Mémoire de M2 de préparation à l'agrégation

Leçon 142 : PGCD et PPCM, algorithmes de calcul. Applications.

Auteur :
Bastien Lecluse

Superviseur :
Matthieu Romagny

Table des matières

1. Introduction

Le but de ce mémoire est de généraliser certaines notions d'arithmétique, et tout particulièrement celles de pgcd et de ppcm, bien connues dans $\mathbf{Z}$, aux anneaux commutatifs unitaires. Les notions de pgcd et de ppcm sont naturelles et bien définies sur $\mathbf{Z}$. Nous verrons que la situation dans un anneau quelconque est plus délicate, et que la notion de divisibilité dans les anneaux quelconques ne garantit en rien l'existence d'un pgcd et d'un ppcm. Le but de ce mémoire va donc être de trouver l'anneau "optimal" pour faire de l'arithmétique, ie d'obtenir des anneaux "ressemblant" à $\mathbf{Z}$ arithmétiquement parlant.

Nous commencerons par quelques rappels d'arithmétique dans un anneau, puis nous définirons une certaine classe d'anneaux garantissant l'existence d'un pgcd et d'un ppcm, les anneaux factoriels. Nous constaterons que ce cadre est encore trop vague pour "imiter" l'arithmétique des entiers, nous parlerons alors des anneaux principaux, anneaux dans lesquelles nous retrouverons la quasi-totalité des propriétés arithmétiques de $\mathbf{Z}$. Pour finir, nous introduirons les anneaux dit euclidiens, permettant d'utiliser des algorithmes de calcul tels que l'algorithme d'Euclide.

Dans toute la suite et sauf indications contraires, A désignera un anneau commutatif unitaire. Les éléments neutres pour l'addition et la multiplication seront respectivement notés 0 et 1.

2. Anneau factoriel

2.1. Arithmétique dans un anneau.

On commence par quelques rappels sur la notion d'arithmétique dans un anneau, les notions fondamentales étant l'inversibilité et la divisibilité.

Définition 1. Un élément $a \in A$ est dit **inversible** s'il existe $b \in A$ tel que $ab = 1$. On note $A^\times$ l'ensemble des inversibles de A.

Proposition 2. L'ensemble $A^\times$ est un groupe pour la multiplication.

Démonstration. On vérifie aisément les axiomes de groupe : l'existence du neutre, tout élément de $A^\times$ admet un inverse dans $A^\times$, et la multiplication est bien une loi de composition interne associative sur $A^\times$. □

Définition 3. Soient $a, b \in A$. On dit que a **divise** b, noté $a \mid b$, si il existe $c \in A$ tel que $b = ac$, ou de manière équivalente, si $(b) \subset (a)$.

Définition 4. On dit que deux éléments $a, b \in A$ sont **associés** si $b \mid a$ et $a \mid b$, ou de manière équivalente que $(a) = (b)$.

Dans le cas des anneaux intègres, on dispose d'une caractérisation pratique pour affirmer que deux éléments sont associés. C'est une propriété tout à fait naturelle dans $\mathbf{Z}$.

Proposition 5. On suppose que A est intègre. Deux éléments $a, b \in A$ sont associés si et seulement si il existe $u \in A^\times$ tel que $a = bu$.

Démonstration. On se donne deux éléments a, b d'un anneau A que l'on suppose intègre. Si $a = 0$, alors le résultat est trivial, on a $a = b = 0$. Supposons que donc $a \neq 0$.
$\Longrightarrow$: on suppose que a et b sont associés. Ils existent donc deux éléments $c, c' \in A$ tels que $a = bc$ et $b = ac'$. Donc en injectant la deuxième égalité dans la première on obtient $a = ac'c$, ce qui peut s'écrire

$$a(1 - c'c) = 0.$$

Or A est intègre et $a \neq 0$, donc $c'c = 1$. Ainsi $c, c' \in A^\times$, ce qui prouve le sens direct.
$\Longleftarrow$: la réciproque est immédiate, car si il existe $u \in A^\times$ tel que $a = bu$, alors on a aussi $b = au^{-1}$. □

C'est là une première différence fondamentale entre l'arithmétique dans $\mathbf{Z}$ et l'arithmétique dans un anneau quelconque, ce qui rend cette dernière bien plus délicate. Cette proposition est en effet fausse dans un anneau non-intègre. Si $\mathbf{K}$ est un corps, considérons l'anneau $R = \mathbf{K}[X, Y, Z]/X(1 - YZ)$. Alors, si x, y, z sont les images de X, Y, Z dans R, il est clair que x divise xy et que xy divise x (car $x = xyz$). Or il n'existe pas de $u \in R^\times$ tel que $xy = ux$ (la vérification est laissée au lecteur).

On suppose désormais que A est un anneau **intègre**.

Définition 6. Soit $p \in A$. On dit que p est **irréductible** si $p \notin A^\times$ et si ses seuls diviseurs sont les inversibles et les éléments associés à p.

Remarque. Un anneau ne possède pas nécessairement d'éléments irréductibles, par exemple si c'est un corps.

Définition 7. On dit que deux éléments sont premiers entre eux si leurs seuls diviseurs communs sont les éléments inversibles.

Exemple 8. Dans l'anneau $\mathbf{Z}[i\sqrt{5}]$, les éléments 3 et $2+i\sqrt{5}$ sont premiers entre eux.

