LES EXTENSIONS DE CORPS

NANCY WALLACE

Définition 1 : Un **monoïde** est un ensemble, disons M, muni d'une opération binaire $\star : M \times M \to M$ associative et tel qu'il existe un élément neutre noté $e_M \in M$ ayant la propriété que :

$$\forall\ m \in M,\ e_M \star m = m \star e_M = m.$$

Exemple : $(\mathbb{Z}, \cdot)$ et $(\mathcal{M}_{n\times n}(\mathbb{Q}), \cdot)$ sont des monoïdes.

Définition 2 : Un **groupe** est un ensemble, disons G, muni d'une opération binaire $\star : G \times G \to G$ associative et tel qu'il existe un élément neutre noté $e_G \in G$ ayant la propriété que :

$$\forall\ g \in G,\ e_G \star g = g \star e_G = g.$$

De plus tous les éléments du groupe sont inversible. C'est à dire, que :

$$\forall g \in G\ \exists\ g^{-1} \in G \text{ tels que } g \star g^{-1} = e_G = g^{-1} \star g.$$

De plus nous disons que le groupe est abélien si l'opération est commutative.
Notons que nous pouvons définir un groupe comme étant un monoïde dont tous les éléments sont inversible.

Exemple : $(\mathbb{Z}, +)$ et $(\mathcal{M}_{n\times n}(\mathbb{Q}), +)$ sont des groupes.

Définition 3 : Un **anneau** est un ensemble, disons A, muni de d'une opérations binaire $\star$ associative et commutative, ayant un élément neutre noté 0_A et dont tous les éléments sont inversible pour l'opération $\star$. L'ensemble est également muni d'une opération $\heartsuit$ associative et distributive sur l'opération $\star$. De plus, A possède un élément neutre noté $1_A \in A$ pour l'opération $\heartsuit$.
Notons que nous pouvons définir un anneau comme étant un monoïde pour $(A_{\setminus\{0_A\}}, \heartsuit)$ et un groupe abélien pour $(A, \star)$ tel que $\heartsuit$ soit distributif sur l'opération $\star$.

Exemple : $(\mathbb{Z}, +, \cdot)$ et $(\mathcal{M}_{n\times n}(\mathbb{Q}), +, \cdot)$ sont des anneaux.

Définition 4 : Un **corps** est un ensemble, disons K, tel que K munie de l'opération binaire associative $\star$ est un groupe abélien et $K_{\setminus\{0_K\}}$ muni de l'opération binaire $\heartsuit$ distributive sur $\star$ est un groupe. Si $K_{\setminus\{0_K\}}$ muni de l'opération binaire $\heartsuit$ est un groupe abélien alors le corps est dit commutatif.

Exemple : $(\mathbb{Q}, +, \cdot)$ et $\left(\left\{M \in \mathcal{M}_{n\times n}(\mathbb{C}) : M = \begin{bmatrix} a & b \\ -\bar{b} & \bar{a} \end{bmatrix}\right\}, +, \cdot\right)$ sont des corps. Notons que le deuxième n'est pas commutatif. Un petit exercice permet de montrer qu'il est isomorphe au corps des Quaternions.

Par abus nous omettons habituellement le symbole d'opération binaire et écrivons simplement gh plutôt que $g \star h$ si le monoïde (respectivement groupe, anneau, corps) n'est pas nécessairement commutatif et $g + h$ si il est commutatif.

Définition 5 : Soit A un anneau. Un **diviseur de zéro** est un élément non nul, $a \in A$ pour lequel il existe $b \in A_{\setminus\{0_A\}}$ tel que $ab = 0_A$. Un anneau est dit **intègre** si il n'a pas de diviseur de zéro.

Exemple : Les matrices $\begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}$ et $\begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}$ sont des diviseurs de zéros, car :

$$\begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}.$$

Théorème 1 : Les corps sont des anneaux intègre.

Preuve : Remarquons d'abord que par définition les corps sont des anneaux.

