème de Bézout[4] puisque comme P est irréductible, A et P sont premiers entre eux. On construit ainsi un corps à q^n éléments.

On vient donc de prouver qu'étant donné un corps $\mathbb{F}_q$ à q éléments et un polynôme irréductible (unitaire) de degré n à coefficients dans $\mathbb{F}_q$ on est capable de construire un corps de cardinal q^n. Ainsi si l'on arrive à prouver qu'il existe dans $\mathbb{F}_p$ des polynômes irréductibles (unitaires) de tout degré, on aura prouvé qu'il existe au moins un corps de cardinal p^n pour tout entier n et tout nombre premier p. C'est ce que nous allons faire. Mais avant cela, nous aurons besoin de dégager plusieurs propriétés de la table de multiplication d'un corps fini.

2.4 La table de multiplication d'un corps fini

On considère ici un corps fini à q éléments que l'on appelle bien entendu $\mathbb{F}_q$. On note p la caractéristique de $\mathbb{F}_q$. On rappelle que p est un nombre premier et que q est une certaine puissance de p, disons $q = p^n$.

Le premier résultat que nous allons prouver est que pour tout $x \in \mathbb{F}_q$, on a $x^q = x$. Déjà le résultat est trivialement vrai pour $x = 0$. Considérons donc un $x \neq 0$ et regardons la suite des puissances $x, x^2, x^3, \ldots$. Parmi ces nombres forcément deux sont égaux disons $x^i = x^j$ et si l'on a par exemple $j > i$, on aura en simplifiant par x^i, $x^{j-i} = 1$. Ainsi il existe un plus petit entier, disons d tel que $x^d = 1$.

On reprend ensuite les idées d'une démonstration que l'on a déjà faite plusieurs fois. On regarde les éléments :

$$1 \quad ; \quad x \quad ; \quad x^2 \quad ; \quad \ldots \quad ; \quad x^{d-1}$$

Ils sont non nuls, deux à deux distincts et on en a écrit d. Soit ils y sont tous (parmi les non nuls), soit il nous en manque. S'il en manque un, disons y, on regarde les nouveaux éléments :

$$y \quad ; \quad yx \quad ; \quad yx^2 \quad ; \quad \ldots \quad ; \quad yx^{d-1}$$

Ils sont encore non nuls, deux à deux distincts et distincts des premiers. On a donc ainsi trouvé $2d$ éléments. Soit on les a tous (parmi les non nuls), soit il nous en manque. Et s'il

[4] Le théorème de Bézout est également vrai pour les polynômes dont les coefficients sont pris dans un corps quelconque.

nous en manque, on fait la même chose avec un nouvel élément z. Et ainsi de suite. Au bout d'un moment, on aura tout épuisé et on aura alors prouvé que d divise $q-1$. Dans tous les cas x^{q-1} est une puissance de $x^d = 1$, il vaut donc 1 lui aussi. En multipliant par x, on déduit $x^q = x$.

Ce simple résultat a des conséquences extraordinaires. Déjà remarquons qu'il généralise de façon remarquable le petit théorème de Fermat. Rappelons que ce dernier dit que $x^p \equiv x \pmod{p}$, et l'on voit si l'on a bien compris le rapport entre $\mathbb{F}_p$ et la congruence modulo p que le petit théorème de Fermat est simplement une reformulation du résultat précédent dans le cas particulier de $\mathbb{F}_p$.

Une première conséquence de ce résultat est la factorisation du polynôme $X^q - X$. En effet, on voit que tous les $x \in \mathbb{F}_q$ sont racines de ce polynôme. On a trouvé q racines d'un polynôme de degré q ; on a donc bien une factorisation complète :

$$X^q - X = \prod_{x \in \mathbb{F}_q} (X - x)$$

En particulier, tout polynôme à coefficients dans $\mathbb{F}_q$ qui divisera $X^q - X$ se factorisera complètement[5] dans $\mathbb{F}_q$. On dit alors qu'il est *scindé*.

Cette dernière chose implique un autre résultat tout aussi important :

Théorème 1. *Il existe un élément $\alpha \in \mathbb{F}_q$ qui est tel que le plus petit entier $n > 1$ pour lequel $\alpha^n = \alpha$ est $n = q$. En particulier, tous les α^i pour $1 \leqslant i \leqslant q-1$ sont distincts et non nuls, et :*

$$\mathbb{F}_q = \left\{0, 1, \alpha, \alpha^2, \ldots, \alpha^{q-2}\right\}$$

Voyons la preuve. Soit d un diviseur de $q-1$. Alors on peut écrire $q - 1 = dd'$ et puis :

$$\frac{X^{q-1} - 1}{X^d - 1} = 1 + X^d + X^{2d} + \ldots + X^{(d'-1)d}$$

et donc $X^d - 1$ est un diviseur de $X^{q-1} - 1$ puis un diviseur de $X^q - X$. En particulier ce polynôme a exactement d racines dans le corps $\mathbb{F}_q$.

Décomposons alors $q-1$ en facteurs premiers : $q - 1 = p_1^{e_1} \ldots p_d^{e_d}$. D'après ce que l'on a dit précédemment, il y a $p_i^{e_i}$ éléments $x \in \mathbb{F}_q$ tels que $x^{p_i^{e_i}} = 1$ et de même il y en a $p_i^{e_i - 1}$ vérifiant $x^{p_i^{e_i-1}} = 1$. En particulier, il y en a au moins un, disons α_i qui est tel que $\alpha_i^{p_i^{e_i}} = 1$ mais $\alpha_i^{p_i^{e_i-1}} \neq 1$. Cela implique que si $\alpha_i^e = 1$, alors e est un multiple de $p_i^{e_i}$, comme on le voit facilement en regardant la suite périodique des puissances successives de α_i.

On note alors $\alpha = \alpha_1 \ldots \alpha_d$. Soit e un entier tel que $\alpha^e = 1$. On a alors $\alpha_1^e \ldots \alpha_d^e = 1$ d'où en élévant cette égalité à la puissance $\frac{q-1}{p_i^{\alpha_i}}$, il vient :

$$\alpha_i^{e\frac{q-1}{p_i^{\alpha_i}}} = 1$$

ce qui prouve que l'exposant $e\frac{q-1}{p_i^{\alpha_i}}$ est un multiple de $p_i^{\alpha_i}$. Les deux nombres $\frac{q-1}{p_i^{\alpha_i}}$ et $p_i^{\alpha_i}$ sont premiers entre eux donc d'après le lemme de Gauss, $p_i^{\alpha_i}$ divise e, et ce pour tout indice i. Finalement e est un multiple du PPCM des $p_i^{\alpha_i}$, c'est-à-dire un multiple de $q-1$. L'élément α que l'on a construit répond donc bien aux exigences du théorème.

[5] C'est-à-dire en produits de facteurs du premier degré.

2.5 Une propriété des polynômes irréductibles

Fixons un nombre premier p et $\mathbb{F}_p$ un corps fini à p éléments. On a vu que pour être assuré de l'existence d'un corps fini à p^n éléments, il nous suffit de construire un polynôme irréductible (unitaire) de degré n à coefficients dans $\mathbb{F}_p$. Ce n'est pas exactement ce que nous allons faire en fait : nous allons simplement prouver qu'il en existe en donnant une approximation de leur nombre.

Soit n un entier et soit $q = p^n$. La remarque essentielle est la factorisation dans $\mathbb{F}_p$ du polynôme $X^q - X$. On a vu, précédemment, que dans $\mathbb{F}_q$ ce polynôme était scindé mais bien sûr il ne pourrait en être de même dans $\mathbb{F}_p$. Cependant on a la chose suivante :

$$X^q - X = \prod \text{polynômes irréductibles (unitaires) de degré } d \text{ divisant } n$$

où chaque polynôme irréductible apparaît une et une seule fois dans le produit et où les polynômes sont supposés irréductibles dans $\mathbb{F}_p$.

Déjà effectivement aucun facteur ne peut apparaître en double, car sinon on aurait des facteurs carrés lorsque l'on décomposerait dans $\mathbb{F}_q$ et on a vu que ce n'était pas le cas. Regardons maintenant P un polynôme irréductible (unitaire) à coefficients dans $\mathbb{F}_p$ et notons d son degré que l'on suppose diviser n. Rajoutons formellement, comme nous l'avons déjà expliqué, une racine x de polynôme P à $\mathbb{F}_p$. On obtient ainsi un corps fini à p^d éléments et donc dans ce corps $x^{p^d} = x$. Cela signifie donc que le polynôme P est un diviseur du polynôme $X^{p^d} - X$ qui est lui même un diviseur de $X^{p^n} - X = X^q - X$ si n est un multiple de d.

On a ainsi prouvé que tout polynôme irréductible (unitaire) de degré divisant n apparait dans la décomposition en facteurs irréductibles de $X^q - X$. Réciproquement, soit P un facteur irréductible (unitaire) de $X^q - X$ et soit d son degré. On veut prouver que d divise n. Regardons à nouveau le corps fini à p^d éléments obtenu à rajoutant à $\mathbb{F}_p$ une racine x du polynôme P. D'après l'étude faite dans le paragraphe précédent, et précisément d'après le théorème 1, il existe dans ce corps un élément α tel que l'on ait exactement l'égalité :

$$\mathbb{F}_{p^d} = \left\{0, 1, \alpha, \alpha^2, \ldots, \alpha^{p^d-2}\right\}$$

L'élément α s'écrit $\alpha = A(x)$ pour un certain polynôme A à coefficients dans $\mathbb{F}_p$, non nul et de degré strictement inférieur à d. D'autre part, si u et v sont des éléments d'un corps de caractéristique p on a la formule :

$$(u+v)^p = u^p + v^p$$

car on constate en développant que tous les autres termes sont multiples de p et donc nuls dans le corps en question. Par récurrence, on obtient directement :

$$(u+v)^{p^i} = u^{p^i} + v^{p^i}$$

pour tout entier i. Dans notre situation, cela nous dit en particulier que $A(x^q) = A(x)^q$. Mais par ailleurs, $x^q = x$ puisque P divise $X^q - X$. Ainsi $A(x^q) = A(x)$. On en déduit que $A(x)^q = A(x)$, soit $\alpha^q = \alpha$. Cela implique donc que $p^d - 1$ divise $q - 1 = p^n - 1$.

Et alors d divise n par un argument relativement simple. Posons la division euclidienne de n par d et écrivons donc $n = ad + b$ avec $0 \leqslant b < d$. On a dans ces conditions :

$$\frac{p^n - 1}{p^d - 1} = p^b \frac{p^{ad} - 1}{p^d - 1} + \frac{p^b - 1}{p^d - 1} = p^b \left(1 + p^d + \ldots + p^{(a-1)d}\right) + \frac{p^b - 1}{p^d - 1}$$

ce qui prouve que $p^d - 1$ divise $p^b - 1$. Mais manifestement $p^b - 1$ est strictement inférieur à $p^d - 1$ et donc la seule possibilité est d'avoir $p^b - 1 = 0$ et donc $b = 0$. Ainsi on a bien prouvé que d divise n.