On rappelle maintenant la définition centrale de ce mémoire : les pgcd et les ppcm.

Définition 9. Soient $a, b \in A$. On dit que $d \in A$ est un pgcd de a et b si d vérifie les propriétés suivantes :
(*i*) $d \mid a$ et $d \mid b$;
(*ii*) pour tout $c \in A$ tel que $c \mid a$ et $c \mid b$, on a $c \mid d$.
On dit que $m \in A$ est un ppcm de a et b si m vérifie les propriétés suivantes :
(*i*) $a \mid m$ et $b \mid m$;
(*ii*) pour tout $c \in A$ tel que $a \mid c$ et $b \mid c$ on a $m \mid c$.
On définit aussi par récurrence le pgcd et le ppcm de $n \geqslant 2$ éléments.

Remarques.
1. Le pgcd et le ppcm de deux éléments n'existent pas nécessairement. Par exemple, dans l'anneau $A = \mathbf{Z}[i\sqrt{5}]$, 9 et $6+3i\sqrt{5}$ n'admettent pas de pgcd, et 3 et $2+i\sqrt{5}$ n'admettent pas de ppcm. On peut trouver une démonstration de ce résultat dans [5], à la page 109.
2. S'ils existent, les pgcd et les ppcm ne sont définis qu'à un inversible près.

Comme il est délicat de travailler avec des objets pouvant ne pas exister, il va nous falloir réduire notre cadre d'étude, la classe des anneaux intègres est trop "grosse". Nous allons introduire une nouvelle classe d'anneaux assurant une décomposition en irréductibles, et par conséquent l'existence de pgcd et de ppcm.

2.2. PGCD et PPCM dans un anneau factoriel

Définition 10. On dit que A est un anneau **factoriel** si A est intègre et si tout élément non nul $a \in A$ s'écrit

$$a = up_1 \cdots p_r$$

où $u \in A^\times$, $p_1, \ldots, p_r$, et cette décomposition est unique à permutation et à inversibles près.

Exemple 11. $\mathbf{Z}$, $\mathbf{R}[X]$, $\mathbf{Q}[X_1, \ldots, X_n, \ldots]$, sont des anneaux factoriels.

On dit que $\mathcal{P}$ est un système complet de représentants des irréductibles de A (s.c.r.i) si $\mathcal{P}$ est un ensemble d'irréductibles tel que pour tout $p \in A$ irréductible, il existe un unique $q \in \mathcal{P}$ tel que p et q soient associés.

Remarque. On peut alors reformuler la définition 10 en utilisant un système de représentants des irréductibles de A, cette dernière étant particulièrement utile en pratique. Ainsi, si A est un anneau intègre et si $\mathcal{P}$ est un s.c.r.i de $\mathcal{A}$, alors A est **factoriel** si pour tout $a \in A\backslash\{0\}$, a s'écrit sous la forme

$$a = u \prod_{p \in \mathcal{P}} p^{v_p(a)},$$

où $u \in A^\times$ et où les $v_p(a)$ pour $p \in \mathcal{P}$ sont une famille d'entiers presque tous nuls. Cette écriture est de plus unique.

Remarque. L'entier $v_p(a)$ est appelé la **valuation p-adique** de a. Par convention, on pose $v_p(0) = +\infty$ pour tout $p \in \mathcal{P}$.

Exemples 12. On peut prendre comme système de représentants :

1. dans $\mathbf{Z}$ les nombres premiers positifs ;
2. dans $\mathbf{K}[X]$ (où $\mathbf{K}$ est un corps) les polynômes unitaires irréductibles.

On retrouve les propriétés classiques des valuations p-adiques d'entiers naturels, dont les démonstrations sont laissées au lecteur.

Proposition 13. Soit $\mathcal{P}$ un s.c.r.i, et soit $p \in \mathcal{P}$. Alors :

1. pour tout $a \in A$, on a $v_p(a) = +\infty$ si et seulement si $a = 0$;
2. pour tous $a, b \in A$,
$$a \mid b \iff \forall\, p \in \mathcal{P}, v_p(a) \leqslant v_p(b);$$
3. pour tous $a, b \in A$,
$$v_p(ab) = v_p(a)v_p(b).$$

Comme nous l'avons vu, l'existence d'un pgcd et d'un ppcm de deux éléments n'est pas assurée dans un anneau quelconque. C'est en revanche le cas dans les anneaux factoriels.

Proposition 14. Dans un anneau factoriel, tout couple d'éléments admet un pgcd et un ppcm.

Démonstration. Soit A un anneau factoriel, et soit $\mathcal{P}$ un s.c.r.i. de A. Soient $a, b \in A$, alors on peut écrire
$$a = u \prod_{p \in \mathcal{P}} p^{v_p(a)}, \quad b = v \prod_{p \in \mathcal{P}} p^{v_p(b)},$$
où u, v sont des éléments inversibles de A. Alors le ppcm de a et b est donné, à multiplication par un inversible près, par
$$\mathrm{ppcm}(a, b) = \prod_{p \in \mathcal{P}} p^{\sup(v_p(a), v_p(b))}.$$
De même, le pgcd de a et b est donné, à multiplication par un inversible près, par
$$\mathrm{pgcd}(a, b) = \prod_{p \in \mathcal{P}} p^{\inf(v_p(a), v_p(b))}.$$
□

Remarque. La preuve précédente nous donne de plus une formule explicite pour calculer le pgcd et le ppcm de deux éléments, à condition de connaître leur décomposition en irréductibles.

