Arithmétique et applications, combinatoire et graphes

Cours No. 1, Corps finis

Rappels :

Groupe : Un *groupe* est un ensemble G muni d'une opération binaire associative $*$ admettant un élément neutre e tel que pour chaque élément x de l'ensemble, il existe un élément y, appelé *élément symétrique*, vérifiant $x * y = y * x = e$. Si pour tout $x, y \in G$ on a $x * y = y * x$ on dit que le groupe est *commutatif* ou *abélien*.

Exemples: 1. $(\mathbf{Z}, +)$, l'ensemble des entiers muni de l'addition.

2. $(\mathbf{Z}/k\mathbf{Z}, +)$, l'ensemble des entiers modulo k muni de l'addition.

3. $((\mathbf{Z}/p\mathbf{Z})^*, \cdot\,)$, l'ensemble des entiers modulo un nombre premier p privé de 0 muni de la multiplication.

4. $(\mathbf{C}, +)$, l'ensemble des nombres complexes muni de l'addition.

5. $(\mathbf{C}^*, \cdot\,)$, l'ensembles des nombres complexes privés de 0 muni de la multiplication.

6. D_4, le groupe diédral qui consiste des 8 rotations et reflexions du carré muni de composition comme opération binaire.

7. S_n, le groupe de $n!$ permutations de n objets muni de composition comme opération binaire.

8. A_p, l'ensemble des fonction $f(x) = ax + b$ avec $a \in (\mathbf{Z}/p\mathbf{Z})^*$ et $b \in \mathbf{Z}/p\mathbf{Z}$ (p premier) muni de composition comme opération binaire.

Parmi ces groupes, lequels sont commutatifs ?

Groupe quotient : Soit G un groupe qu'on suppose abélien et soit H un sous-groupe de G. On écrit $*$ pour la multiplication dans G et y^{-1} pour l'élément symétrique de y. Alors la relation (*équivalence modulo* H)

$$x \sim y \qquad \Leftrightarrow \qquad y^{-1} * x \in H\,,$$

est une relation d'équivalence sur G. La classe d'équivalence de $y \in G$ est

$$y * H = \{y * h : h \in H\}\,.$$

Par exemple, si $G = \mathbf{Z}$, $*$ est l'opération d'addition $+$ et $H = n\mathbf{Z}$, alors

$$x \sim y \qquad \Leftrightarrow \qquad x - y \in n\mathbf{Z}\,.$$

La classe de $y \in \mathbf{Z}$ est $y + H = y + n\mathbf{Z} = \{y + nk : k \in \mathbf{Z}\}$.

On écrit G/H pour l'ensemble des classes d'équivalence ; il s'agit d'un groupe. Si on note $\overline{y}$ pour la classe $y * H$, on a

$$\overline{xy} := \overline{x * y} \qquad \text{et} \qquad \overline{y}^{-1} := \overline{y^{-1}}\,.$$

Le cardinal $|G/H|$ de G/H s'appelle *l'indice de H dans G*. Le cardinal $|G|$ s'appelle *l'ordre de G*.

Théorème (Lagrange) : Soient G un groupe fini (abélien) et K, H deux sous-groupes tels que $K \subset H$. On a

$$|G/K| = |G/H| \times |H/K|\,.$$

En particulier, pour tout sous-groupe H de G on a $|G| = |G/H| \times |H|$.

Soit G un groupe fini; *l'ordre* d'un élément $a \in G$ est le plus petit entier n tel que $a^n = a * a * \cdots * a = e$ où e est l'élément neutre. En appliquant le théorème de Lagrange au sous-groupe $H =< a >$ engendré par a : $H = \{e, a, a^2, a^3, \ldots\}$, on obtient le corollaire:

Corollaire : *L'ordre de tout élément de G divise le cardinal de G.*

Groupe cyclique : Il s'agit d'un groupe G engendré par un seul élément : il existe $a \in G$, tel que $G =< a >$.