Finalement, on a démontré que tous les polynômes irréductibles (unitaires) de degré d divisant n apparaissent comme facteur de $X^q - X$, qu'ils n'apparaissent qu'une fois et qu'il n'en apparait pas d'autres. On obtient bien la factorisation annoncée.

De façon plus générale, si $\mathbb{F}_q$ est un corps à q éléments, on sait factoriser le polynôme $X^{q^n} - X$ dans $\mathbb{F}_q$. On aura une formule analogue :

$$X^{q^n} - X = \prod \text{polynômes irréductibles (unitaires) de degré } d \text{ divisant } n$$

où chaque polynôme irréductible apparaît une et une seule fois dans le produit et où les polynômes sont supposés irréductibles dans $\mathbb{F}_q$ cette fois-ci. La démonstration de cette assertion est exactement la même que celle dans le cas de $\mathbb{F}_p$. Remarquez par ailleurs que si l'on fait $n = 1$, on retrouve bien la factorisation complète du polynôme $X^q - X$ dans $\mathbb{F}_q$.

2.6 Décompte des polynômes irréductibles

Appelons $t(n)$ le nombre de polynômes irréductibles (unitaires) de degré n. D'après la formule que l'on a prouvée dans le paragraphe précédent, la comparaison des degrés donne directement :

$$p^n = \sum_{d|n} dt(d)$$

La chose à peine croyable est que cette formule peut s'inverser et donner une expression des $t(n)$. Plus généralement, si f et g sont deux fonctions de $\mathbb{N}^\star$ dans $\mathbb{R}$ définissons la *convolée* de f et de g par :

$$(f * g)(n) = \sum_{dd'=n} f(d)\, g(d')$$

ceci signifiant que la somme est étendue à tous les couples d'entiers (d, d') vérifiant $dd' = n$. De façon équivalente, si l'on préfère, on peut choisir d'étendre la somme à tous les diviseurs d de n, et on somme alors les $f(d)\, g\left(\frac{n}{d}\right)$.

Une fonction intéressante pour cette opération est la fonction e définie par $e(1) = 1$ et $e(n) = 0$ pour tout $n \geqslant 2$. En effet, on vérifie immédiatement qu'elle est telle que $e * f = f$ pour toute fonction f. Deux propriétés bien utiles également sont la commutativité et l'associativité. Plus exactement, pour toutes fonctions f, g et h, on a :

$$\begin{aligned} f * g &= g * f \\ (f * g) * h &= f * (g * h) \end{aligned}$$

Ici, si l'on pose $f(n) = nt(n)$, $g(n) = 1$ et $h(n) = p^n$ pour tout entier n, on a prouvé que $h = f * g$. Et il est possible de construire une fonction μ que l'on appelle la *fonction de Möbius* vérifiant $\mu * g = e$. En convolant notre égalité par μ des deux côtés, on aura alors $f = h * \mu$ et donc une expression de $t(n)$:

$$t(n) = \frac{1}{n} \sum_{d|n} \mu(d)\, p^{n/d}$$

Il reste à définir la fonction de Möbius. Si n est divisible par un carré, on pose $\mu(d) = 0$. Sinon, n s'écrit de façon unique comme le produit $p_1 \dots p_r$ où les p_i sont des nombres premiers deux à deux distincts et on pose $\mu(n) = (-1)^r$. En particulier, on a $\mu(1) = 0$ puisque dans ce cas $r = 0$. Nous laissons au lecteur le soin de faire le calcul et de voir que $\mu * g = e$.

Voyons plutôt ce que cela donne dans notre situation. On a quelque chose du genre :

$$t(n) = \frac{p^n}{n} - \frac{p^{n/d}}{n} - \dots$$

où, ici, d est le plus petit diviseur de n et où donc la somme continue avec les autres diviseurs et avec les signes correspondants. En particulier le nombre de termes que l'on soustrait est majoré, disons par le nombre de diviseurs de n qui est lui-même majoré par $2\sqrt{n}$. D'autre part, chacun de ces termes est plus petit que $\frac{p^{n/2}}{n}$ et donc on aura :

$$|nt(n) - p^n| \leqslant 2\sqrt{np^n}$$

ce qui prouve que $t(n) > 0$ sauf peut-être pour les cas $p = 2$ et $n \leqslant 2$ et $p = 3$ et $n = 1$, cas que l'on vérifie à part à la main.

On note également que cet encadrement donne l'ordre de grandeurs du nombre de polynômes irréductibles (unitaires) de degré n dans $\mathbb{F}_p$: il y en a en gros $\frac{p^n}{n}$. Ou, si l'on préfère, il y en a en moyenne un sur n. Ainsi, pour générer un polynôme irréductible de degré n à coefficients dans $\mathbb{F}_p$, une bonne technique consiste à générer aléatoirement des polynômes de degré n et à tester leur irréductibilité. La propriété précédente dit qu'il faut en moyenne n essais avant d'en trouver un bon, ce qui est tout à fait raisonnable.

3 Grand rassemblement pour les chiffres

3.1 Objectif

Il faut retenir une leçon de ce qui précède qui n'est peut-être pas encore apparue clairement. Il faut comprendre que les corps s'emboîtent les uns dans les autres dans le sens suivant. Soit $q = p^n$ une puissance d'un nombre premier p. Considérons un corps fini $\mathbb{F}_{q^m}$ à $q^m = p^{nm}$ éléments. Alors dans $\mathbb{F}_{q^m}$ le polynôme $X^q - X$ est scindé puisque c'est un diviseur de $X^{q^m} - X$ et l'ensemble de ses racines forment un sous-corps de $\mathbb{F}_{q^m}$ de cardinal q. On voit donc que l'on peut dire que $\mathbb{F}_q$ est inclus dans $\mathbb{F}_{q^m}$.

Cette dernière phrase n'a pas un sens précis car pour l'instant, on appelle $\mathbb{F}_q$ n'importe quel corps fini à q éléments : que peut bien signifier que $\mathbb{F}_q$ est inclus dans $\mathbb{F}_{q^n}$? Nous allons essayer de donner un sens précis à cette affirmation.

L'idée pour cela est de construire un grand corps qui va englober tous les $\mathbb{F}_q$ quand q est une puissance de p. Bien sûr, un tel corps ne pourra pas être fini mais peu importe. Pour arriver à ce corps, l'idée est de partir de $\mathbb{F}_p$ puis d'arriver à $\mathbb{F}_{p^2}$ en ajoutant une racine d'un polynôme irréductible de degré 2, puis d'aller ensuite à $\mathbb{F}_{p^4}$ en ajoutant à nouveau une racine d'un polynôme irréductible de degré 2 à coefficients dans $\mathbb{F}_{p^2}$ et ainsi de suite. Évidemment, il va falloir à un moment prendre en compte les polynômes irréductibles de degré 3 si on veut avoir une chance de trouver $\mathbb{F}_{p^3}$ dans ce corps limite. Nous allons en fait

procéder comme le suggère le schéma suivant :

$$\begin{array}{ccccccccccccc}
 & \mathbb{F}(1) & \subset & \mathbb{F}(2) & \subset & \mathbb{F}(4) & \subset & \ldots & \subset & \mathbb{F}(2^n) & \subset & \ldots \\
\subset & \mathbb{F}(2^\infty) & \subset & \mathbb{F}(2^\infty 3) & \subset & \mathbb{F}\left(2^\infty 3^2\right) & \subset & \ldots & \subset & \mathbb{F}(2^\infty 3^n) & \subset & \ldots \\
\subset & \mathbb{F}(2^\infty 3^\infty) & \subset & \mathbb{F}(2^\infty 3^\infty 5) & \subset & \mathbb{F}\left(2^\infty 3^\infty 5^2\right) & \subset & \ldots & \subset & \mathbb{F}(2^\infty 3^\infty 5^n) & \subset & \ldots \\
 & & & \vdots & & & & \vdots & & & & \\
 & & & & & \subset \bar{\mathbb{F}}_p & & & & & &
\end{array}$$

On part donc de $\mathbb{F}(1) = \mathbb{F}_p$ et on rajoute une racine d'une équation de degré 2. On tombe ainsi sur $\mathbb{F}(2) = \mathbb{F}_{p^2}$. En rajoutant encore une racine d'une équation de degré 2, on va tomber sur $\mathbb{F}(4) = \mathbb{F}_{p^4}$ et ainsi de suite. On construit comme cela une suite de corps $\mathbb{F}(2^n)$ de cardinal p^{2^n} inclus les uns dans les autres et on note $\mathbb{F}(2^\infty)$ la réunion de tous ces corps.

À $\mathbb{F}(2^\infty)$, on ajoute maintenant une racine d'un polynôme irréductible de degré 3 pour obtenir $\mathbb{F}(2^\infty 3)$ puis on continue pour réaliser toute la deuxième ligne du schéma. On ajoute ensuite les racines des polynômes irréductibles de degré 5 puis ainsi de suite pour tous les nombres premiers ℓ.

Les « nombres » qui apparaissent entre parenthèses sont ce que l'on appelle des *entiers surnaturels*. Un entier surnaturel a une définition tout à fait formelle : c'est un produit fini de facteurs de la forme $p_i^{\alpha_i}$ où les p_i sont des nombres premiers et où les α_i sont des entiers ou éventuellement ∞.

Il n'est pas possible en général d'additionner des entiers surnaturels. Mais par contre on peut les multiplier, simplement en ajoutant les exposants des deux facteurs et en convenant que ∞ ajouté à n'importe quoi fait encore ∞. On peut également définir une notion de divisibilité en disant que a est divisible par b si pour tout nombre premier, l'exposant qui affecte ce nombre premier dans a est plus petit que celui qui l'affecte dans b. On peut aussi parler de plus grand commun diviseur ou de plus grand commun multiple en prenant respectivement le min ou le max des exposants. Ainsi, on peut faire un semblant d'arithmétique avec les entiers surnaturels.

On a une série de propriétés intéressantes :

Propriété 1. *Si n est un entier* naturel *qui divise un entier surnaturel s pour lequel on a défini $\mathbb{F}(s)$, alors il y a dans $\mathbb{F}(s)$ un sous-corps fini à $q = p^n$ éléments.*

Soit s un entier surnaturel pour lequel $\mathbb{F}(s)$ est défini et soit $x \in \mathbb{F}(s)$. Alors il existe un entier naturel *n divisant s tel que $x^{p^n} = x$.*

Tout polynôme à coefficients dans $\mathbb{F}_p$ admet une racine dans $\bar{\mathbb{F}}_p$.

Montrons cela rapidement et commençons par la première affirmation. Déjà si $s = 2^n$ où n est un entier ou éventuellement ∞, c'est facile. Les diviseurs entiers de s sont les 2^m pour m entier et $m \leqslant n$. Si n est entier, $\mathbb{F}(2^n)$ contient par construction $\mathbb{F}(2^m)$ pour tout $m \leqslant n$, qui est bien un corps à p^{2^m} éléments. Si $n = \infty$, on dit simplement que $\mathbb{F}(2^\infty)$ est la réunion de $\mathbb{F}\left(2^t\right)$ et donc en particulier contient le sous-corps $\mathbb{F}(2^m)$ qui a p^{2^m} éléments.