On suppose désormais que A est un anneau **factoriel**.

Corollaire 15. Pour tous $a, b \in A$, aux inversibles près on a
$$\mathrm{pgcd}(a, b) \cdot \mathrm{ppcm}(a, b) = ab.$$

Démonstration. Cela découle directement de la preuve de la proposition 14. □

Proposition 16. Soient $a, b \in A$ et m un ppcm de a et b. Alors $(a) \cap (b) = (m)$.

Démonstration. Soit $c \in A$. Alors par définition du ppcm

$$c \in (m) \iff m \,|\, c \iff a \,|\, c \text{ et } b \,|\, c \iff c \in (a) \cap (b).$$

□

Cette existence de la décomposition en irréductibles dans les anneaux factoriels permet de retrouver une grande partie des théorèmes classiques d'arithmétique dans $\mathbf{Z}$, notamment le lemme d'Euclide (lemme 17) et le théorème de Gauss (théorème 18). On fera attention au fait que les démonstrations ne s'appuient en revanche pas sur la relation de Bézout, qui comme nous le verrons, est fausse dans les anneaux factoriels.

Lemme 17 (d'Euclide.)**.** Soit p un élément irréductible de A. Alors pour tous $a, b \in A$,

$$p \,|\, ab \Rightarrow p \,|\, a \text{ ou } p \,|\, b.$$

Démonstration. Soit $\mathcal{P}$ un s.c.r.i de A contenant p. En vertu de la proposition 13, l'hypothèse de l'énoncé se retraduit alors par $1 \leqslant v_p(a) + v_p(b)$. Or $v_p(a), v_p(b) \in [\![0, +\infty]\!]$, donc nécessairement $v_p(a) \leqslant 1$ ou $v_p(b) \leqslant 1$, donc $p \,|\, a$ ou $p \,|\, b$. □

Théorème 18 (de Gauss.)**.** Soient $a, b, c \in A$. Si a divise bc et si a est premier avec b, alors a divise c.

Démonstration. Par hypothèse a divise bc, il existe donc $d \in A$ tel que $ad = bc$. On fixe $\mathcal{P}$ un s.c.r.i de A. Soit $p \in \mathcal{P}$ quelconque, on va montrer que $v_p(a) \leqslant v_p(c)$. Par la proposition 13, on sait que

$$v_p(a) + v_p(d) = v_p(b) + v_p(c) = 0,$$

et

$$v_p(a) = 0 \text{ ou } v_p(b) = 0$$

car a et b sont premiers entre eux. Si $v_p(a) = 0$, alors comme $v_p(c) \in \mathbf{N} \cup \{+\infty\}$ on a clairement $v_p(a) \leqslant v_p(c)$. Supposons donc $v_p(a) \geqslant 1$. Alors $v_p(b) = 0$, et donc

$$v_p(a) \leqslant v_p(a) + v_p(d) = v_p(b) + v_p(c) = v_p(c).$$

Ceci étant vrai pour tout $p \in \mathcal{P}$, a divise c, ce qui achève la démonstration. □

Remarque. On vérifie aisément que deux éléments a et b sont premiers entre eux si et seulement si 1 est un pgcd de a et b.

Application : les équations diophantiennes. Ces nouveaux outils étant à disposition, on peut s'intéresser à un exemple classique d'équations en arithmétique dans $\mathbf{Z}$, les équations diophantiennes. Nous allons essayer de généraliser ces équations dans un cadre d'anneau plus général. Soient $a, b \in A$ deux éléments non nuls, que l'on suppose premiers entre eux. On considère l'équation

$$ua - vb = 1 \tag{E}$$

d'inconnues $u, v \in A$. On suppose que l'on dispose d'une solution particulière $(u_0, v_0) \in A^2$ de E. Alors les solutions de (E) sont les couples $(u_0 + kb, v_0 + ka)$ où $k \in A$. En effet, on vérifie facilement qu'un tel couple est solution. Réciproquement, si $(u, v) \in A^2$ est une solution de (E), alors par soustraction on a

$$(u - u_0)a - b(v - v_0) = 0, \tag{1}$$

donc a divise $b(v-v_0)$. Or a et b sont premiers entre eux, donc par le théorème de Gauss (théorème 18), a divise $v-v_0$. Il existe donc $k \in A$ tel que $ak = v - v_0$, soit $v = ak + v_0$. En injectant cette égalité dans l'égalité (1), il vient $(u-u_0)a - abk = 0$. Or a est non nul et A est intègre, donc $u = u_0 + bk$.
Les questions naturelles nous venant à l'esprit sont alors :

— Sous quelles conditions existe-t-il une solution particulière ?
— Si elle existe, comment la trouver ?