Anneau : Un *anneau* est un groupe abélien A noté additivement muni d'une loi de multiplication $A \times A \to A$, $(a, b) \mapsto ab$ vérifiant les propriétés suivantes :

- il existe un élément $1 \in A$ tel que pour tout $a \in A$, $1a = a1 = a$ (élément neutre pour la multiplication) ;
- pour tous a, b et c dans A, $(ab)c = a(bc)$ (associativité) ;
- pour tous a, b et c dans A, $a(b + c) = ab + ac$ et $(b + c)a = ba + ca$ (distributivité de la multiplication sur l'addition).

Remarque : Ce qu'on vient de définir est *un anneau unitaire*, car il possède l'élément neutre 1 pour la multiplication – on peut, plus généralement, étudier des anneaux qui ne contient pas 1.

Anneau commutatif : pour tous a et b dans A, $ab = ba$ (commutativité).

Anneau intègre : $ab = 0 \Rightarrow a = 0$ ou $b = 0$.

Anneau euclidien : il s'agit d'un anneau commutatif intègre A pour lequel il existe une application $\delta : A^* \to \mathbf{N}$, appelée *jauge* (ou parfois *stathme*) vérifiant les deux propriétés suivantes :

- $\forall\ a, b \in A^*,\ \delta(ab) \geq \max\{\delta(a), \delta(b)\}$;

• $\forall\ a, b \in A^*,\ b \neq 0,\ \exists\ q, r \in A$ t.q. $a = bq + r$ et $r = 0$ ou $\delta(r) < \delta(b)$.

Exemples : • L'anneau $\mathbf{Z}$ des entiers est un anneau euclidien avec $\delta(x) = |x|$.

• L'anneau $\mathbb{K}[x]$ des polynômes en une variable est euclidien, avec $\delta(P(x)) =$ degré de P.

Idéal : On appelle *idéal* d'un anneau commutatif A tout sous-groupe (pour l'addition) $I \subset A$ tel que pour tout $a \in I$ et tout $x \in A$, $xa \in I$. Parfois on utilise la notation $I \lhd R$ pour indiquer que I est un idéal dans A.

Anneau quotient : Soit A un anneau commutatif et I un idéal de A. On peut définir une relation d'équivalence sur A : $x \sim y \Leftrightarrow x - y \in I$. On note l'ensemble des classes d'équivalence par A/I : il s'agit de *l'anneau quotient*. On peut munir A/I de la structure d'un anneau comme suite. Soit $x + I := \{x + r : r \in I\}$ la classe d'équivalence qui contient x ; alors on définit:

$$(x + I) + (y + I) := (x + y) + I \qquad \text{et} \qquad (x + I) \cdot (y + I) = (x \cdot y) + I\,.$$

Dans la suite on écrit $\overline{x}$ pour la classe $x + I$.

Exercice : montrer que ces opérations sont bien définies et donnent à A/I la structure d'un anneau.
Exemple : $n\mathbf{Z}$ est un idéal de l'anneau $\mathbf{Z}$. Alors l'anneau quotient $\mathbf{Z}/n\mathbf{Z}$ est l'ensemble de classes de congruences modulo n.

Caractéristique d'un anneau : Soit A un anneau commutatif et soit c l' homomorphisme :

$$\begin{array}{rccc} c: & \mathbf{Z} & \to & A \\ & n & \mapsto & n \cdot 1 \end{array}$$

Alors $c(\mathbf{Z})$ est un sous-anneau de A et $\ker c$ est un idéal de $\mathbf{Z}$. Deux cas peuvent se présenter :

1. Soit c n'est pas injective, et donc son noyeau est un idéal non-trivial dans $\mathbf{Z}$, nécessairement de la forme $\ker c = q\mathbf{Z}$ et dans ce cas $c(\mathbf{Z})$ est isomorphe à $\mathbf{Z}/q\mathbf{Z}$.
2. Soit c est injective et $\ker c = \{0\}$. Dans ce cas A contient un sous-anneau infini isomorphe à $\mathbf{Z}$. on pose dans ce cas $q = 0$.

Définition : l'entier q s'appelle la *caractéristique* de l'anneau A et sera notée $car(A)$.