Voyons maintenant le cas où $s = 2^\infty 3$. Par définition $\mathbb{F}(2^\infty)$ est la réunion des tous les corps $\mathbb{F}\left(2^t\right)$ et $\mathbb{F}(2^\infty 3)$ s'obtient en rajoutant à $\mathbb{F}(2^\infty)$ une racine d'un polynôme irréductible de degré 3. Ce polynôme est à coefficients dans $\mathbb{F}(2^\infty)$ et comme il n'y a qu'un nombre fini de coefficients, il est en fait à coefficients dans $\mathbb{F}\left(2^t\right)$ pour un t suffisamment grand. Bien entendu, à coefficients dans ce corps plus petit, il reste irréductible. Ainsi, il y

a dans $\mathbb{F}(2^\infty 3)$ des sous-corps à p^{2t3} éléments pour t suffisamment grand. Or dans $\mathbb{F}_{q^n}$, il y a un sous-corps à q éléments, d'où on déduit que dans $\mathbb{F}(2^\infty 3)$, il y aura bien un sous-corps à $\mathbb{F}(2^m 3)$ pour tout m. Ce qui fallait démontrer.

Finalement, le cas général se traite exactement de la même façon. Évidemment, on sait caractériser un sous-corps de $\mathbb{F}(s)$ de cardinal $q = p^n$, ce sera l'ensemble des racines de polynôme $X^q - X$.

Pour la seconde assertion, il s'agit de tenir un raisonnement analogue. Dans un premier temps si $s = 2^\infty$ et si $x \in \mathbb{F}(2^\infty)$, alors x est dans un $\mathbb{F}(2^n)$ pour un certain entier n et donc $x^{2^n} = x$. Maintenant supposons $s = 2^\infty 3$ et soit $x \in \mathbb{F}(2^\infty 3)$. Notons t la racine ajoutée pour passer de $\mathbb{F}(2^\infty)$ à $\mathbb{F}(2^\infty 3)$. L'élément x s'écrit alors $x = a_0 + a_1 t + a_2 t^2$ où les a_i sont éléments de $\mathbb{F}(2^\infty)$. En particulier, il existe un entier n tel que les a_i et les coefficients du polynôme irréductible dont t est racine soient tous dans $\mathbb{F}(2^n)$ et alors x est dans le corps fini où on a ajouté à $\mathbb{F}(2^n)$ l'élément t. Ce corps est de cardinal $q = p^{2^n 3}$, et donc $x^q = x$, ce qui termine la preuve pour $s = 2^\infty 3$. Le cas général est plus pénible mais pas plus compliqué. Il s'agit juste de reprendre les idées précédentes et de les adapter quand il y a un paquet d'extensions.

Le troisième point : soit un polynôme à coefficients dans $\mathbb{F}_p$. Appelons P un facteur irréductible de ce polynôme, disons de degré d. Alors d'après ce qui précède, il y a dans $\bar{\mathbb{F}}_p$ un sous-corps fini à $q = p^d$ éléments. Mais alors P divise $X^q - X$ et $X^q - X$ est scindé dans ce sous-corps fini. Cela implique que P admet une racine dans ce sous-corps fini et donc dans $\bar{\mathbb{F}}_p$, ce qui conclut la preuve.

On vient de donner les conséquences de la construction que l'on propose mais on n'a toujours pas expliqué comment faire cette construction. C'est ce que nous nous proposons d'expliquer maintenant.

3.2 Cas $\ell \neq p$

On se donne un nombre premier ℓ et on note $\ell_1, \ldots, \ell_k$ les nombres premiers rangés par ordre croissant et strictement inférieurs à ℓ. Notons s l'entier surnaturel $\ell_1^\infty \ldots \ell_k^\infty$. On suppose que l'on dispose du corps $\mathbb{F}(s)$ et on veut construire les corps $\mathbb{F}(s\ell^n)$ pour tout entier n.

Le premier cran

L'idée consiste à rajouter une racine ℓ-ième à $\mathbb{F}(s)$ mais pour cela, il faut au moins trouver un élément $a \in \mathbb{F}(s)$ qui n'admet pas de racine ℓ-ième. Et en fait, cela est assez souvent possible. Rappelons que si $\mathbb{K}$ est un corps fini à q éléments, on peut toujours trouver un α tel que :

$$\mathbb{K} = \left\{0, 1, \alpha, \alpha^2, \ldots, \alpha^{q-2}\right\}$$

Avec cette description, on voit que les puissances ℓ-ième sont exactement les α^i où i est tel qu'il existe u et v tels que $u\ell + v(q-1) = i$. Autrement dit, d'après le théorème de Bézout, α^i est une puissance ℓ-ième si et seulement si i est un multiple de $\text{PGCD}(\ell, q-1)$ ce qui revient encore à la condition :

$$\left(\alpha^i\right)^{\frac{q-1}{\text{PGCD}(\ell, q-1)}} = 1$$

dans le corps $\mathbb{K}$, et c'est cette dernière condition que nous allons retenir.

En particulier, on voit que si ℓ n'est pas premier avec $q-1$, il y a dans $\mathbb{K}$ un élément qui n'est pas une puissance ℓ-ième. Tout cela est bien intéressant mais ne s'applique hélas pas à notre situation : nous avons un corps infini $\mathbb{F}(s)$ et on a donc besoin de faire une adaptation. On se rappelle pour cela que si n est un entier naturel divisant s, c'est-à-dire un entier naturel s'écrivant sous la forme $n = \ell_1^{\alpha_1} \dots \ell_k^{\alpha_k}$ pour certains entiers α_i, alors $\mathbb{F}(s)$ admet un sous-corps fini à p^n éléments.

Choisissons donc un tel n et un tel sous-corps fini $\mathbb{K}$. On aimerait pouvoir choisir ce n de façon à ce que $p^n - 1$ soit un multiple de ℓ, car dans ces conditions on serait assuré de l'existence d'un élément $a \in \mathbb{K}$ n'admettant pas de racine ℓ-ième dans $\mathbb{K}$. On voit déjà que si $\ell = p$, cela ne va pas être possible car $p^n - 1$ est toujours premier avec p.

Supposons donc à partir de maintenant que $\ell \neq p$. On voit alors d'après le petit théorème de Fermat qu'il suffit de choisir $n = \ell - 1$ pour que ℓ divise $p^n - 1$ comme on le souhaite. Et c'est tout à fait possible car dans la décomposition en facteurs premiers de $\ell - 1$, il n'apparaît bien évidemment que des nombres premiers strictement inférieurs à ℓ. On choisit donc n ainsi et $\mathbb{K}$ un sous-corps fini de $\mathbb{F}(s)$ à p^n éléments.

En fait, on peut même un peu mieux choisir $\mathbb{K}$ et supposer en outre qu'il contient toutes les racines ℓ-ièmes de l'unité, c'est-à-dire que le polynôme $X^\ell - 1$ se scinde dans $\mathbb{K}$. En effet, on remarque en premier lieu que ce polynôme se factorise sous la forme suivante :

$$X^\ell - 1 = (X-1)\left(X^{\ell-1} + \dots + X + 1\right)$$

et tous les facteurs irréductibles de $X^{\ell-1} + \dots + X + 1$ sont de degré inférieur ou égal à $\ell - 1$ et donc le PPCM de ces degrés, disons m, divise s. D'autre part, d'après ce que l'on sait de la factorisation de $X^{p^m} - X$, on en déduit que $X^\ell - 1$ est un diviseur de $X^{p^m} - X$. Ainsi, si l'on choisit non pas un corps à p^n éléments mais à p^{nm} éléments, ce qui est encore possible car nm divise s, on aura à la fois l'existence d'un $a \in \mathbb{K}$ qui n'est pas une puissance ℓ-ième et le fait que dans $\mathbb{K}$ le polynôme $X^\ell - 1$ est scindé. Choisissons donc le $\mathbb{K}$ ainsi. On n'en changera plus par la suite.

On peut même dire un peu mieux. Choisissons ε une racine ℓ-ième de 1 différente de 1. Alors pour tout entier i, ε^i est encore une racine ℓ-ième de 1. Mais il est impossible qu'il existe $0 \leqslant i < j < \ell$ tel que $\varepsilon^i = \varepsilon^j$ car sinon on aurait $\varepsilon^{j-i} = 1$ mais comme $j - i$ est premier avec ℓ, on en déduirait que $\varepsilon = 1$, ce qui n'est pas. Ainsi on a toutes les racines du polynôme $X^\ell - 1$, ce sont $1, \varepsilon, \varepsilon^2, \dots, \varepsilon^{\ell-1}$ et donc on dispose dans $\mathbb{K}$ de la factorisation :

$$X^\ell - 1 = \prod_{i=0}^{\ell-1} (X - \varepsilon^i)$$

Tout ce qui précède implique que le polynôme $P(X) = X^\ell - a$ est irréductible dans $\mathbb{K}$. En effet, si ce n'était pas le cas, d'après le même argument que précédemment, il serait scindé dans $\mathbb{F}(s)$, et si l'on note $t \in \mathbb{F}(s)$ une racine on aurait la factorisation :

$$X^\ell - a = \prod_{i=0}^{\ell-1} (X - \varepsilon^i t)$$

factorisation qui a lieu dans $\mathbb{F}(s)$.

D'autre part, si P n'est pas irréductible, il aurait un facteur irréductible (unitaire) Q le divisant strictement. Ce facteur serait forcément de la forme :

$$Q(X) = \prod_{i \in I} (X - \varepsilon^i t)$$

où I est un sous-ensemble de $\{0,\ldots,\ell-1\}$. Mais alors les polynômes suivants :

$$Q_j(X) = \prod_{i\in I}\left(X - \varepsilon^{i+j}t\right) = \varepsilon^j Q\left(\frac{X}{\varepsilon^j}\right)$$

seraient encore à coefficients dans $\mathbb{K}$ et encore des diviseurs de P. Ces diviseurs doivent tous être soit égaux à Q, soit premiers avec Q puisque Q est irréductible (unitaire) et que deux facteurs irréductibles (unitaires) sont forcément premiers entre eux. Et on voit que pour cela, la seule solution est de prendre pour I un singleton. Cela signifierait que $t \in \mathbb{K}$, ce que l'on a supposé être faux. Finalement, on trouve bien que P est irréductible dans $\mathbb{K}$.

On peut finalement déduire que l'élément a n'admet pas non plus de racine ℓ-ième dans $\mathbb{F}(s)$. En effet, supposons que ce ne soit pas le cas, et notons t un élément de $\mathbb{F}(s)$ tel que $t^\ell = a$. L'irréductibilité dans $\mathbb{K}$ du polynôme $X^\ell - a$ assure, d'après ce que l'on sait de la factorisation de $X^{q^\ell} - X$, que $X^\ell - a$ est un diviseur de $X^{q^\ell} - X$ et donc que $t^{q^\ell} = t$ où $q = p^{nm}$ désigne le cardinal de $\mathbb{K}$. Mais d'autre part, d'après la deuxième partie de la proposition 1, il existe un entier h divisant s tel que $t^{p^h} = t$. Ainsi si $d = \textsc{Pgcd}\left(q^\ell - 1, p^h - 1\right)$, on a $t^d = 1$. Mais puisque m et ℓ sont premiers entre eux, ce $\textsc{Pgcd}$ divise $q-1$, ce qui prouve que $t^q = t$ et que $t \in \mathbb{K}$ (car on a vu comment se factorisait le polynôme $X^q - X$ dans $\mathbb{K}$ qui a q éléments). Mais on avait supposé que a n'admettait pas de racine ℓ-ième dans $\mathbb{K}$ et donc t ne peut appartenir à $\mathbb{K}$.