La réponse (partielle) à ces questions, est le théorème de Bézout, bien connu dans $\mathbf{Z}$. En effet, dans $\mathbf{Z}$, ce théorème nous affirme que pour tous $n, m \in \mathbf{Z}$,

$$\text{pgcd}(n,m) = \pm 1 \iff \exists\,(u,v) \in \mathbf{Z}^2,\ un - vm = 1.$$

Donc dans $\mathbf{Z}$ l'équation (E) admet toujours une solution, et donc une infinité de solutions. Le théorème de Bézout est en revanche faux dans les anneaux factoriels. On peut par exemple considérer l'anneau $\mathbf{K}[X,Y]$, où $\mathbf{K}$ est un corps, X et Y sont premiers entre eux dans $\mathbf{K}[X,Y]$ mais

$$(X) + (Y) = (X,Y) \neq (1),$$

il n'existe donc pas de polynômes $P, Q \in \mathbf{K}[X,Y]$ tels que $PX - QY = 1$. Nous allons encore une fois réduire notre cadre d'étude, et introduire une nouvelle classe d'anneaux dans lesquels le théorème de Bézout est vrai. Nous verrons que c'est le cadre "optimal", a minima du point de vue théorique, pour faire de l'arithmétique.

3. Anneaux principaux

Définition 19. Un anneau intègre A est dit **principal** si tout idéal de A est principal, ie engendré par un seul élément.

L'étude des anneaux principaux en arithmétique est motivée par la proposition suivante, dont ou pourra retrouver la démonstration dans [2] aux pages 528-529.

Proposition 20. Un anneau principal est factoriel.

La réciproque est fausse, il existe des anneaux factoriels non principaux. Par exemple si A est factoriel alors $A[X]$ est factoriel mais $A[X]$ est principal si et seulement si A est un corps. La preuve de ce résultat peut être trouvée dans [6], à la page 51.

On suppose désormais que A est un anneau **principal**.

3.1. Théorème de Bézout

Proposition 21. Soient $a, b \in A\backslash\{0\}$ et soit d un pgcd de a et b. Alors $(a) + (b) = (d)$, ce qui signifie aussi qu'il existe $u, v \in A$ tels que $ua + vb = d$.

Démonstration. On rappelle que la somme d'idéaux est la borne supérieure de ces mêmes idéaux pour l'inclusion. Par définition du pgcd, (d) est le sup (au sens de l'inclusion), des idéaux (a) et (b) dans l'ensemble des idéaux principaux de A (cela est juste une traduction de la définition 9 en termes d'idéaux). Or A est principal, tous ses idéaux sont principaux, donc (d) est le sup des idéaux (a) et (b) dans l'ensemble des idéaux de A, c'est donc $(a) + (b)$. □

Théorème 22 (de Bézout.)**.** Deux éléments $a, b \in A\backslash\{0\}$ sont premiers entre eux si et seulement si il existe $u, v \in A$ tel que $au + bv = 1$.

Comme nous l'avons vu, le théorème de Bézout est faux dans l'anneau $\mathbf{K}[X, Y]$, où $\mathbf{K}$ est un corps. Cela prouve que l'anneau $\mathbf{K}[X, Y]$ n'est pas un anneau principal.

Démonstration. Si $\text{pgcd}(a, b) = 1$ modulo $A^\times$, alors la proposition précédente affirme qu'il existe $u, v \in A$ tels que $au + bv = 1$. Réciproquement, si l'on dispose de $u, v \in A$ tels que $au + bv = 1$, alors $\text{pgcd}(a, b)$ divise $au + bv$, donc $\text{pgcd}(a, b)$ divise 1. Ainsi $\text{pgcd}(a, b) = 1$ modulo $A^\times$, ce qui prouve la réciproque du théorème. □

L'équation diophantienne (E) admet alors toujours une solution particulière si A est principal, et donc une infinité de solutions. Nous allons maintenant présenter deux applications du théorème de Bézout dans les anneaux principaux, la forme normale de Smith des matrices à coefficients dans un anneau principal et le théorème chinois.

3.2. Forme de Smith

On fixe deux entiers $m, n \in \mathbf{N}^*$. On se donne un s.c.r.i $\mathcal{P}$ de A. On dit qu'un élément $a \in A$ est normalisé si $a \neq 0$ et si $a = \prod_{p\in\mathcal{P}} p^{v_p(a)}$. On peut alors parler du pgcd normalisé et du ppcm normalisé de deux éléments.

Définition 23. Deux matrices $M, M' \in \mathcal{M}_{m,n}(A)$ sont dites **équivalentes** s'il existe $P \in \text{GL}_m(A)$ et $Q \in \text{GL}_n(A)$ telles que $M' = PMQ$.

Exemple 24. Lorsque A est un corps, deux matrices sont équivalentes si et seulement si elles ont le même rang.

Pour $r \leqslant \min(n, m)$ et $a_1, \ldots, a_r \in A$, on note $E(a_1, \ldots, a_r)$ la matrice

$$\begin{pmatrix} a_1 & & & \\ & \ddots & & 0_{r,n-r} \\ & & a_r & \\ 0_{m-r,r} & & & 0_{m-r,n-r} \end{pmatrix}.$$

Théorème 25. Soit $M \in \mathcal{M}_{m,n}(A)$. Alors il existe $r \in \mathbf{N}^*$ et $a_1, \ldots, a_r \in A$, non nuls et normalisés, vérifiant

$$a_1 \,|\, a_2 \,|\, \cdots \,|\, a_r,$$

tels que que M soit équivalente à la matrice $E(a_1, \ldots, a_r)$. De plus, l'entier r et les éléments $a_1, \ldots, a_r$ sont uniques. Cette matrice est la **forme de Smith** de M.
On a de plus que $r = \text{rg}\,(M)$ (M étant vue comme un élément de $\mathcal{M}_{m,n}(\text{Frac}(A))$), et pour tout $j \in [\![0, r]\!]$,

$$\mu_j(M) = a_1 \cdots a_j,$$

où $\mu_j(M)$ désigne le pgcd normalisé des mineurs d'ordre j de M (avec la convention $\mu_0(M) = 1$).