Par contradiction soit K un corps qui n'est pas un anneau intègre. Il existe alors $a, b \in K_{\setminus\{0_K\}}$ tel que $ab = 0_K$, il est possible que $a = b$. Puisque K est un corps tout ses éléments sont inversibles, nous avons donc $a^{-1} \in K$ tel que $a^{-1}a = 1_K$. Donc $b = 1_K b = (a^{-1}a)b = a^{-1}(ab) = a^{-1}0_K = 0_K$. Ce qui contredit $b \in K_{\setminus\{0_K\}}$.

Nous avons donc bien que les corps sont tous des anneaux intègres.

Notation 1 : Un corps à p éléments est noté $\mathbb{F}_p$

Théorème 2 : (Wedderburn) Tout corps fini est commutatif.

La preuve de ce théorème utilise des outils qui dépasse le cadre de cette exposé. Il est, cependant, possible de trouver une preuve dans [1] à la page 427. Une autre preuve donné par Ernst Witt est disponible dans [2] à la page 35.

Définition 6 : Soit G, H deux groupes muni respectivement des opérations $\star$ et $\heartsuit$. Un **morphisme de groupe** est une application $f : G \to H$ tel que :

$$\forall g, k \in G, f(g \star k) = f(g) \heartsuit f(k).$$

Un petit exercice permet de montrer que cette définition implique que $f(e_G) = e_H$.

Définition 7 : Soit A, B deux anneaux muni respectivement des opérations $\star$,$+_A$ et $\heartsuit$,$+_B$. Un **morphisme d'anneau** est une application $f : A \to B$ tel que :

$$\begin{aligned} \forall a, b \in A,\ f(a \star b) &= f(a) \heartsuit f(b), \\ f(a +_A b) &= f(a) +_B f(b), \\ f(1_A) &= 1_B \end{aligned}$$

Un **isomorphisme** de groupe (respectivement d'anneau, de corps) est un morphisme de groupe (respectivement d'anneau, de corps) bijectif. Autrement dit, si f est in isomophisme il existe f^{-1} tel que $f \circ f^{-1} = f^{-1} \circ f = Id$.

Un **automorphisme** de groupe (respectivement d'anneau, de corps) est un isomorphisme d'un groupe de groupe (respectivement d'anneau, de corps) dans lui-même.

Notons que si $ker\{f\} = \{0_G\}$ alors le morphisme est injectif et si $Im\{f\} = H$ le morphisme est surjectif.

Les **morphismes de corps** sont tout simplement des morphisme d'anneau, puisque les corps sont des anneaux intègre par le théorème 1.

Proposition 1 : Les morphisme de corps non triviaux sont toujours injectif.

Preuve : Par contradiction, supposons qu'il existe K, C deux corps non triviaux et $f : K \to C$, un morphisme de corps non injectif. Nous aurions alors qu'il existe :

$$x \in Ker\{f\} = \{x \in K | f(x) = 0_C\} \text{ tel que } x \neq 0_K.$$

Mais comme K est un corps et x est non nul, il existe :

$$x^{-1} \in K \text{ tel que } xx^{-1} = 1_k.$$

Nous avons donc :

$$f(1_K) = f(xx^{-1}) = f(x)f(x^{-1}) = 0 \cdot f(x^{-1}) = 0_C.$$

Or comme f est un morphisme de corps nous devons avoir $f(1_K) = 1_C$.

Donc $0_C = 1_C$ et C est un corps trivial d'où la contradiction ∎

Exemple :

$$f : \mathbb{Q} \to \mathbb{C} \qquad g : \mathbb{C} \to \mathcal{M}_{2\times 2}(\mathbb{R}) \qquad h : \mathbb{H} \to \mathcal{M}_{2\times 2}(\mathbb{C})$$

$$x \mapsto x, \qquad z = a + ib \mapsto \begin{bmatrix} a & b \\ -b & a \end{bmatrix}, \qquad w = a + ib + jc + kd \mapsto \begin{bmatrix} a & b \\ -\bar{b} & \bar{a} \end{bmatrix}.$$

Sont des morphisme injectif. Par contre, ils ne sont pas tous surjectif.

Définition 8 : Un **corps premier** est un corps dont les seules sous-corps sont propre. Autrement dit, ses seules sous-corps sont $\{0_k\}$ et K.

Théorème 3 : Tout corps commutatif K non trivial contient un sous-corps qui est un corps premier isomorphe à $\mathbb{Q}$ ou à $\mathbb{Z}/\mathbb{Z}_p$, p premier.