Corps: Un *corps* est un anneau A tel que $A \setminus \{0\}$ (0 l'élément neutre pour l'addition) est un groupe par rapport à la multiplication. Il y a une différence culturelle dans la

définition ! En France un corps n'est pas nécessarairement commutatif, dans les pays anglophones on comprend la condition de commutativité. De toute manière on a

Théorème de Wedderburn : Tout corps fini est commutatif.

(dans les pays anglophones ce théorème affirme : tout anneau intègre fini est un corps et en particulier commutatif).

Idéal maximal : Soit A un anneau commutatif. On dit qu'un idéal I de A est *maximal* si $I \neq A$ et si les seuls idéaux de A contenant I sont A et I.
Exemples: • Les idéaux de $\mathbf{Z}$ sont de la forme $n\mathbf{Z}$ avec $n \in \mathbf{Z}$; si n divise m, alors $m\mathbf{Z} \subset n\mathbf{Z}$. Par suite, les idéaux maximaux de Z sont les idéaux $p\mathbf{Z}$, où p est un nombre premier.

• Si $\mathbb{K}$ est un corps, les idéaux maximaux de l'anneau $\mathbb{K}[x]$ de polynômes en x sont les idéaux engendrés par un polynoôme irréductible.

Théorème : Soit A un anneau commutatif. Un idéal I de A est maximal si et seulement si l'anneau A/I est un corps.

Modèle d'un corps fini : $\mathbf{Z}/p\mathbf{Z}$ est un corps fini pour tout nombre premier p. On considère l'anneau euclidien $(\mathbf{Z}/p\mathbf{Z})[x]$. Soit $f(x) \in (\mathbf{Z}/p\mathbf{Z})[x]$ irréductible de degré n et soit $I = (f(x))$ l'idéal engendré par $f(x)$. Alors $(\mathbf{Z}/p\mathbf{Z})[x]/I$ est un corps. Chaque élément de $(\mathbf{Z}/p\mathbf{Z})[x]/I$ est une classe d'équivalence de la forme $g(x)+I$. Par la division euclidienne, on peut écrire

$$g(x) = a(x)f(x) + r(x)$$

où le reste $r(x)$ est de degré $< n$ et par suite

$$g(x) + I = r(x) + I\,.$$

Il s'ensuit que les éléments de $(\mathbf{Z}/p\mathbf{Z})[x]/I$ sont en corréspondance avec les polynômes $r(x)$ à coefficients dans $\mathbf{Z}/p\mathbf{Z}$ tel que $\deg r(x) < n$. Il y a p possibilités pour chaque coefficient et donc p^n tels polynômes. On voit alors que ce corps contient p^n éléments.

Remarque : Si $\deg f(x) = 2$, pour montrer que $f(x)$ est irréductible, il suffit de vérifier que $f(a) \neq 0$ pour tout $a \in \mathbf{Z}/p\mathbf{Z}$ (Exercice : pourquoi ?)

Théorème : Tout corps fini est de caractéristique un nombre premier p et possède p^n éléments où $n \in \mathbf{N}^*$.

Preuve : Soit K un corps fini et soit H le sous-groupe additif engenré par 1. Supposons que $|H| = mn$ pour des entiers positifs $m, n \neq 1$. Alors $0 = (mn)1 = (m1)(n1)$, ce

qui contredit le fait que K est un corps (donc intègre). D'où $|H| = p$ pour un nombre premier p et $H = \mathbf{Z}/p\mathbf{Z}$. Il s'ensuit que K est un espace vectoriel sur H, et puisque K est fini il possède une base avec un nombre fini d'éléments n disons. L'ordre de K est le nombre de combinaisons linéaires des éléments de la base : p^n.

Théorème (Existence et unicité des corps finis) : Soit $q = p^n$ où p désigne un nombre premier et $n \in \mathbf{N}^*$. Il existe un corps à q éléments et ce corps est unique à isomorphisme près.

Définition : Le corps fini à q éléments est noté $\mathbb{F}_q$ ou $GF(q)$. C'est le *corps de Galois d'ordre q*.

Remarque : On omet la preuve du théorème, mais en fait $\mathbb{F}_q = \{x \in K : x^q - x = 0\}$ où K désigne une clôture algébrique du corps $\mathbf{Z}/p\mathbf{Z}$.