Nous allons pour le moment démontrer uniquement la deuxième partie du théorème (qui prouve l'unicité de la forme de Smith). Bien que le théorème reste vrai dans le cadre des anneaux principaux, nous démontrerons l'existence d'une forme de Smith plus tard dans un cadre légèrement plus restrictif. Cela nous permettra de donner une preuve algorithmique, et donc une méthode pour construire la forme de Smith d'une matrice.

Démonstration. Nous supposons que l'existence d'une forme de Smith est établie, donc que M est équivalente à la matrice $E(a_1, \dots, a_r)$. Au vu de la forme de la matrice $E(a_1, \dots, a_r)$, comme les $(a_i)_{1 \leqslant i \leqslant r}$ sont non nuls, il est clair que $r = \operatorname{rg}(E(a_1, \dots, a_r)) = \operatorname{rg}(M)$. Montrons le dernier point. On va montrer que le pgcd (normalisé) de tous les mineurs d'ordre k de M, pour $k \in [\![1, \min(m,n)]\!]$ est invariant par opérations élémentaires sur les lignes et les colonnes. On étudie les différentes opérations possibles. Soient C une matrice extraite de M d'ordre k, $a \in A$.

1. $L_i \leftarrow L_i + aL_j$.
   (a) Si $L_i, L_j \notin C$ ou si C contient uniquement L_j, alors C ne change pas (donc son déterminant non plus).
   (b) Si $L_i, L_j \in C$, $\det(C)$ est inchangé.
   (c) Si C contient uniquement L_i, le déterminant de cette nouvelle matrice est de la forme $\det(C) + a\det(C')$, où C' est une matrice de taille k obtenue par permutation des lignes d'une autre matrice extraite.
2. $L_i \leftarrow aL_i$. Le déterminant de C ne change pas ou bien est multiplié par un élément de $A^\times$.
3. $L_i \leftrightarrow L_j$.
   (a) Si $L_i, L_j \in C$ ou si $L_i, L_j \notin C$, le mineur ne change pas au signe près.
   (b) Si C ne contient qu'une seule ligne, elle est transformée en une matrice de taille k obtenue par permutation des lignes d'une autre matrice extraite.

On raisonne de même avec les colonnes. On constate alors que peu importe l'opération élémentaire effectuée, le pgcd des mineurs ne change pas. Ainsi, pour tout $j \in [\![0, r]\!]$,

$$\begin{aligned}\mu_j(M) &= \mu_j(E(a_1, \dots, a_r)) \\ &= \operatorname{pgcd}\{a_{i_1} \cdots a_{i_j} : 1 \leqslant i_1 < \cdots < i_j \leqslant r\} \\ &= a_1 \cdots a_j\end{aligned}$$

car $a_1 \,|\, a_2 \,|\, \cdots \,|\, a_r$. En particulier, on a

$$a_j = \frac{a_1 \cdots a_j}{a_1 \cdots a_{j-1}} = \frac{\mu_j(C)}{\mu_{j-1}(C)},$$

ce qui démontre l'unicité de la forme (normalisé) de Smith. □

Nous présenterons quelques exemples de calcul de la forme de Smith plus tard, une fois l'algorithme de construction établi. Ce théorème a plusieurs applications importantes : résolutions de systèmes, théorème de la base adaptée pour les modules, classification des groupes abéliens de type fini. On pourra trouver des démonstrations de tous ces résultats dans [2].

3.3. Théorème chinois

On commence par énoncer et démontrer le théorème chinois dans le cadre le plus général possible, celui des anneaux commutatifs unitaires. Nous verrons par la suite des applications de ce théorème dans le cadre des anneaux principaux.

Théorème 26. Soit R un anneau commutatif unitaire et soient I, J des idéaux de R tels que $I + J = R$. Pour $x \in R$, on note respectivement $\hat{x}$, $\overline{x}$ et $\mathring{x}$ les classes de x modulo $I \cap J$, I et J. Alors l'application

$$\Phi : \left| \begin{array}{ccc} R/(I \cap J) & \longrightarrow & R/I \times R/J \\ \hat{x} & \longmapsto & (\overline{x}, \mathring{x}) \end{array} \right.$$

est bien définie et est un isomorphisme d'anneaux.