On a donc fait le premier cran et on a construit $\mathbb{F}(s\ell)$. Il reste donc à faire les autres.

Les autres crans

Malgré les apparences, la situation se présente légèrement mieux maintenant car on n'a plus besoin de trouver un élément dont on pourrait extraire une racine ℓ-ième, on l'a en fait déjà. On rappelle que pour passer de $\mathbb{F}(s)$ à $\mathbb{F}(s\ell)$, on a rajouté une racine ℓ-ième d'un élément a que l'on va à partir de maintenant noter $\sqrt[\ell]{a}$. Il se trouve que dans de nombreux cas, ce nouvel élément $\sqrt[\ell]{a}$ n'admet pas de racine ℓ-ième dans $\mathbb{F}(s\ell)$. On pourra pour aller à $\mathbb{F}\left(s\ell^2\right)$ rajouter une racine ℓ-ième de $\sqrt[\ell]{a}$ et ainsi de suite pour les suivants.

Le lemme fondamental pour itérer cette construction est le suivant :

Lemme 1. *Soit $\mathbb{K}$ un corps fini de cardinal q une puissance de p. Soit ℓ un nombre premier différent de p. On suppose que le polynôme $X^\ell - 1$ est scindé dans $\mathbb{K}$ et qu'il y a dans $\mathbb{K}$ un élément a qui n'admet pas de racine ℓ-ième. De plus si $\ell = 2$, on suppose que q est un carré.*

On note $\mathbb{K}[\sqrt[\ell]{a}]$ le corps obtenu en rajoutant à $\mathbb{K}$ une racine ℓ-ième de a. Alors dans ce nouveau corps $\sqrt[\ell]{a}$ n'admet pas de racine ℓ-ième.

Faisons la démonstration. D'après l'étude faite pour le premier cran, le polynôme $X^\ell - a$ est irréductible dans $\mathbb{K}$ et donc le corps $\mathbb{K}[\sqrt[\ell]{a}]$ sera de cardinal q^ℓ. Rappelons le critère que l'on avait donné pour savoir si un élément est ou non une puissance ℓ-ième : un élément x dans un corps de cardinal q est une puissance ℓ-ième si et seulement si :

$$x^{\frac{q-1}{\textsc{Pgcd}(\ell,q-1)}} = 1$$

Ainsi ici on sait par hypothèse que :

$$a^{\frac{q-1}{\textsc{Pgcd}(\ell,q-1)}} \neq 1$$

Pour que cette inégalité puisse avoir lieu, il faut impérativement que $\text{PGCD}(\ell, q-1) \neq 1$ et donc que ℓ divise $q-1$ puisque ℓ est premier. On sait donc que $a^{\frac{q-1}{\ell}} \neq 1$ et on veut prouver que $(\sqrt[\ell]{a})^{\frac{q^\ell-1}{\ell}} \neq 1$.

Écrivons pour cela :

$$\frac{q^\ell-1}{\ell} = \frac{q-1}{\ell} \cdot \frac{q^\ell-1}{q-1} = \frac{q-1}{\ell} \cdot \left(1+q+\ldots+q^{\ell-1}\right)$$

On sait que ℓ divise $q-1$ et donc qu'il existe un entier k tel que $q = 1+k\ell$. En élevant à la puissance i par la formule du binôme de Newton, on trouve la congruence $q^i \equiv 1+ik\ell \pmod{\ell^2}$ et puis finalement en faisant la somme :

$$1+q+\ldots+q^{\ell-1} \equiv \ell + \frac{\ell(\ell-1)}{2}k\ell \equiv \ell + \frac{\ell-1}{2}k\ell^2 \pmod{\ell^2}$$

Donc si ℓ est impair (*i.e.* différent de 2), la somme $1+q+\ldots+q^{\ell-1}$ est congrue à ℓ modulo ℓ^2 et donc il existe un autre entier k tel que :

$$\frac{q^\ell-1}{\ell} = \frac{q-1}{\ell} \cdot \left(\ell+k\ell^2\right) = (q-1) + k(q-1)\ell$$

et finalement $(\sqrt[\ell]{a})^{\frac{q^\ell-1}{\ell}} = a^{\frac{q-1}{\ell}}$ qui est bien différent de 1.

Si maintenant $\ell = 2$, on a $p \neq 2$ et donc p et q impairs. En outre, comme q est supposé être un carré, on a forcément $q \equiv 1 \pmod 4$. D'autre part $\frac{q^2-1}{2} = \frac{q-1}{2}(q+1) \equiv q-1 \pmod{2(q+1)}$ et on conclut comme précédemment.

Ceci démontre donc le lemme.

Maintenant il faut expliquer comment cela nous aide dans notre construction. Supposons dans un premier temps $\ell \neq 2$ et notons $\mathbb{K}$ le sous-corps fini de $\mathbb{F}(s)$ considéré précédemment. On avait construit un élément $a \in \mathbb{K}$ qui n'admettait pas de racine ℓ-ième dans $\mathbb{F}(s)$. On vient alors de prouver que $\sqrt[\ell]{a}$ n'admettait pas de racine ℓ-ième dans $\mathbb{K}[\sqrt[\ell]{a}]$ et donc on a construit les corps représentés sur le schéma suivant :

$$\begin{array}{ccccc} \mathbb{K} & \subset & \mathbb{K}[\sqrt[\ell]{a}] & \subset & \mathbb{K}[\sqrt[\ell^2]{a}] \\ \cap & & \cap & & \\ \mathbb{F}(s) & \subset & \mathbb{F}(s)[\sqrt[\ell]{a}] & & \end{array}$$

Si $\mathbb{K}$ a q éléments, alors $\mathbb{K}[\sqrt[\ell]{a}]$ en a q^ℓ et $\mathbb{K}[\sqrt[\ell^2]{a}]$ en a q^{ℓ^2} puisque le polynôme $X^\ell - \sqrt[\ell]{a}$ est irréductible dans $\mathbb{K}[\sqrt[\ell]{a}]$ d'après le même argument que celui qui prouvait que $X^\ell - a$ était irréductible sur $\mathbb{K}$. On veut prouver que $\sqrt[\ell]{a}$ n'a pas de racine ℓ-ième dans $\mathbb{F}(s)[\sqrt[\ell]{a}]$ pour pouvoir continuer la construction. Supposons que ce ne soit pas le cas et appelons t une telle racine. Puisque le polynôme $X^\ell - \sqrt[\ell]{a}$ est irréductible dans $\mathbb{K}[\sqrt[\ell]{a}]$, c'est un diviseur de $X^{q^{\ell^2}} - X$ et donc on a $t^{q^{\ell^2}-1} = 1$. D'autre part, d'après la deuxième affirmation de la proposition 1, il existe un entier m divisant $s\ell$ tel que $t^{p^m-1} = 1$. Du fait que $\text{PGCD}(q^{\ell^2}-1, p^m-1)$ est un diviseur de $q^\ell - 1$, on aboutit à $t^{q^\ell} = t$ puis que $t \in \mathbb{K}[\sqrt[\ell]{a}]$, ce qui est supposé faux.

On obtient ainsi le deuxième cran. En itérant le procédé exactement de la même façon, on construit toute la suite comme on le voulait.

Si $\ell = 2$, c'est encore plus facile puisque l'on n'a pas à manipuler de corps infini. Il peut toutefois y avoir un souci au début puisque l'on n'est pas certain que la racine carrée que l'on rajoute la première fois puisse resservir. Si ce n'est pas le cas, ce n'est pas grave. On choisit simplement un autre élément qui n'a pas de carré : notez que trivialement dans un corps fini de caractéristique différente de 2, il y a toujours un nombre qui n'admet pas de racine carrée, car $1^2 = (-1)^2$ et donc l'application $x \mapsto x^2$ ne peut pas atteindre tous les éléments du corps.

3.3 Cas $\ell = p$

On se plonge maintenant dans le cas $\ell = p$. Comme précédemment on appelle $\ell_1, \ldots, \ell_k$ les nombres premiers strictement inférieurs à ℓ, s l'entier surnaturel $s = \ell_1^\infty \ldots \ell_k^\infty$, et on suppose le corps $\mathbb{F}(s)$ construit. On veut alors construire les suivants, c'est-à-dire les $F(sp^n)$ pour tout n.

La bonne nouvelle, c'est qu'on ne va pas avoir besoin de construire un corps $\mathbb{K}$ comme précédemment. En fait $\mathbb{K} = \mathbb{F}_p = \mathbb{F}(1)$ va convenir. La mauvaise nouvelle, évidemment, c'est que l'on ne va pas pouvoir extraire des racines p-ièmes. Il faut donc trouver un autre polynôme irréductible.

Le premier cran

On part de $\mathbb{F}_p$ et on considère le polynôme $P(X) = X^p - X - 1$. Un fait évident est que P n'a pas de racine dans $\mathbb{F}_p$. En effet, si $x \in \mathbb{F}_p$, on a $x^p = x$ et donc $P(x) = -1 \neq 0$. On a même mieux : le polynôme P est irréductible dans $\mathbb{F}_p$. La preuve ressemble fort à celle fait dans le cas $\ell \neq p$: supposons que ce polynôme ne soit pas irréductible et notons Q un facteur irréductible à coefficients dans $\mathbb{F}_p$. Ajoutons à $\mathbb{F}_p$ une racine t de Q, on obtient ainsi le corps $\mathbb{K}$.

Si $i \in \mathbb{F}_p$, on a $(t+i)^p = t^p + i^p = t^p + i$ et donc $P(t+i) = 0$. On a ainsi trouvé p racines du polynôme P, on les a toutes. Ceci fournit la factorisation de P dans $\mathbb{K}$:

$$P(X) = \prod_{i \in \mathbb{F}_p} (X - t - i)$$

Comme Q est supposé être un facteur de P, il s'écrit sous la forme :

$$Q(X) = \prod_{i \in I} (X - t - i)$$

où I est un certain sous-ensemble de $\mathbb{F}_p$. On regarde alors les polynômes Q_j définis de la façon suivante :

$$Q_j(X) = \prod_{i \in I} (X - t - i - j) = Q(X - j)$$

ils sont encore à coefficients dans $\mathbb{F}_p$ et des diviseurs de P. D'autre part, si j est fixé, comme Q est irréductible, il doit soit être premier avec Q_j soit lui être égal. La seule possibilité pour cela est que I soit de cardinal 1, mais alors on aurait $t \in \mathbb{F}_p$ et ce n'est pas le cas. Donc P est bien irréductible dans $\mathbb{F}_p$.