Théorème : Soit K un corps fini. Alors le groupe multiplicatif K^* est cyclique.

Preuve : Clairement K^* est un groupe multiplicatif commutatif. Soit n l'ordre de ce groupe est soit $n = p_1^{n_1} p_2^{n_2} \cdots p_t^{n_t}$ la décomposition de n en facteurs premiers. Soit S_i un sous-groupe d'ordre $p_i^{n_i}$ pour chaque $i = 1, \ldots, t$ (dont l'existence est assuré par le théorème de Sylow). Soit $k_i = p_i^{n_i - 1}$. S'il existe un i tel que S_i n'est pas cyclique, alors $a^{k_i} = 1$ pour tout $a \in S_i$. Mais dans ce cas $f(x) = x^{k_i} - 1$ a $p_i^{n_i}$ racines dans K, une contradiction (car il s'agit d'un polynôme de degré $p_i^{n_i - 1}$). Il s'ensuit que chaque S_i est cyclique avec un générateur a_i. Soit $b = a_1 a_2 \cdots a_t$. Puisque l'ordre de b est l'ordre de K^*, l'élément b est un générateur de K^*.

Définition : On appelle *élément primitif de* $\mathbb{F}_q$ tout générateur du groupe multiplicatif $\mathbb{F}_q^*$.

Corollaire : Toute extension finie d'un corps fini $\mathbb{F}_q$ est une extension simple, i.e. de la forme $\mathbb{F}_q(\alpha)$.

Preuve : Si $\mathbb{F}_q \subset \mathbb{F}_r$ et si α est un élément primitif de $\mathbb{F}_r$, alors $\mathbb{F}_r^* = \{1, \alpha, \alpha^2, \ldots, \alpha^{r-1}\}$ donc $\mathbb{F}_r = \mathbb{F}_q(\alpha)$.

Corollaire : Pour tout entier $n \geq 1$ il existe au moins un polynôme irréductible de degré n dans $\mathbb{F}_q[x]$.

Preuve : Soit α un élément primitif de $\mathbb{F}_{q^n}$. On a $\mathbb{F}_{q^n} = \mathbb{F}_q(\alpha)$. Le polynôme minimal f de α dans $\mathbb{F}_q[x]$ est irréductible, et de degré n puisque $\mathbb{F}_q(\alpha)$ est isomorphe à $\mathbb{F}_q[x]/(f)$

et $\dim_{\mathbb{F}_q} \mathbb{F}_q[x]/(f) = \deg f$ (*polynôme minimal* est le polynôme unitaire de plus petit degré qui annulle α – voir ci-dessous).

Polynôme minimal : Une *extension* d'un corps K est un corps L qui contient K comme sous-corps. Un élément de L qui est une racine d'un polynôme non nul sur K est dit *algébrique* sur K. Si tout élément de L est algébrique sur K on dit que l'extension est algébrique. Le *polynôme minimal* d'un élément algébrique d'une extension de K est le polynôme unitaire de degré minimal parmi les polynômes à coefficients dans le corps de base K qui annulle l'élément. Il s'agit d'un polynôme irréductible.

Exemple : On considère $\mathbb{F}_3 = \mathbf{Z}/3\mathbf{Z}$. Le corps $L = \{a + b\sqrt{2} : a, b \in \mathbb{F}_3\}$ est une extension algébrique de $\mathbb{F}_3$ – vérifier cette affirmation. On remarque que $L \cong \mathbb{F}_{3^2}$. Le polynôme minimal de $\sqrt{2}$ est $x^2 + 1 \in \mathbb{F}_3[x]$. Le polynôme $x^4 + 2 \in \mathbb{F}_3[x]$ anulle $\sqrt{2}$ mais il n'est pas minimal.

Racines primitives, polynômes primitifs : Un élément primitif d'un corps fini est un générateur de son groupe muliplicatif. Le polynôme minimal d'un élément primitif est un *polynôme primitif*. Plus précisamment, si on considère le corps fini $\mathbb{F}_{p^n}$, un polynôme irréductible $f(x)$ avec coefficients dans $\mathbf{Z}/p\mathbf{Z}$ est un polynôme primitif si son degré est n et s'il présente une racine $\alpha \in \mathbb{F}_{p^n}$ telle que $\{0, 1, \alpha, \alpha^2, \ldots, \alpha^{p^n-2}\} = \mathbb{F}_{p^n}$. Il existe toujours un polynôme primitif de degré n.