Démonstration. On vérifie facilement que l'application $x \in R \longmapsto (\overline{x}, \overset{\circ}{x})$ est un morphisme d'anneaux, de noyau $I \cap J$. Par factorisation on obtient donc un morphisme injectif $\Phi : R/(I \cap J) \longrightarrow R/I \times R/J$ tel que pour tout $x \in R$, $\Phi(\hat{x}) = (\overline{x}, \overset{\circ}{x})$. Montrons que Φ est surjectif. Puisque $I + J = R$, il existe $u \in I$ et $v \in J$ tels que $u + v = 1$. Soit alors $\overline{a} \in R/I$ et $\overset{\circ}{b}$, où $a, b \in R$. On pose $x = va + ub$. On a alors

$$\begin{aligned}\Phi(\hat{x}) &= (\overline{x}, \overset{\circ}{x}) \\ &= (\overline{va} + \overline{u}\overline{b}, \overset{\circ}{u}\overset{\circ}{a} + \overset{\circ}{u}\overset{\circ}{b}) \\ &= (\overline{a}, \overset{\circ}{b})\end{aligned}$$

car $\overline{v} = \overline{1}$ et $\overset{\circ}{u} = \overset{\circ}{1}$. Ainsi Φ est surjective, c'est donc un isomorphisme. □

Remarque. Le théorème chinois se généralise au cas de $n \geqslant 2$ idéaux $I_1, \ldots, I_n$ deux à deux étrangers, i.e. tels que $I_i + I_j = A$ si $i \neq j$.

En particulier, dans un anneau principal on en déduit le corollaire suivant.

Corollaire 27. Soient $a, b \in A$ premiers entre eux. Pour $x \in A$, on note respectivement $\hat{x}$, $\overline{x}$ et $\overset{\circ}{x}$ les classes de x modulo (ab), (a) et (b). Alors l'application

$$\Phi : \left| \begin{array}{ccc} A/(ab) & \longmapsto & A/(a) \times A/(b) \\ \hat{x} & \longmapsto & (\overline{x}, \overset{\circ}{x}) \end{array} \right.$$

est un isomorphisme. Si de plus $u, v \in A$ sont tels que $au + bv = 1$, alors l'isomorphisme réciproque associe à $(\overline{x}, \overset{\circ}{y}) \in A/(a) \times A/(b)$ la classe $\hat{z} \in A/(ab)$ de $z = vbx + uay$.

Démonstration. a et b étant premier entre eux, on a $(a) + (b) = (1) = A$. Dans ce cas, $(ab) = (\mathrm{ppcm}(a, b)) = (a) \cap (b)$. On applique alors le théorème chinois avec les idéaux (a) et (b). □

Nous allons maintenant présenter deux applications du théorème chinois : une formule permettant de calculer $\varphi(n)$ connaissant la décomposition en nombres premiers de n ainsi que la résolution de systèmes de congruence. Nous verrons plus tard une autre application de ce théorème, permettant de factoriser des polynômes à coefficients dans un corps fini.

L'anneau $\mathbf{Z}/n\mathbf{Z}$ et la fonction indicatrice d'Euler. Soient p, q des entiers positifs premiers entre eux. L'anneau $\mathbf{Z}$ est principal, donc par le théorème chinois on a un isomorphisme

$$\mathbf{Z}/pq\mathbf{Z} \simeq \mathbf{Z}/p\mathbf{Z} \times \mathbf{Z}/q\mathbf{Z}.$$

Soit maintenant $n \in \mathbf{N}^*$. On écrit $n = p_1^{v_{p_1}(n)} \cdots p_r^{v_{p_r}(n)}$ où $r \in \mathbf{N}^*$ et où les p_i sont des nombres premiers deux à deux distincts. Alors par récurrence on a un isomorphisme

$$\mathbf{Z}/n\mathbf{Z} \simeq \prod_{i=1}^{r} \mathbf{Z}/p_i^{v_{p_i}(n)}\mathbf{Z}.$$

Si φ désigne la fonction indicatrice d'Euler, alors on a, en passant aux éléments inversibles,

$$\varphi(n) = \prod_{i=1}^{r} \varphi(p_i^{v_{p_i}(n)}) = \prod_{i=1}^{r} p_i^{v_{p_i}(n)-1}(p_i - 1) = n \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right).$$

Système de congruences. Soient $a, b, m, n \in A$. Si $a, b \in A$ sont premiers entre eux, alors le système de congruences d'inconnue x

$$\begin{cases} x \equiv m \pmod{(a)} \\ x \equiv n \pmod{(b)} \end{cases}$$

admet une unique solution modulo (ab). Si $au+bv = 1$, cette solution est donnée par $\Phi^{-1}((\overline{m}, \overset{\circ}{n})) = \hat{z}$, où $z = vbm + uan$. Par exemple, si $A = \mathbf{Z}$, alors le système de congruences

$$\begin{cases} x \equiv 2 \pmod{5} \\ x \equiv 4 \pmod{3} \end{cases}$$

admet des solutions, car 5 et 3 sont premiers entre eux. De plus, $5 \times 2 + 3 \times (-3) = 1$, donc l'ensemble des solutions de ce système est

$$\{22 + 15k : k \in \mathbf{Z}\}.$$

Bien que utiles en théorie, ces résultats perdent de leur intérêt en pratique car il n'existe pas, dans le cadre des anneaux principaux, de méthode ou d'algorithme permettant de déterminer une relation de Bézout entre deux éléments, ou juste de calculer leur pgcd. Cela est en revanche possible dans $\mathbf{Z}$: c'est l'algorithme d'Euclide, qui se base sur la division euclidienne. Par analogie, on va introduire une nouvelle classe d'anneaux, une classe d'anneaux possédant une division euclidienne, ce qui nous permettra d'utiliser des algorithmes de calcul.