On rajoute donc à $\mathbb{F}_p$ une racine de P obtenant ainsi un corps de cardinal p^p. Si l'on note t la racine ajoutée, on va avoir $t^{p^p - 1} = 1$. Si t avait le mauvais goût d'être déjà dans $\mathbb{F}(s)$, il existerait un entier m divisant s tel que $t^{p^m - 1} = 1$. Mais m et s seraient premiers entre eux, et donc on aurait $t^{p-1} = 1$, ce qui implique $t^p = t$ et $t \in \mathbb{F}_p$. Et on vient de voir

que cela n'est pas possible. Le polynôme P n'admet donc pas de racine dans $\mathbb{F}(s)$ et la même démonstration que précédemment prouve qu'il est irréductible dans ce corps.

On rajoute alors une racine de ce polynôme irréductible dans $\mathbb{K}(s)$ et on obtient ainsi le corps $\mathbb{K}(sp)$, ce qui termine bien le premier cran.

Le second cran

Pour l'instant on a construit les corps suivants :

$$\begin{array}{ccc} \mathbb{F}_p & \subset & \mathbb{F}_p[t] \\ \cap & & \cap \\ \mathbb{F}(s) & \subset & \mathbb{F}(s)[t] \\ & & = \mathbb{F}(sp) \end{array}$$

où donc t désigne une racine du polynôme $X^p - X - 1$. On va construire un troisième corps sur la ligne du haut et on verra ensuite que, comme toujours, on peut reporter cette même construction sur la ligne du bas.

On cherche donc un polynôme irréductible de degré p à coefficients dans $\mathbb{F}_p[t]$. On le cherche sous la forme $P(X) = X^p - X - a$. Bien entendu, on ne peut plus prendre $a = 1$ puisque l'on a déjà rajouté la racine en question. Il nous faut donc trouver un $a \in \mathbb{F}_p[t]$ tel que le polynôme P n'ait pas de racine dans $\mathbb{F}_p[t]$. Supposons qu'il ait une telle racine, disons t'. On a alors :

$$t'^p = t' + a$$

puis en élevant cette égalité à la puissance p plusieurs fois, on arrive au système :

$$\begin{array}{rcl} t'^p & = & t' + a \\ t'^{p^2} & = & t'^p + a^p \\ t'^{p^3} & = & t'^{p^2} + a^{p^2} \\ & \vdots & \\ t'^{p^p} & = & t'^{p^{p-1}} + a^{p^{p-1}} \end{array}$$

et en additionnant toutes ces égalités, on obtient des simplications et la formule :

$$t'^{p^p} = t'^p + \left(a + a^p + \ldots + a^{p^{p-1}}\right)$$

Ainsi si l'on arrive à trouver a tel que le nombre $a + a^p + \ldots + a^{p^{p-1}}$ soit non nul, on pourrait conclure à une absurdité puisque les éléments $x \in \mathbb{F}_p[t]$ vérifient tous $x^{p^p} = x$.

Il s'agit donc de trouver un élément $a \in \mathbb{F}_p[t]$ tel que $a + a^p + \ldots + a^{p^{p-1}} \neq 0$. On pourrait penser à prendre $a = t$ mais cela ne marche pas. En effet, on a :

$$t + t^p + \ldots + t^{p^{p-1}} = t + (t+1) + (t+2) + \ldots + (t+p-1) = pt + \frac{p(p-1)}{2}$$

et ce nombre est nul dès que p est impair. En fait, on peut considérer $a = t^{p-1}$. Calculons a^{p^i}. Déjà, on a $t^p = t + 1$ et donc en divisant cette égalité par t, on trouve $a = 1 + \frac{1}{t}$. Puis en élévant à la bonne puissance, on trouve :

$$a^{p^i} = 1 + \frac{1}{t^{p^i}} = 1 + \frac{1}{t+i}$$

Mais on a vu que les $t+i$ sont toutes les racines du polynôme $X^p - X - 1$ et donc les $\frac{1}{t+i}$ sont celles du polynôme :

$$X^p \left[\left(\frac{1}{X} \right)^p - \frac{1}{X} - 1 \right] = -X^p - X^{p-1} + 1$$

La somme de ces racines est donnée par la formule habituelle et on trouve ici qu'elle vaut -1. De tout cela, on déduit que :

$$a + a^p + \ldots + a^{p^{p-1}} = -1 \neq 0$$

et donc que a convient bien.

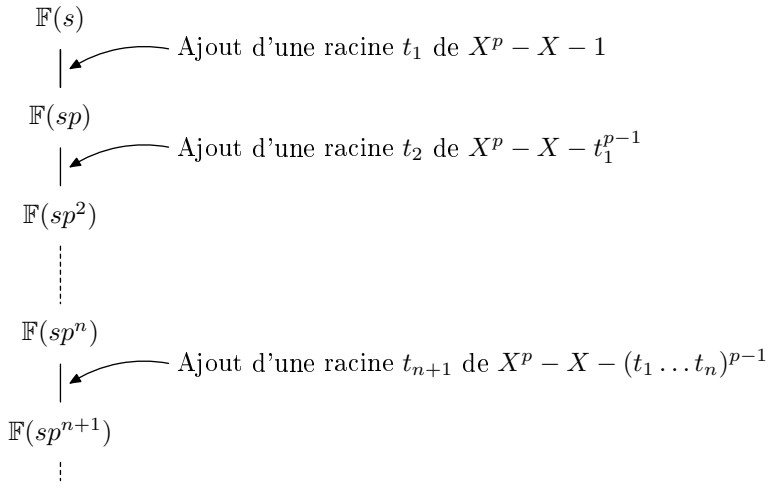
On raisonne maintenant comme pour le premier cran. On prouve dans un premier temps que le polynôme $X^p - X - a$ est irréductible dans $\mathbb{F}_p[t]$, puis dans $\mathbb{F}(sp)$ et on rajoute les racines convenables. On a donc complété notre diagramme :

$$\begin{array}{ccccc} \mathbb{F}_p & \subset & \mathbb{F}_p[t] & \subset & \mathbb{F}_p[t,t'] \\ \cap & & \cap & & \cap \\ \mathbb{F}(s) & \subset & \mathbb{F}(sp) & \subset & \mathbb{F}\left(sp^2\right) \end{array}$$

Les crans suivants

Il s'agit de faire exactement la même manipulation et de construire à chaque fois un nouveau a qui conviendra. Nous allons nous contenter de donner les polynômes qui conviennent successivement, sans prouver qu'ils fonctionnent bien. Il n'y a aucun piège, et rien de plus à comprendre que pour les deux premiers crans, les détails sont juste un peu plus délicats à écrire.

On fait les constructions schématisées sur le dessin suivant :



Pour passer de $\mathbb{F}(s)$ à $\mathbb{F}(sp)$, on ajoute comme on l'a vu t_1 une racine du polynôme $X^p - X - 1$. Ensuite, pour passer à $\mathbb{F}\left(sp^2\right)$, on ajoute t_2 racine de $X^p - X - t_1^{p-1}$. Puis pour passer à $\mathbb{F}\left(sp^3\right)$, on ajoute une racine de $X^p - X - (t_1 t_2)^{p-1}$. De façon générale donc, pour passer de $\mathbb{F}(sp^n)$ à $\mathbb{F}\left(sp^{n+1}\right)$, on ajoute t_{n+1} une racine du polynôme $X^p - X - (t_1 \ldots t_n)^{p-1}$, et on vérifie que ceci fonctionne sans problèmes.

3.4 Conclusion

On a donc finalement réussi la construction que l'on s'était proposé de faire. On a construit une suite de corps inclus les uns dans les autres selon le schéma suivant :

$$\begin{array}{ccccccccccccc}
 & \mathbb{F}(1) & \subset & \mathbb{F}(2) & \subset & \mathbb{F}(4) & \subset & \ldots & \subset & \mathbb{F}(2^n) & \subset & \ldots \\
\subset & \mathbb{F}(2^\infty) & \subset & \mathbb{F}(2^\infty 3) & \subset & \mathbb{F}\left(2^\infty 3^2\right) & \subset & \ldots & \subset & \mathbb{F}(2^\infty 3^n) & \subset & \ldots \\
\subset & \mathbb{F}(2^\infty 3^\infty) & \subset & \mathbb{F}(2^\infty 3^\infty 5) & \subset & \mathbb{F}\left(2^\infty 3^\infty 5^2\right) & \subset & \ldots & \subset & \mathbb{F}(2^\infty 3^\infty 5^n) & \subset & \ldots \\
 & & & \vdots & & & & \vdots & & & & \\
 & & & & & \subset \bar{\mathbb{F}}_p & & & & & &
\end{array}$$

Et la construction, même si elle a pu vous paraître un peu compliquée, n'a pas grand chose de sorcier. On la fait ligne par ligne.

Pour faire la ligne ℓ, si $\ell \neq p$, on commence par chercher un élément qui n'aurait pas de racine ℓ-ième et on lui en extrait une, ce qui donne le corps suivant. Ensuite, on extrait une racine ℓ-ième de celle que l'on vient de rajouter et ainsi de suite, on obtient par ce procédé tous les corps de la ligne. Il faut faire attention au cas $\ell = 2$, où la construction pourrait ne fonctionner qu'à partir du deuxième cran. Les extensions que l'on obtient ici s'appellent des *extensions de Kummer*.

Si $\ell = p$, on n'extrait pas de racine p-ième car cela n'est pas possible, mais on extrait des racines des polynômes explicités précédemment. Les extensions obtenues sont des *extensions d'Artin-Schreier*.

Au final, on obtient un corps regroupant tous les chiffres, corps que l'on appelle $\bar{\mathbb{F}}_p$. On peut montrer que dans ce corps tout polynôme admet une racine. On dit alors que $\bar{\mathbb{F}}_p$ est *algébriquement clos*. On peut même montrer un peu mieux, c'est que tout élément de $\bar{\mathbb{F}}_p$ est racine d'un polynôme à coefficients dans $\mathbb{F}_p$. Autrement dit, en faisant notre construction, on a bien rajouté toutes les racines des polynômes, mais pas plus. Le corps $\bar{\mathbb{F}}_p$ est ce que l'on appelle une *clôture algébrique* de $\mathbb{F}_p$.

Pour faire l'analogie avec le corps plus classique $\mathbb{Q}$, on pourrait dire que $\mathbb{Q}$ est inclus dans $\mathbb{C}$, l'ensemble des nombres complexes, qui est un corps algébriquement clos. Seulement dans $\mathbb{C}$, il y a des éléments qui ne sont pas racine d'un polynôme à coefficients rationnels, c'est ce que l'on appelle les *éléments transcendants*. Par exemple π ou e sont transcendants... mais ce n'est pas facile à prouver. Le premier nombre transcendant qui ait été exhibé est le nombre de Liouville qui vaut :

$$\sum_{i=0}^{\infty} \frac{1}{10^{i!}}$$

où $i!$ (lire *factorielle* i) désigne le produit $1 \times 2 \times \ldots \times i$. Bref, $\mathbb{C}$ n'est pas une clôture algébrique de $\mathbb{Q}$, il est trop gros. Et de fait, on peut construire un sous-corps de $\mathbb{C}$ qui est une clôture algébrique de $\mathbb{Q}$; c'est simplement l'ensemble des complexes qui sont racines d'un polynôme à coefficients rationnels. Décrire plus précisément cet ensemble par contre est très difficile.