Exemple : Dans l'exemple ci-dessus, l'élément $\sqrt{2}$ n'est pas primitif dans L, mais $1+\sqrt{2}$ l'est. Le polynôme $x^2 + x + 2$ est primitif pour cet élément.

Une autre façon de dire la même chose : un polynôme $f(x)$ à coefficients dans $\mathbb{F}_p$ (p premier) est primitive si $f(x)$ est irréductible et si $\overline{x}$ est un générateur du groupe cyclique K^* où $K = \mathbb{F}_p[x]/(f(x))$. En effet $\overline{x}$ est racine de $f(x)$ dans K : $f(\overline{x}) = \overline{0}$.

Exemple : On poursuit le même exemple. Le corps $K = \mathbb{F}_3[x]/(x^2 + x + 2)$ s'identifie avec $\mathbb{F}_{3^2}$ qui s'identifie avec L. On vérifie comme exercice que $\overline{x}$ engendre le groupe multiplicatif K^*. On peut alors en déduire un isomorphisme entre K et L en remarquant que $K^* =< \overline{x} >$ et $L^* =< 1 + \sqrt{2} >$. En effet, on identifie $\overline{x}$ avec $1 + \sqrt{2}$.

Remarque : Un polynôme irréductible de degré n sur le corps $\mathbb{F}_2$ est primitif si l'ordre de $\overline{x}$ (l'ordre de α est le plus petit entier m tel que $\alpha^m = 1$) est $2^n - 1$. Par exemple, le polynôme $x^2 + x + 1$ est primitive car il est irréductible et l'ordre de $\overline{x}$ dans $\mathbb{F}_2[x]/(x^2 + x + 1)$ est $3 = 2^n - 1$: $x^3 = x(x^2) = x(x + 1) = x^2 + x = x + x + 1 = 1$ (mod $x^2 + x + 1$).

Trouver l'élément symétrique multiplicatif dans un corps fini – l'algorithme d'Euclide-Bézout : Soit A un anneau euclidien et soit $a, b \in A$ non-nuls. Alors il existe un plus grand commun diviseur (pgcd) d de a et b qui s'exprîme comme $d = au + bv$ (l'équation de Bézout) pour $u, v \in A$. Le cas lorsque $A = \mathbf{Z}$ est typique :

Exemple : On calcule le pgcd c de 81 et 75 et on résout $81x + 75y = c$.

etape						
1						r_2
					$\swarrow$	$= 75$
2	81	$=$	q_2	75	$+$	r_3
		$\swarrow$	$= 1$		$\swarrow$	$= 6$
3	75	$=$	q_3	6	$+$	r_4
		$\swarrow$	$= 12$		$\swarrow$	$= 3$
4	6	$=$	q_4	3	$+$	r_5
			$= 2$			$= 0$

Dès que le reste égale 0 le pgcd est donné par le reste précedant, en ce cas 3. Pourquoi 3 est le pgcd ? D'abord si on remonte le fil on voit que $3|81$ et $3|75$; d'autre part, en descendant le fil on voit que si $c|81$ et $c|75$ alors $c|r_3$ ... $c|3$.

Pour résoudre l'équation de Bézout dans cet exemple on peut remonter le fil :

$$\begin{aligned} 3 &= 75 - 12 \times 6 = 75 - 12 \times (81 - 75) \\ &= -12 \times 81 + (1 + 12) \times 75 = -12 \times 81 + 13 \times 75\,. \end{aligned}$$