4. Anneaux euclidiens, algorithme de calcul

Définition 28. Un anneau intègre est dit **euclidien** s'il existe une fonction $\nu : A\backslash\{0\} \longrightarrow \mathbf{N}$ telle que si $a \in A, b \in A\backslash\{0\}$, alors il existe $q, r \in A$ vérifiant $a = bq+r$, avec $\nu(r) < \nu(b)$ ou $r = 0$.

Exemples 29.
— $\mathbf{Z}$ est euclidien pour la valeur absolue ;
— si $\mathbf{K}$ est un corps alors $\mathbf{K}[X]$ est euclidien, avec $\nu = \deg$.

Les anneaux euclidiens conservent toutes les propriétés arithmétiques des anneaux principaux. C'est l'objet de la proposition suivante.

Proposition 30. Un anneau euclidien est principal.

Démonstration. Soit I un idéal de A non réduit à $\{0\}$. Montrons que I est principal. Soit $b \in I$, $n \neq 0$, tel que $\nu(b)$ soit minimal. On va montrer que $I = (b)$. Clairement $(b) \subset I$. Réciproquement, soit $a \in I$. L'élément b est non nul, donc par division euclidienne, il existe $q, r \in A$ tels que

$$a = bq + r \quad \text{avec } r = 0 \text{ ou } \nu(r) < \nu(b).$$

Or I est un idéal, donc comme $a, b \in I$, par propriété d'absorption, $r = a - bq \in I$. Par minimalité de $\nu(b)$ parmi les éléments de I, on a $\nu(r) \geqslant \nu(b)$, donc $r = 0$ et $a = bq$. Ainsi $I = (b)$, tout idéal de A est principal, donc A est principal. □

Remarque. La réciproque est fausse, l'anneau $\mathbf{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$ est un exemple d'anneau principal mais non euclidien. Une démonstration de cette assertion peut être lue dans [6].

On suppose désormais que (A, ν) est un anneau **euclidien**.

Sauf indications contraires et en l'absence d'ambiguïté, on notera tout simplement A pour (A, ν). On fixe également un s.c.r.i $\mathcal{P}$ de A, les pgcd seront implicitement les pgcd normalisés par rapport à $\mathcal{P}$ (de même pour les ppcm). Comme annoncé, l'avantage des anneaux euclidiens est qu'on dispose d'algorithmes de calcul. C'est l'objet de la prochaine section.

4.1. Algorithme d'Euclide

Lemme 31. Soient $a \in A, b \in A\backslash\{0\}$, et q et r le quotient et le reste de le division euclidienne de a par b. Alors

1. Si $a = 0$, $\text{pgcd}(a, b) = b$;
2. Sinon, $\text{pgcd}(a, b) = \text{pgcd}(b, r)$.

Démonstration. Le premier point est évident. Supposons que $a \neq 0$. Si d est un diviseur de a et b, alors d divise aussi $a - bq$, donc d divise aussi b et r. Réciproquement, si d divise b et r, on voit de la même façon que d divise b et a. Les diviseurs de a et b sont les diviseurs de b et r, donc en particulier $\text{pgcd}(a, b) = \text{pgcd}(b, r)$. □

Ce simple lemme va nous permettre, si nous disposons d'une division euclidienne, de calculer algorithmiquement le pgcd de deux éléments. Par le corollaire 15, on pourra alors aussi en déduire le ppcm de deux éléments.

Théorème 32 (algorithme d'Euclide.)**.** Soient a, b deux éléments non nuls de A. On définit une suite $(r_i)_{i\in\mathbf{N}}$ d'éléments de A par

$$\begin{cases} r_0 = a\,; \\ r_1 = b\,; \\ r_i = r_{i-2} \,\%\, r_{i-1} \quad \text{pour } i \geqslant 2 \text{ et si } r_{i-1} \neq 0\,; \end{cases}$$

où $x \,\%\, y$ désigne le reste de la division euclidienne de x par y. Alors cette suite est finie car il existe un entier $n + 1$ pour lequel $r_{n+1} = 0$, et on a alors

$$\text{pgcd}(a, b) = r_n.$$

Avant de prouver ce théorème, donnons deux exemples de son utilisation.

Exemples 33.

1. Dans l'anneau $\mathbf{Z}$, $\text{pgcd}(459, 116) = ?$. On écrit les divisions euclidiennes successives.

$$\begin{aligned} 459 &= 116 \times 3 + 111 \\ 116 &= 111 \times 1 + 5 \\ 111 &= 5 \times 22 + \boxed{1} \\ 5 &= 5 \times 1 + 0. \end{aligned}$$

   Donc $\text{pgcd}(459, 116) = 1$, ils sont premiers entre eux.

2. Dans l'anneau $\mathbf{R}[X]$, $\text{pgcd}(X^3+3X^2+X, X^3+2X) = ?$. On utilise à nouveau l'algorithme d'Euclide.

$$\begin{aligned} X^3 + 3X^2 + X &= (X^3 + 2X) \times (1) + (3X^2 - X) \\ X^3 + 2X &= (3X^2 - X) \times \left(\frac{1}{3}X - \frac{1}{9}\right) + \boxed{\frac{17}{9}X} \\ 3X^2 - X &= \left(\frac{17}{9}X\right) \times \left(\frac{27}{17}X - \frac{9}{17}\right) + 0. \end{aligned}$$

   Donc $\text{pgcd}(X^3 + 3X^2 + X, X^3 + 2X) = X$ (une fois normalisé).