Preuve : Soit A l'intersection de tous les sous-corps non triviaux de K. Nous avons que $0_K, 1_K \in A$ puisque tous les sous-corps contiennent $0_K, 1_K$. De plus si a est dans A alors a est dans tous les sous-corps et comme tous les sous corps possèdent leurs inverses alors a^{-1}et $-a$ sont dans A. Enfin si a et b sont dans A alors a et b sont dans tous les sous-corps et comme tous les sous corps sont fermés pour leurs opérations binaire alors ab et $a + b$ sont dans A. Donc A est un corps et c'est le plus petit sous corps de K, car si il en existait un plus petit il serait dans l'intersection des sous-corps.

Si A est infini, comme A est fermé pour l'addition. Nous devons avoir :

$$\underbrace{1_A + \cdots + 1_A}_{\text{n fois}} = n \cdot 1_A \in A, \ \forall n \in \mathbb{N}$$

Puisque A possède ses inverses nous trouvons de la même façon que A doit avoir :

$$-n \cdot 1_A \in A \ \forall n \in \mathbb{N} \text{ donc } n \cdot 1_A \in A \ \forall n \in \mathbb{Z} \text{ et}$$

$$n^{-1} \cdot 1_A \in A \ \forall n \in \mathbb{Z}_{\setminus\{0\}} \text{ donc } r \cdot 1_A \ \forall r \in \mathbb{Q}.$$

Notons que ceci définit le plus petit sous-corps de K.

Nous avons alors que le morphisme de corps f pour lequel $f(1_a) = 1 \in \mathbb{Q}$ est surjectif et comme A est non trivial et par la proposition 1 tous les morphisme de corps sont injectif nous avons bien la bijection.

Donc $A \simeq \mathbb{Q}$.

Si A est fini soit p le plus petit entier tel que :

$$\underbrace{1_A + \cdots + 1_A}_{\text{p fois}} = 0_A$$

Celui-ci existe puisque A est fermé pour l'addition et est fini. De plus, pour tout $n, 0 < n < p$ l'inverse additif de $n \cdot 1_A$ est simplement $(p - n) \cdot 1_A$.

Si p n'est pas premier il existe $r, s \in \mathbb{N}^*$ tel que $rs = p$, mais alors r serait diviseur de zéro donc A n'est pas un corps ce qui est absurde alors p doit être premier.

Si p est premier pour tout $n, 0 < n < p$ nous avons par le lemme de Bézout qu'il existe $k, l, \in \mathbb{Z}$ tel que $kn + lp = 1$ donc $kn \cdot 1_A \equiv 1_A \mod p$. Donc $n \cdot 1_A$ est inversible. Notons que ceci définit le plus petit sous-corps de K.

Nous avons alors que le morphisme de corps f pour lequel $f(1_a) = 1 \in \mathbb{Z}/p\mathbb{Z}$ est surjectif et par la proposition 1 tous les morphisme de corps sont injectif nous avons bien la bijection.

Donc $A \simeq \mathbb{Z}/p\mathbb{Z}$, p premier ∎

Vous pouvez trouver à la page.72 de [3] une plus belle preuve, mais elle use d'outils qui non pas été aborder ici.

Définition 9 : La **caractéristique**, disons p, d'un corps fini est le cardinal de son sous-corps premier. Les corps infini sont de caractéristique 0.

Définition 10 : Soit K un corps fini de caractéristique p. Un **morphisme de Frobenius** l'application :

$$\begin{aligned} F : K &\to K \\ a &\mapsto a^p. \end{aligned}$$

Proposition 2 : Soit K un corps fini de caractéristique p et F un morphisme de Frobenius. Si K est fini c'est un **automorphisme** (C'est pourquoi nous parlons habituellement d'automorphisme de Frobenius). Si $K \simeq \mathbb{Z}/p\mathbb{Z}$ alors F est l'identité.