Afin de construire un algorithme, on explicite les termes généraux de cette procédure:

$$(1) \qquad r_{k-1} = q_k r_k + r_{k+1} \qquad \text{et} \qquad \begin{cases} x_{k+1} &= x_{k-1} - q_k x_k \\ y_{k+1} &= y_{k-1} - q_k y_k \end{cases}$$

qui sont définies de telle sorte que

$$(2) \qquad ax_k + by_k = r_k\,.$$

Pour démarrer un algorithme il faut des conditions initiales:

$$r_1 = a, \quad q_1 \text{ pas defini}, \quad x_1 = 1, \quad y_1 = 0 \quad \text{afin que } a \times x_1 + b \times y_1 = r_1\,;$$

$$r_2 = b, \quad q_2 \text{ a trouver}, \quad x_2 = 0, \quad y_2 = 1 \quad \text{afin que } a \times x_2 + b \times y_2 = r_2\,.$$

Afin de trouver q_2 on résout:

$$(3) \qquad r_1 = q_2 r_2 + r_3 \qquad \leftrightarrow \qquad a = q_2 b + r_3 \qquad (k = 2)\,.$$

On vérifie pour x_3 et y_3 :

$$x_3 = x_1 - q_2 x_2 = 1 - q_2 \times 0 = 1 \qquad y_3 = y_1 - q_2 y_2 = 0 - q_2 \times 1 = -q_2 \,;$$

alors : $ax_3 + by_3 = r_3 \quad \leftrightarrow \quad a \times 1 - b \times q_2 = r_3$. C'est bien l'équation (3) .

On vérifie pour x_4 et y_4 :

$$x_4 = x_2 - q_3 x_3 = 0 - q_3 \times 1 = -q_3 \qquad y_4 = y_2 - q_3 y_3 = 1 + q_3 \times q_2 \,;$$

alors : $ax_4 + by_4 = r_4 \quad \leftrightarrow \quad -a \times q_3 + b \times (1 + q_2 q_3) = r_4$. Mais

$$r_2 = q_3 r_3 + r_4 \quad \leftrightarrow \quad b = q_3(r_1 - q_2 r_2) + r_4 \quad \leftrightarrow \quad b(1 + q_3 q_2) - a q_3 = r_4 \,,$$

comme il le faut (car $r_1 = a$ et $r_2 = b$).

On montre l'étape général par récurrence : on suppose (1) et (2) vérifées jusqu' à k et on montre que, avec les définitions (1), l'équation (2) est vérifiée pour $k+1$: (i) l'équation (2) est bien vérifié pour $k = 1, 2$ (et même pour $k = 3, 4$) ; (ii) étape $k+1$:

$$\begin{aligned} & ax_{k+1} + by_{k+1} &&= r_{k+1} \\ \Leftrightarrow \quad & a(x_{k-1} - q_k x_k) + b(y_{k-1} - q_k y_k) &&= r_{k-1} - q_k r_k \\ \Leftrightarrow \quad & (ax_{k-1} + by_{k-1}) - q_k(ax_k + by_k) &&= r_{k-1} - q_k r_k \,, \end{aligned}$$

qui est vraie par l' hypothèse de récurrence.

On remarque que l'algorithme s'arrête car en chaque étape le reste r_k diminue strictement et il est borné inférieurement par 0.

L' algorithme :

D'abord on construit un algorithme pour la division euclidienne ; on note que dans un algorithme, pour exprîmer le prochain étape a_{i+1} en fonction de a_i on écrit (en prenant l'exemple ci-dessous) $a_i := a_i - b$ plutôt que $a_{i+1} = a_i - b$, ou parfois $a_i \leftarrow a_i - b$:

Entrée : a, b des nombres naturels avec b non-nul

Sortie : q et r tels que $a = qb + r$ avec $0 \le r < b$

Initialisation : $a_0 = a$

tant que $a_i \ge b$ *faire*

$a_i := a_i - b \quad (= a - (i+1)b)$

fin tant que

$a_i < b$ *alors retourner* $q = ib$ et $r = a - ib$

fin

On note cet algorithme par $\delta(a,b)$ et on écrit $(q,r)=\delta(a,b)$.