Mais par contre, si l'on part de $\mathbb{F}_p$, on vient de donner une description relativement explicite de $\bar{\mathbb{F}}_p$. En particulier, en faisant un peu attention, elle est tout à fait programmable sur un ordinateur, et en réfléchissant un peu même de manière très efficace.

Notez finalement que, comme nous l'avons déjà dit, à partir de $\bar{\mathbb{F}}_p$, on peut retrouver les corps finis. Un corps fini de cardinal p^n est simplement donné par l'ensemble des solutions

de l'équation $x^{p^n} = x$. Ce n'est sûrement pas par contre la bonne façon de s'y prendre si l'on veut faire des calculs effectifs dans les corps finis.

4 Les nombres

4.1 Additionner, soustraire, multiplier et diviser

Peut-être vous rappelez-vous que l'on avait étudié les corps finis dans le seul but de pouvoir parler de nombres sur lesquels on pourrait faire des opérations sans retenue. On va donc maintenant reprendre les constructions initiées au début.

Fixons q une puissance d'un nombre premier p, et fixons $\mathbb{F}_q$ un corps fini à q éléments. On considère l'ensemble des nombres qui s'écrivent sous la forme :

$$a_n\, a_{n-1}\, \ldots\, a_0\, ,\, a_{-1}\, a_{-2}\, \ldots$$

où l'écriture « décimale » est *a priori* infinie. Les chiffres a_i sont donc des éléments de $\mathbb{F}_q$. On additionne et on multiplie ces nombres plus ou moins de la façon usuelle ; simplement, on ne tient pas compte des retenues.

L'ensemble des nombres ainsi formé est un corps. L'associativité et la commutativité de l'addition se vérifient directement. Les propriétés équivalentes pour la multiplication sont un peu plus laborieuses mais ne posent pas de difficultés majeures et nous allons simplement admettre ici qu'elles sont vérifiées. De même d'ailleurs que la distributivité. L'opposé du nombre $a_n\, a_{n-1}\, \ldots\, a_0\, ,\, a_{-1}\, a_{-2}\, \ldots$ est sans surprise le nombre $b_n\, b_{n-1}\, \ldots\, b_0\, ,\, b_{-1}\, b_{-2}\, \ldots$ où donc $b_i = -a_i$ pour tout indice i.

Faisons à présent le calcul de l'inverse. Considérons donc un nombre x non nul s'écrivant :

$$x \;=\; a_n\, a_{n-1}\, \ldots\, a_0\, ,\, a_{-1}\, a_{-2}\, \ldots$$

et supposons que le chiffre a_n est non nul. L'indice n n'est pas forcément supposé positif, bien entendu. En fait, quitte à diviser ce nombre par 10^n (c'est-à-dire le nombre formé d'un 1 suivi de n fois le chiffre 0), on peut supposer que $n = 0$. On cherche donc des éléments $b_i \in \mathbb{F}_q$ tels que :

$$\begin{array}{cccccccc} & & & a_0\, , & a_{-1} & a_{-2} & a_{-3} & \ldots \\ \times & b_n & \ldots & b_0\, , & b_{-1} & b_{-2} & b_{-3} & \ldots \\ \hline & & & 1\, , & 0 & 0 & 0 & \ldots \end{array}$$

Déjà tous les b_i pour $i > 0$ doivent être nuls. En effet, sinon, on désignerait par n le plus grand indice tel que $b_n \neq 0$, et il y aurait dans le produit un chiffre non nul en position n, et cela ne doit pas être. On cherche maintenant quelle peut être la valeur de b_0.

Mais si l'on fait l'opération, on tombe sur la condition $a_0 b_0 = 1$, ce qui ne laisse pas le choix, il faut prendre $b_0 = \frac{1}{a_0}$ qui est bien défini puisque $a_0 \neq 0$. Voyons maintenant la condition sur b_{-1}. En regardant le premier chiffre après la virgule du résultat, on voit que l'on a la contrainte $a_0 b_{-1} + b_0 a_{-1} = 0$ et donc, encore une fois, on n'a pas le choix, il faut prendre $b_{-1} = -\frac{b_0 a_{-1}}{a_0}$. On remarque que c'est encore possible puisque l'on ne fait que diviser par a_0 qui bien entendu est toujours non nul.

Pour b_{-2}, en regardant le deuxième chiffre après la virgule, on a la contrainte $a_0 b_{-2} + a_{-1} b_{-1} + a_{-2} b_0 = 0$, ce qui définit b_{-2}. On continue ainsi à construire successivement les chiffres de notre inverse. Ainsi l'inverse de x existe bien.

En conclusion, on a bien défini de cette façon un corps. Nous allons à présent essayer de résoudre des équations dans ce corps.

4.2 Méthode générale pour résoudre une équation

De façon générale, pour résoudre une équation on procède comme pour le calcul de l'inverse. On calcule successivement les chiffres de la solution. Le plus délicat en fait est souvent de trouver la position que doit occuper le premier chiffre. Supposons donc qu'on ait à résoudre une équation polynomiale de la forme :

$$a_n x^n + a_{n+1} x^{n+1} + \ldots + a_1 x + a_0 = 0$$

où les a_i sont des nombres donnés donc, avec disons $a_n \neq 0$, et où x est l'inconnue.

On aimerait calculer la position du premier chiffre de x. Notons[6] de façon générale $v(t)$ la position du premier chiffre dans le nombre t. Notons de plus $v(0) = -\infty$. On a alors quelques propriétés évidentes mais bien utiles qui sont :

$$\begin{aligned} v(xy) &= v(x) + v(y) \\ v(x+y) &\leqslant \sup(v(x), v(y)) \end{aligned}$$

et il y a égalité dans la dernière inégalité dès que $v(x) \neq v(y)$.

En particulier, on voit que pour que l'équation que l'on cherche à résoudre ait une chance d'être vérifiée, il faut qu'il existe deux indices i et j distincts tels que a_i et a_j soient non nuls et tels que $v\left(a_i x^i\right) = v\left(a_j x^j\right)$. En effet, si ce n'était pas le cas, d'après ce que l'on vient de dire, on aurait :

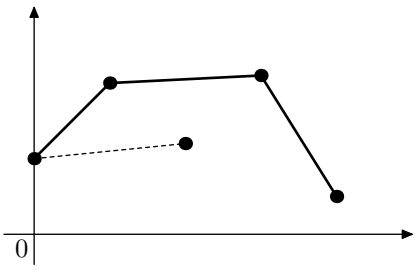
$$v\left(a_n x^n + a_{n+1} x^{n+1} + \ldots + a_1 x + a_0\right) = \sup_i v\left(a_i x^i\right) > -\infty$$

ce qui n'est pas possible. Mais cela nous fournit une valeur précise pour $v(x)$, précisément :

$$v(x) = -\frac{v(a_i) - v(a_j)}{i - j}$$

Il n'y a donc qu'un nombre fini de valeurs possibles pour $v(x)$.

On peut même continuer à en éliminer quelques unes ensuite. En effet, si x est solution, on peut trouver des indices i et j vérifiant $v\left(a_i x^i\right) = v\left(a_j x^j\right)$, mais également $v\left(a_i x^i\right) \geqslant v\left(a_k x^k\right)$ pour tout k. Pour exploiter cette nouvelle condition, généralement on dessine ce que l'on appelle le *polygone de Newton* de l'équation : on place dans le plan les points M_i de coordonnées $(i, v(a_i))$ et on les relie deux à deux sauf si le segment que l'on tracerait ainsi un segment se retrouverait totalement en dessous d'autres segments d'extremités M_i. Ainsi, sur le dessin suivant, on trace les segments représentés en gras, mais pas le segment en pointillé puisqu'il se trouve entièrement en dessous de segments gras :



[6] Pour ceux qui sont familiers, des anneaux de valuation discrète, le v de cet exposé désigne l'opposé de la valuation habituellement considérée.

Les $v(x)$ sont alors les opposés des pentes des segments tracés. En effet, on voit que si un segment n'a pas été tracé, c'est qu'il existe des entiers i, j et k tels que :

$$v\left(a_i x^i\right) = v\left(a_j x^j\right) \leqslant v\left(a_k x^k\right)$$

et donc le couple (i, j) ne donne pas un $v(x)$ valable.

Un léger problème se pose : les valeurs possibles pour $v(x)$ ne sont pas forcément entières. Il y a deux façons d'y apporter une solution : soit on cherche les solutions dans notre corps et donc on élimine ces valeurs, soit on accepte de construire des solutions ailleurs. Par exemple, supposons que l'on ait à résoudre $x^2 = 10$. On aura alors forcément $2v(x) = 1$ et donc il n'y a pas de solution dans notre corps. Mais si on rajoute un faux « 10 », un « 10 » dans lequel le premier 1 sera en position $\frac{1}{2}$, on remarque que ce nombre élevé au carré vaut bien le vrai 10, et donc qu'il est solution de l'équation.

Pour des raisons pratiques, il est utile de changer les notations. À partir de maintenant, écrivons le nombre :

$$a_n\, a_{n-1}\, \ldots\, a_0\, ,\, a_{-1}\, a_{-2}\, \ldots$$

sous la forme :

$$a_n t^n + a_{n-1} t^{n+1} + \ldots + a_0 + a_{-1}\frac{1}{t} + a_{-2}\frac{1}{t^2} + \ldots$$

Cette nouvelle notation a l'avantage de préciser la position d'un chiffre dans l'écriture. Notre faux « 10 » avec le 1 en position $\frac{1}{2}$ que l'on voulait rajouter s'écrit $t^{1/2}$, et on le distingue donc bien du vrai 10 qui lui s'écrit t. En outre, la notation est bien cohérente puisque $t^{1/2}$ serait une racine carrée de t.

Revenons-en à notre équation. On a déterminé les positions possibles pour le premier chiffre. Elles sont données par les quotiens finis $-\frac{v(a_i)-v(a_j)}{i-j}$. Soit v une telle position. On cherche x sous la forme $x = x_v t^v + x^{(1)}$ où $x_v \in \mathbb{F}_q$ est le chiffre placé en position v et $x^{(1)}$ est le reste, c'est-à-dire le nombre formé par les autres chiffres. En particulier, on aura $v\left(x^{(1)}\right) < v$.

Lorsque l'on réinjecte cela dans l'équation de départ, on tombe sur deux équations, l'une portant sur x_v et l'autre sur $x^{(1)}$, que l'on résout séparément. Pour le chiffre x_v, on a simplement une équation dans le corps des chiffres (pas forcément plus facile en réalité, mais supposons que l'on sache la résoudre), et pour $x^{(1)}$ on applique à nouveau la même méthode en se rappelant que l'on veut en outre $v\left(x^{(1)}\right) < v$. On obtient ainsi le premier chiffre de $x^{(1)}$ et donc le deuxième chiffre de x.

4.3 Trois situations génériques

Nous donnons ici des exemples simples qui illustrent la méthode expliquée précédemment. Nous allons en fait donner trois exemples qui illustrent trois situations bien différentes. Par chance, il se trouve que dans un sens que l'on précisera par la suite, toute équation est un certain mélange de ces trois cas.

Le cas non ramifié

Le terme « non ramifié » signifie que l'on ne va pas devoir intercaler des chiffres. Autrement dit, les v que l'on va calculer seront toujours entiers.