Preuve : Montrons d'abord que c'est bien un morphisme. Pour tout $a, b \in K$ nous avons :

$$\begin{aligned} F(ab) = (ab)^p &= a^p b^p, \text{ puisque } K \text{ est commutatif,} \\ &= F(a)F(b), \text{ par définition de } F. \end{aligned}$$

$$\begin{aligned} F(a+b) = (a+b)^p &= \sum_{i=0}^{p} \binom{p}{i} a^i b^{p-i}, \text{ par le binôme de Newton,} \\ &= a^p + b^p + \sum_{i=1}^{p-1} \binom{p}{i} a^i b^{p-i}, \\ &= a^p + b^p + \sum_{i=1}^{p-1} \frac{p!}{(p-i)!i!} a^i b^{p-i}, \\ &\equiv a^p + b^p, \text{ car } p \text{ est premier et } p-i,\ i < p\ \forall i, \text{ donc } p-i \not| p \text{ et } i \not| p\ \forall i, \\ &= F(a) + F(b), \text{ par définition de } F. \end{aligned}$$

$$F(1_k) = (1_K)^p = 1_K, \text{ par définition de neutre multiplicatif.}$$

Donc le morphisme de Frobenius est bien un morphisme d'anneau (donc de corps).

Si K est fini c'est un automorphisme, car les morphismes de corps sont injectif par la proposition 1 et lorsque les groupes sont finis et de même cardinal les morphismes injectif sont également surjectif, d'où la bijection.

Si $K \simeq \mathbb{Z}/p\mathbb{Z}$ alors par le théorème de Fermat nous avons $a^{p-1} \equiv 1 \mod p$ et donc que $a^p \equiv a \mod p$, c'est donc bien l'identité ∎

Définition 11 : Soit K un corps. Une **extension de corps** de K, disons L, est un corps contenant K. Autrement dit, L est une extension de K si et seulement si K est un sous-corps de L.

Remarque : L peut être vu comme un espace vectoriel su K. Le **degré** de l'extension est la dimension de L sur K.

Exemple : Les nombres complexe peuvent être vu comme un espace vectoriel sur $\mathbb{R}$. La dimension de l'extension est de degré 2, car $\mathbb{C}$ est engendré par la base $\{1, i\}$ sur $\mathbb{R}$.

Théorème 4 : les n itérations de l'automorphisme de Frobenius $(Id, F, F^2, \cdots, F^{n-1})$ sont des automorphismes de $\mathbb{F}_{p^n}$ un corps fini (donc commutatif), p premier.

Preuve : Montrons d'abord que la composition d'un automorphisme d'anneau est un automorphisme d'anneau. Soit f et g deux automorphismes de $\mathbb{F}_{p^n}$, et $a, b \in \mathbb{F}_{p^n}$, nous avons :

$$(f \circ g)(ab) = f(g(ab)) = f(g(a)g(b)) = f(g(a))f(g(b)) = (f \circ g)(a)(f \circ g)(b),$$
$$(f \circ g)(a + b) = f(g(a) + g(b)) = f(g(a)) + f(g(b)) = (f \circ g)(a) + (f \circ g)(b),$$
$$(f \circ g)(1_{\mathbb{F}_{p^n}}) = f(g(1_{\mathbb{F}_{p^n}})) = f(1_{\mathbb{F}_{p^n}}) = 1_{\mathbb{F}_{p^n}}.$$

Donc $f \circ g$ est bien un morphisme et puisque f et g sont des automorphismes il existe f^{-1}, g^{-1} tels que $f^{-1} \circ f = f \circ f^{-1} = Id$ et $g^{-1} \circ g = g \circ g^{-1} = Id$.

Par définition d'automorphismes f^{-1} et g^{-1} sont des automorphismes. Donc $g^{-1} \circ f^{-1}$ est un morphisme par ce qui précède. Nous avons alors que $g^{-1} \circ f^{-1} \circ f \circ g$ et $f \circ g \circ g^{-1} \circ f^{-1}$ sont des morphisme. Or nous avons :

$$g^{-1} \circ f^{-1} \circ f \circ g = g^{-1} \circ (f^{-1} \circ f) \circ g = g^{-1} \circ Id \circ g = g^{-1} \circ g = Idet$$
$$f \circ g \circ g^{-1} \circ f^{-1} = f \circ (g \circ g^{-1}) \circ f^{-1} = f \circ Id \circ f^{-1} = f \circ f^{-1} = Id.$$

Donc $f \circ g$ est bijectif et c'est un automorphisme.