L'algorithme d'Euclide-Bézout peut s' érire comme suite :

Entrée : a, b des nombres naturels non nuls

Sortie : r nombre naturel et x, y des entiers tels que $r = \text{pgcd}\,(a,b)$ et $r = ax + by$

Initialisation : $r_1 = a$, $x_1 = 1$, $y_1 = 0$, $r_2 = b$, $x_2 = 0$, $y_2 = 1$,

tant que $r_{k+1} \neq 0$ *faire*

$(q_k,\, r_{k+1}) = \delta(r_{k-1},\, r_k)$

$(x_k,\, y_k) := (x_{k-1} - q_k x_k,\, y_{k-1} - q_k y_k)$

fin tant que $r_{k+1} = 0$ *alors retourner* $r = r_k$, $x = x_k$, $y = y_k$

fin

On considère un corps fini $K = (\mathbf{Z}/p\mathbf{Z})[x]/(f)$ pour un polynôme irréductible $f(x)$ dans $(\mathbf{Z}/p\mathbf{Z})[x]$. Pour $g(x) \in (\mathbf{Z}/p\mathbf{Z})[x]$ on écrit $\overline{g} = \overline{g}(x)$ pour son image dans K. Pour $\overline{g} \in K$ non-nul on veut trouver un élément $\overline{u} \in K$ tel que $\overline{g}\,\overline{u} = \overline{1}$. On note d'abord que $(\mathbf{Z}/p\mathbf{Z})[x]$ est euclidien. Puisque f est irréductible, il s'ensuit que $\text{pgcd}(g,f) = 1$. Par suite il existe des polynômes $u(x), v(x) \in (\mathbf{Z}/p\mathbf{Z})[x]$ tel que

$$u(x)g(x) + v(x)f(x) = 1\,,$$

et par conséquence $\overline{u}\,\overline{g} = \overline{1}$. Pour trouver $u(x)$ on applique l'algorithme d'Euclide-Bézout:

$$\begin{aligned} f(x) &= u_1(x)g(x) + r_1(x) \\ g(x) &= u_2(x)r_1(x) + r_2(x) \\ r_1(x) &= u_3(x)r_2(x) + r_3(x) \\ \cdots &\quad \cdots \end{aligned}$$

Exemple de travail : Soit $K = (\mathbf{Z}/3\mathbf{Z})[x]/(f)$ où $f = x^2 + x + 2$. D'abord on démontre que f est irréductible en vérifiant que $f(a) \neq 0$ pour tout $a \in \mathbf{Z}/3\mathbf{Z}$. Combien d'éléments y-a-t-il dans K ? Expliciter les éléments de K, déterminer les éléments symétriques multiplicatifs de quelques uns.

Morphisme de Fröbenius :

Lemme : Soit $\mathbb{K}$ un corps fini de caractéristique p, alors $(a+b)^{p^i} = a^{p^i} + b^{p^i}$ pour tout $a, b \in \mathbb{K}$ et $i \in \mathbf{N}^*$.

Preuve : On raisonne par récurrence sur i – exercice.

Corollaire : Soit $\varphi : \mathbb{F}_q \to \mathbb{F}_q$ l'application $\varphi(a) = a^p$ où $q = p^n$, alors φ et un morphisme de corps, appelé *morphisme de Fröbenius*.

Preuve : Il est claire que $\varphi(0) = 0$, $\varphi(1) = 1$ et $\varphi(ab) = \varphi(a)\varphi(b)$. Par le lemme ci-dessus, on a aussi $\varphi(a+b) = \varphi(a) + \varphi(b)$. Le morphisme φ est aussi injectif et donc surjectif. En effet φ^n est l'application identité.

Exemple : On considère le corps $\mathbb{F}_q$ où $q = p^2$ déduit d'un polynôme irréductible du type $x^2 - \beta$. Donc tout élément de $\mathbb{F}_q$ s'écrit sous la forme $a + bx$. Quel est le morphisme de Fröbenius ? On a

$$(a+bx)^p = a^p + b^p x^p = a + bx^p = a + b(x^2)^{(p-1)/2}x = a + b\beta^{(p-1)/2}x$$

Mais β n'est pas un carré et il s'ensuit que $\beta^{(p-1)/2} = -1(\mod p)$ (pourquoi ?), d'où

$$(a+bx)^p = a - bx\,.$$

Référence : D-J. Mercier, Corps finis, 2003, http://megamaths.perso.neuf.fr/ccof0001.pdf