Prenons $q = 11$. Alors $\mathbb{F}_q$ est un corps fini à 11 éléments, par exemple l'ensemble $\{0, 1, \ldots, 10\}$ muni de l'addition et de la multiplication modulo 11. Considérons le nombre $a = 3,1415\ldots$ où on continue avec les décimales de π. Évidemment, ce nombre n'a aucun rapport avec le véritable π. Déjà, ces deux nombres ne vivent pas du tout dans le même espace.

Supposons que l'on veuille résoudre l'équation $x^2 = a$. On voit dans ces conditions que l'on a forcément $v = 0$, et donc on cherche x sous la forme $x = x_0 + x^{(1)}$ où x_0 est un chiffre et $x^{(1)}$ est un nombre tel que $v\left(x^{(1)}\right) < 0$. On a donc à résoudre :

$$x^2 = \left(x_0 + x^{(1)}\right)^2 = x_0^2 + \left(2x_0x^{(1)} + {x^{(1)}}^2\right) = a$$

On voit que $v\left(2x_0x^{(1)} + {x^{(1)}}^2\right) < 0$ et donc la seule possibilité est d'avoir :

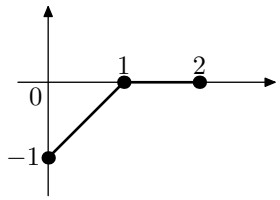
$$\begin{aligned} x_0^2 &= 3 \\ 2x_0x^{(1)} + {x^{(1)}}^2 &= 0,1415\ldots \end{aligned}$$

Il y a deux solutions à la première équation dans $\mathbb{F}_{11}$, comme on le voit par exemple en testant toutes les possibilités. Ces solutions sont 5 et 6. Continuons par exemple avec $x_0 = 6$ (cela marche exactement pareil avec $x_0 = 5$).

On s'intéresse maintenant à la deuxième équation qui devient :

$${x^{(1)}}^2 + x^{(1)} = 0,1415\ldots$$

Comme précédemment on cherche les positions possibles pour le premier chiffre de $x^{(1)}$. Pour la première fois, on trace ici le polygone de Newton. Il ressemble à ça :



et on voit donc que les $v\left(x^{(1)}\right)$ possibles sont 0 et -1. Mais on rappelle que l'on veut $v\left(x^{(1)}\right) < 0$ et donc forcément $v\left(x^{(1)}\right) = -1$. On cherche donc $x^{(1)}$ sous la forme $x^{(1)} = x_{-1} + x^{(2)}$. L'équation se transforme à nouveau et on obtient une équation pour x_{-1} et une pour $x^{(2)}$ et on continue ainsi.

Ce qu'il peut se passer, c'est que l'équation à résoudre dans le corps des chiffres n'ait pas de solution. Par exemple si π avait commencé par 2 et non par 3, on aurait eu à résoudre $x_0^2 = 2$ qui n'a pas de solution dans $\mathbb{F}_{11}$. Mais peu importe, il aurait juste fallu considérer une extension de $\mathbb{F}_{11}$ dans laquelle cette équation a une solution.

Le cas modérément ramifié

Dans ce cas, on intercale effectivement des chiffres mais les positions qui apparaissent ont un même dénominateur commun. Il n'y a pas grand chose à dire de plus dans ce cas que dans le cas précédent en fait.

Pour exemple, on peut juste modifier le précédent et résoudre toujours dans le même corps :

$$x^2 = 31,4159\ldots$$

Ici, dès la première étape, on va trouver $v = \frac{1}{2}$. On va donc poser $x = x_{1/2}t^{1/2} + x^{(1)}$ et on va reporter dans l'équation comme on l'a expliqué. On ne va pas refaire l'amorce du calcul, c'est exactement la même chose que dans le cas non ramifié.

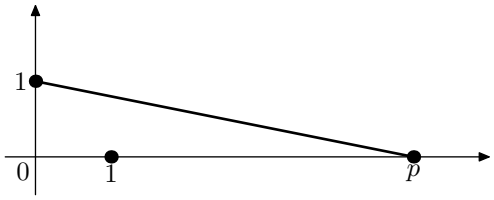
En fait, ce que l'on peut remarquer plus subtilement c'est que notre équation s'écrit $x^2 = at$ et donc encore $\left(\frac{x}{t^{1/2}}\right)^2 = a$ et on se ramène ainsi au cas précédent.

Le cas sauvagement ramifié

Une équation bien moins agréable est la suivante :

$$x^p = x + t$$

Commençons par la traiter par la méthode des polygones de Newton. Le polygone qu'il faut tracer est le suivant :



et on voit qu'il n'y a qu'un seul segment de pente $-\frac{1}{p}$. On écrit donc $x = x_{1/p}t^{1/p} + x^{(1)}$. Et l'équation devient :

$$x_{1/p}^p t + x^{(1)p} = x_{1/p}t^{1/p} + x^{(1)} + t$$

En identifiant les termes qui s'identifient entre eux, on arrive au système :

$$\begin{aligned} x_{1/p}^p &= 1 \\ x^{(1)p} &= x_{1/p}t^{1/p} + x^{(1)} \end{aligned}$$

La première équation admet pour solution $x_{1/p} = 1$, c'est même la seule. Et donc maintenant, on se retrouve avec :

$$x^{(1)p} = x^{(1)} + t^{1/p}$$

On est donc ramené à un problème assez équivalent à celui du départ. On trace le polygone de Newton correspondant qui admet un segment de pente $-\frac{1}{p^2}$ et on poursuit la résolution ainsi. On arrive sans surprise au système :

$$\begin{aligned} x_{1/p^2}^p &= 1 \\ x^{(2)p} &= x_{1/p^2}t^{1/p^2} + x^{(2)} \end{aligned}$$

et donc on prend $x_{1/p^2} = 1$, ce qui donne l'équation :

$$x^{(2)p} = x^{(2)} + t^{1/p^2}$$

qui se résout encore de façon analogue. Finalement, on voit que si solution il y a, elle devrait s'exprimer de la façon suivante :

$$x_0 = t^{1/p} + t^{1/p^2} + t^{1/p^3} + \ldots + t^{1/p^n} + \ldots$$

et les dénominateurs qui apparaissent dans les exposants ne sont pas bornés. On ne sait pas encore trop calculer avec x mais on peut imaginer sans mal que x_0^p s'exprime de la façon suivante :

$$x_0^p = t + t^{1/p} + t^{1/p^2} + \ldots + t^{1/p^n} + \ldots$$

et donc on aurait bien au moins $x_0^p = x_0 + t$.

Cependant cela ne va pas toujours être le cas, c'est-à-dire que l'on ne va pas forcément ainsi tomber sur une solution. Précisément regardons l'équation :

$$x^p = x\,(t+1)^{p-1} + t\,(t^p + 1)$$

Ce n'est sans doute pas l'exemple le plus simple, mais quelques manipulations algébriques élémentaires montrent que cette équation peut se réécrire sous la forme :

$$\left(\frac{x}{t+1}\right)^p = \frac{x}{t+1} + t$$

et on se ramène ainsi à l'équation précédente. Une solution est donc $x_0\,(t+1)$ qui devrait s'écrire au final sous la forme :

$$\begin{aligned} x_1 \;=\; & t^{1+1/p} + t^{1+1/p^2} + t^{1+1/p^3} + \ldots + t^{1+1/p^n} + \ldots \\ & + t^{1/p} + t^{1/p^2} + t^{1/p^3} + \ldots + t^{1/p^n} + \ldots \end{aligned}$$

Ainsi, si l'on cherche à trouver cette solution avec la méthode des polygones de Newton, on trouve à la première itération le terme $t^{1+1/p}$, puis le terme t^{1+1/p^2}, et ainsi de suite... Et au final, on n'obtient que :

$$x_1' = t^{1+1/p} + t^{1+1/p^2} + t^{1+1/p^3} + \ldots + t^{1+1/p^n} + \ldots$$

ce qui n'est pas entièrement x_1. Pour rattraper les autres termes, il faut encore continuer : on écrit $x = x_1' + x^{(\infty)}$ et on cherch l'équation vérifiée par $x^{(\infty)}$, qui se trouve être la la première équation traitée. On la résout alors comme cela a déjà été expliqué.

On peut prouver que *si l'on continue suffisamment longtemps*, on va toujours obtenir une solution. Mais avant de donner une démonstration, il faudrait donner un énoncé précis et ce n'est déjà, là, pas facile. Typiquement, il faut parler d'ordinaux et d'induction transfinie. Nous n'allons donc pas nous attarder plus sur ce point.

4.4 Grand rassemblement pour les nombres

Toutes les constructions faites précédemment sont bien jolies mais les nombres considérés existent plus par l'opération du Saint-Esprit qu'autre chose. Il faudrait définir un cadre dans lequel tout ce que l'on a dit précédemment trouve une justification. Plus exactement, on aimerait construire un corps dans lequel on retrouve tous les éléments que l'on a vu apparaître jusqu'à présent. Ceci est donc l'objet de ce paragraphe.

Que prendre donc comme corps ? Notons $\bar{\mathbb{F}}_p$ une clôture algébrique de $\mathbb{F}_p$, comme nous l'avons construite dans la troisième section. Une première idée serait de considérer l'ensemble des éléments de la forme

$$x = \sum_{e \in \mathbb{Q}} a_e t^e$$

où les a_e sont des éléments de $\bar{\mathbb{F}}_p$, c'est-à-dire plus formellement l'ensemble des fonctions de $\mathbb{Q}$ dans $\bar{\mathbb{F}}_p$. Cela ne peut pas marcher, car on aura des difficultés pour définir le produit des deux nombres $1 + t + t^2 + \ldots + t^n + \ldots$ et $1 + t^{-1} + t^{-2} - \ldots - t^{-n} - \ldots$. Tous les produits $t^i \cdot t^{-i}$ vont contribuer au terme constant du produit et donc pour déterminer ce terme constant, il faudrait additionner une infinité de fois le chiffre 1 dans $\bar{\mathbb{F}}_p$, ce que l'on ne sait pas faire.

On pense alors bien sûr à imposer la condition disant qu'il doit exister un nombre v tel que $a_e = 0$ pour tout $e \geqslant v$. Mais on trouve rapidement un problème analogue, par exemple lorsque l'on veut multiplier les deux nombres suivants :

$$t + t^{1/2} + t^{1/3} + \ldots + t^{1/n} + \ldots$$

$$t^{-1} + t^{-1/2} + t^{-1/3} + \ldots + t^{-1/n} + \ldots$$

En fait, la condition à imposer est l'existence d'un chiffre « le plus à gauche », l'existence du $v(x)$ quoi ! On regarde donc l'ensemble I des rationnels e tel que $a_e \neq 0$ et on impose que cet ensemble admette un plus grand élément. Cette condition discrédite donc les faux nombres $1 + t + t^2 + \ldots + t^n + \ldots$ et $t^{-1} + t^{-1/2} + t^{-1/3} + \ldots + t^{-1/n} + \ldots$. Seulement, bien entendu, cette condition ne va pas suffire : l'élément qui s'écrit $1 + t^{-1} + t^{-1/2} + t^{-1/3} + \ldots + t^{-1/n} + \ldots$ ne va pas être évincé alors qu'il devrait l'être.