Nous avons donc bien que l'itération d'automorphisme de Frobenius est un automorphisme de $\mathbb{F}_{p^n}$ ∎

En fait il y en a exactement n automorphismes de $\mathbb{F}_{p^n}$, mais la preuve utilise des outils qui dépasse largement le cadre de cette exposé. Il est, cependant, possible de trouver une preuve dans [4] à la page 101.

Définition 12 : Soit K un corps commutatif et L une extension de K. Le **groupe de Galois** noté $Gal(L, K)$ est l'ensemble des automorphisme de L pour lesquels les éléments de K sont invariant.

Exemple : Par la remarque au bas du théorème 4 et par la proposition 2, $Gal(\mathbb{F}_{p^n}, \mathbb{F}_p)$ est l'ensemble des n itérations de l'automorphisme de Frobenius $(Id, F, F^2, \cdots, F^{n-1})$.

Théorème 5 : Soit $\mathbb{F}_p$ un corps fini de caractéristique p premier et soit $P(x) \in \mathbb{F}_p[x]$ irréductible dans $\mathbb{F}_p$ de degré n alors $\mathbb{F}_p[x]/\langle P(x)\rangle \simeq \mathbb{F}_{p^n}$.

Nous allons maintenant construire un corps à 8 éléments à partir d'un corps à 2 éléments. Prenons le corps à 2 éléments $\mathbb{Z}/2\mathbb{Z}$ et le polynômes x^3+x+1, irréductible dans $\mathbb{Z}/2\mathbb{Z}$.

Comme $\deg(x^3+x+1) = 3$, il suffit de voir que x^3+x+1 n'a pas de racines dans $\mathbb{Z}/2\mathbb{Z}$. Nous avons alors :

$$1^3+1+1 = 3 \equiv 1 \mod 2 \not\equiv 0 \mod 2 \text{ et } 0^3+0+1 = 1 \not\equiv 0 \mod 2.$$

Soit α une racine de $x^3+x+1=0$ dans $\mathbb{F}_8$.
Puisque $\alpha^3+\alpha+1=0$, nous avons alors :

$$\alpha = \alpha,$$

$$\alpha^2 = \alpha^2,$$

$$\alpha^3 = -\alpha - 1 = \alpha + 1, \text{ car } -1 \equiv 1 \mod 2,$$

$$\alpha^4 = \alpha(\alpha+1) = \alpha^2 + \alpha,$$

$$\alpha^5 = \alpha(\alpha^2+\alpha) = \alpha^3 + \alpha^2 = \alpha^2 + \alpha + 1,$$

$$\alpha^6 = \alpha(\alpha^2+\alpha+1) = \alpha^3 + \alpha^2 + \alpha = \alpha^2 + 2\alpha + 1 = \alpha^2 + 1,$$

$$\alpha^7 = \alpha(\alpha^2+1) = \alpha^3 + \alpha = 2\alpha + 1 = 1.$$

Nous avons que $\{0, 1, \alpha, \alpha^2\alpha^3, \alpha^4, \alpha^5, \alpha^6\}$ est clairement fermé pour le produit. De plus il suffit de faire la table d'addition pour voir qu'elle l'est également pour l'addition. Les éléments neutre 0 et 1 sont présent, nous avons donc bien un corps à 8 éléments.

Nous pouvons également le voir comme un espace vectoriel de dimension 3 sur $\mathbb{Z}/2\mathbb{Z}$ engendré par $\{1, \alpha, \alpha^2\}$.

Pour finir, voici un critère de conservation dans une extension de l'irréductibilité d'un polynôme.

Théorème 6 : Soit K un corps L une extension de K. Soit $P \in K[x]$ un polynôme irréductible sur K de degré n. Si le degré de l'extension L, disons q, est premier avec n alors P est irréductible sur L.

La preuve de ce théorème utilise des outils qui dépasse le cadre de cette exposé. Il est, cependant, possible de trouver une preuve dans [3] à la page 79.

Références

[1] Kostrikin, *Introduction à l'algèbre.*

[2] Martin Aigner, Günter M.Ziegler *Raisonnements divins.*

[3] Daniel Pellerin, *Cours d'algèbre.*

[4] Pierre Samuel, *Théorie algébrique des nombres.*