En fait, on ne veut pas simplement que E ait un plus grand élément, mais que tout sous-ensemble (non vide) de E en ait un. Autrement dit, tous les « sous-nombres » de E doivent avoir un « chiffre le plus à gauche ».

Et cela fonctionne. On considère M donc l'ensemble des fonctions $a : \mathbb{Q} \to \mathbb{F}_p$ telles que tout sous-ensemble non vide de $\{e \in \mathbb{Q} \,/\, a(e) \neq 0\}$ possède un plus grand élément. Bien sûr une telle fonction représente le nombre :

$$\sum_{e \in \mathbb{Q}} a(e)\, t^e$$

On notera $S(a)$ et on appellera *support de* a l'ensemble $\{e \in \mathbb{Q} \,/\, a(e) \neq 0\}$ sur lequel on a fait notre hypothèse.

Avant de continuer, constatons que tous les nombres qui sont apparus dans les exemples traités précédemment étaient de cette forme, c'est rassurant.

Voyons maintenant si l'on est capable de définir des opérations sur cet ensemble M. L'addition ne pose pas de problème : la somme de $\sum_{e \in \mathbb{Q}} a(e)\, t^e$ et de $\sum_{e \in \mathbb{Q}} b(e)\, t^e$ est le nombre $\sum_{e \in \mathbb{Q}} (a(e) + b(e))\, t^e$, et il faut juste vérifier que $S(a+b)$ possède encore la propriété voulue. Prenons donc I un sous-ensemble de cet ensemble et posons $I_1 = I \cap S(a)$ et $I_2 = I \cap S(b)$. On remarque directement que l'on a $I = I_1 \cup I_2$. Si l'un des deux ensembles de l'union est vide, c'est que I est tout entier inclus soit dans $S(a)$, soit dans $S(b)$, et donc il admet un plus grand élément. Sinon, I_1 et I_2 admettent tous les deux un plus grand élément, et le plus grand de ces deux nombres est le plus grand élément de I.

Faisons la multiplication. On a envie de développer et donc de définir quelque chose qui ressemblerait à :

$$\left(\sum_{e\in\mathbb{Q}} a(e)\,t^e\right)\cdot\left(\sum_{e\in\mathbb{Q}} b(e)\,t^e\right)=\sum_{e\in Q}\left(\sum_{i+j=e} a(i)\,b(j)\right)t^e$$

Mais pour cela, il faut justifier que pour tout e, la somme $\sum_{i+j=e} a(i)\,b(j)$ ne comporte qu'un nombre fini de termes non nuls et aussi que l'ensemble des e pour lesquels elle est non nulle vérifie la bonne propriété.

Commençons par la première vérification donc. Fixons un rationnel e et notons donc A l'ensemble des indices $i\in\mathbb{Q}$ tels que a_i et b_{e-i} soient tous les deux non nuls. Supposons par l'absurde que cet ensemble d'indices soit infini. C'est un sous-ensemble non vide de $S(a)$ et donc il admet un plus grand élément, disons i_1. L'ensemble $A\setminus\{i_1\}$ est encore non vide (puisque A est supposé infini) et inclus dans $S(a)$ donc il admet à son tour un plus grand élément, disons i_2. Ainsi de suite puisque A est infini, on construit une suite strictement croissante :

$$i_1>i_2>\ldots>i_n\ldots$$

d'éléments de A. L'ensemble $\{e-i_1,e-i_2,\ldots,e-i_n,\ldots\}$ définit alors un sous-ensemble de $S(b)$ qui n'admet pas de plus grand élément. C'est absurde. On en déduit que A est fini et donc que la somme porte bien sur un nombre fini de termes.

Pour le second point qu'il faut vérifier, on remarque dans un premier temps que tout élément de $S(ab)$ s'écrit comme une somme d'un élément de $S(a)$ et d'un élément de $S(b)$. Soit X un sous-ensemble non vide de $S(ab)$. Supposons que X n'admette pas de plus grand élément ; cela signifie que chaque fois que l'on prend un $x\in X$, il existe $x'\in X$ avec $x'>x$. Ainsi on peut construire une suite strictement croissante (x_n) d'éléments de X. Chacun des x_n s'écrit $x_n=a_n+b_n$ avec $a_n\in S(a)$ et $b_n\in S(b)$. L'ensemble $\{b_1,b_2,\ldots,b_n,\ldots\}$ est inclus dans $S(b)$ et donc admet un plus grand élément, c'est l'un des b_i disons b_{i_1}. De même l'ensemble $\{b_{i_1+1},b_{i_1+2},\ldots,b_{i_1+m},\ldots\}$ admet un plus grand élément, c'est b_{i_2}. De cette façon, on construit une suite d'indices :

$$i_1<i_2<i_3<\ldots<i_n<\ldots$$

telle que :

$$b_{i_1}\geqslant b_{i_2}\geqslant b_{i_3}\geqslant\ldots\geqslant b_{i_n}\geqslant\ldots$$

Attention, on n'a pas forcément des inégalités strictes, ici ! Quoi qu'il en soit, comme la suite (x_n) est strictement croissante et que $a_n=x_n-b_n$, on déduit :

$$a_{i_1}<a_{i_2}<a_{i_3}<\ldots<a_{i_n}<\ldots$$

avec des inégalités strictes. En particulier, l'ensemble formé des a_{i_j} est inclus dans $S(a)$ et n'admet pas de plus grand élément. Voici notre contradiction, de laquelle découle la propriété que l'on voulait prouver.

On sait donc bien définir une addition et une multiplication sur l'ensemble M. Les propriétés de commutativité, d'associativité et de distributivité ne posent pas de problème majeur. Trouver l'opposé d'un élément de M est aussi immédiat.

En fait, M est un corps, et même un corps algébriquement clos. Autrement dit on sait calculer l'inverse des éléments de M et même résoudre des équations polynomiales. Aussi bien pour l'un que pour l'autre, on procède par « approximations successives » en déterminant les chiffres les uns après les autres, c'est-à-dire en utilisant la méthode de Newton que l'on a explicitée précédemment.

4.5 Vers une clôture algébrique

Le corps que l'on a construit est certes algébriquement clos mais il est beaucoup trop gros, un peu comme $\mathbb{C}$ est démesurément gros par rapport à $\mathbb{Q}$. Nous entendons par là qu'il y a plein d'éléments dans M qui ne sont jamais atteints par la résolution d'équations polynomiales.

Par exemple, il est possible de prouver que si l'on définit un corps N, disons, un peu comme M mais en imposant que tous les coefficients a_e d'un nombre a soient dans un même $\mathbb{F}_q$, on obtient un corps beaucoup plus petit que N qui est lui aussi algébriquement clos. Tous les éléments, donc, qui sont dans M mais pas dans N ne vont pouvoir s'obtenir comme solution d'une équation polynomiale.

Cela dit, cette restriction n'est pas non plus suffisante. Il faut aussi voir par exemple que la ramification sauvage ne peut se produire qu'avec des puissances de p. Plus exactement si l'on prend le corps N' formé des éléments $a \in M$ pour lesquels il existe un entier d tel que tout $e \in S(A)$ s'écrive $\frac{k}{dp^n}$ pour certains k et n... donc si l'on prend le corps N' formé de ces éléments disions-nous, on obtient encore un corps algébriquement clos[7].

Ensuite, bien sûr, on peut prendre l'intersection de N et de N' qui fonctionne encore. Mais là encore, ce n'est pas une clôture algébrique. Si l'on veut vraiment atteindre une clôture algébrique, il faut exprimer d'autres conditions précises et un peu techniques sur les exposants et les coefficients. Nous n'en dirons pas plus. Sachez simplement que le problème de caractériser précisément la clôture algébrique à l'intérieur de M est un problème résolu.

[7] C'est en ce sens, que nous disions quelques paragraphes auparavant, qu'il n'y a que trois grandes familles de solutions : les non ramifiées, les modérément ramifiées et les sauvagement ramifiées.

Bibliographie commentée

Comme le titre l'indique, cet exposé traite des corps. Un *corps* est un objet algébrique qui est généralement présenté de façon très succincte en classe préparatoire ou en licence. Tout manuel de cours de prépa présentera donc les définitions rigoureuses de groupes, d'anneaux, de corps, de morphismes, concepts intervenant de façon sous jascente dans cet exposé.

La seconde partie de ce texte, appelé *Les chiffres*, traite des corps finis. L'étude des corps finis est très bien faite dans [1]. Ce livre prend le parti de se baser sur les applications à l'algorithmique et principalement aux codes correcteurs d'erreurs et à la cryptographie. Il est donc très concret, contrairement à d'autres livres d'algèbre plus classiques qui donnent une autre présentation, souvent en parallèle avec la théorie de Galois. Un de ces livres plus abstraits est par exemple [2], et un bon livre présentant la théorie de Galois de façon très élémentaire est [3].

Si l'on souhaite s'embarquer plus amplement dans l'algèbre et dans la théorie pure, un bon livre de référence est [4].

La troisième partie est relativement originale, car il est rare que l'on présente une clôture algébrique de telle façon. On a souvent simplement besoin de l'existence d'icelle et des propriétés galoisiennes. Toutefois, la présentation que l'on donne a *peut-être* un avantage pédadogique : bien qu'étant sans doute plus compliquée à établir, elle possède un certain aspect concret et plus visuel, qui peut probablement en rassurer certains et à en déstabiliser d'autre. De façon anecdotique, soulignons que dans [5], Conway construit un corps qu'il appelle On_2 et bien que la présentation diffère de celle de cet exemple, la construction revient à celle que l'on donne dans le cas $p = 2$.

La dernière partie est consacrée à ce que l'on appelle communément les *corps locaux*. Ceux-ci sont étudiés de façon très claire et très détaillée dans [6], du moins dans la première partie. Ce dernier livre demande encore un bagage algébrique « minimal », quoiqu'il en soit nécessaire si l'on désire vraiment se plonger dans cette théorie.

Dans le texte qui précède, nous nous sommes restreints à l'étude des corps locaux de *caractéristique égale et positive*. La construction de la clôture algébrique que nous avons ébauchons est traitée complètement dans [7], qui est un véritable article de recherche, donc plutôt difficle. Il existe des constructions équivalentes pour d'autres corps locaux, dit de *caractéristique mixte*, comme on peut en trouver dans [8]. Cependant, ce dernier cas est encore plus complexe.

Références

[1] M. Demazure, *Cours d'algèbre : primalité, divisibilité, codes*, Cassini, Paris, 1997

[2] P. Ribenboim, *Arithmétique des corps*, Hermann, Paris, 1972

[3] E. Artin, *Galois Theory*, Notre Dame, Indiana, 1959

[4] S. Lang, *Algebra*, third edition, Addison-Wesley Publishing Company, 1993

[5] J. Conway, *On number and games*, second edition, AK Peters, 2001

[6] J.P. Serre, *Corps locaux*, Hermann, Paris, 1968

[7] `http://xxx.lanl.gov/ps/math.AG/9810142`

[8] `http://xxx.lanl.gov/ps/math.AG/9906030`