Passons maintenant à la preuve du théorème.

Démonstration. Comme r_{i+1} est le reste d'une division dont le diviseur est r_i, on a soit $r_{i+1} = 0$ soit $\nu(r_{i+1}) < \nu(r_i)$. Si on suppose les r_i pour $i \in \mathbf{N}$ tous non nuls, alors la suite $(\nu(r_i))_{i\in\mathbf{N}}$ est une suite à valeurs entières, positives, et strictement décroissante, ce qui est impossible. Il existe donc bien un indice $n+1$ tel que $r_{n+1} = 0$. On a alors par le lemme 31

$$\mathrm{pgcd}(a,b) = \mathrm{pgcd}(b,r_2) = \mathrm{pgcd}(r_2,r_3) = \cdots = \mathrm{pgcd}(r_n,r_{n+1}) = \mathrm{pgcd}(r_n,0) = r_n.$$

□

Par le théorème de Bézout (théorème 22), dans un anneau principal, pour tous éléments a, b il existe des éléments u, v tels que $au + bv = \mathrm{pgcd}(a,b)$. Dans la pratique, on a très souvent besoin non seulement de connaître un pgcd mais aussi une relation de Bézout entre les éléments. Nous l'avons en effet constaté avec les résolutions de systèmes linéaires ou avec les équations diophantiennes. Le résultat suivant est une généralisation de l'algorithme d'Euclide, qui permet d'obtenir une relation de Bézout en plus du pgcd de deux éléments.

Théorème 34 (algorithme d'Euclide étendu)**.** Soient a, b deux éléments non nuls de A. On définit une suite $(r_i)_{i\in\mathbf{N}}$ de la même manière que dans l'algorithme d'Euclide. On définit aussi deux suites par

$$\begin{cases} u_0 = 1, \quad u_1 = 0, \quad \text{pour } i \geqslant 2 \text{ et si } r_{i-1} \neq 0,\ u_i = -q_{i-1}u_{i-1} + u_{i-2}\,; \\ v_0 = 0, \quad v_1 = 1, \quad \text{pour } i \geqslant 2 \text{ et si } r_{i-1} \neq 0,\ v_i = -q_{i-1}v_{i-1} + v_{i-2}\,; \end{cases}$$

où q_i est le quotient de la division euclidienne de r_{i-1} par r_i. Alors ces suites sont finies, car il existe un entier $n+1$ pour lequel $r_{n+1} = 0$, et on a alors

$$\begin{cases} \mathrm{pgcd}(a,b) = r_n\,; \\ u_n a + v_n b = \mathrm{pgcd}(a,b). \end{cases}$$

La preuve est semblable à celle de l'algorithme d'Euclide, bien que plus calculatoire. Le lecteur intéressé par les détails pourra regarder [2], aux pages 532-534, ou [7] à la page 46.

Exemples 35. En reprenant l'exemple précédent dans $\mathbf{Z}$, on a

$$\begin{aligned} 1 &= 111 - 5 \times 22 \\ &= 111 - (116 - 111) \times 22 \\ &= 111 \times 23 + 116 \times (-22) \\ &= (459 - 116 \times 3) \times 23 + 116 \times (-22) \\ &= 459 \times 23 + 116 \times (-91). \end{aligned}$$

4.2. **Forme de Smith (preuve algorithmique)**

Démonstration. On présente ici une preuve algorithme de l'existence d'une matrice $E(a_1,\ldots,a_r)$ équivalente à M. Toutes les opérations élémentaires à venir seront réalisées grâce à des matrices de transvection, de dilatation et de transposition, voir [2] pour plus de détail sur ces manipulations. Si $M = 0$, le résultat est évident. On suppose donc que $M \neq 0$. Nous allons montrer, en permutant et dilatant les lignes et colonnes de M, que cette dernière est équivalente à une matrice de la forme

$$\begin{pmatrix} a & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & M' & \\ 0 & & & \end{pmatrix},$$

où $a \in A$ est normalisé et divise tous les coefficients de M', ce qui permettra de conclure par récurrence.

Étape 1. Soit alors b un coefficient non nul de M tel que $\nu(b)$ soit minimal. On le place en haut à gauche à l'aide d'échanges de lignes et de colonnes (ie en multipliant à gauche ou à droite par des matrices de transposition).

Étape 2.

1. Si b divise tous les éléments de la première ligne et de la première colonne, on passe à **l'étape 3**.
2. Sinon, il existe au moins un élément a de la première ligne ou de la première colonne tel que b ne divise pas a. Par division euclidienne, on écrit $a = bq + b_1$, où $q, b_1 \in A$, b_1 non nul, et $\nu(b_1) < \nu(b)$. À l'aide d'opérations du type $L_i \leftarrow L_i + \alpha L_1$ et $L_i \leftarrow C_i + \alpha C_1$ et par échanges de lignes / colonnes (où $\alpha \in A$ et $i \geqslant 2$), on remplace b par b_1. On normalise ensuite b_1 grâce à des matrices de dilatation. Si tous les éléments de la première ligne et de la première colonne sont divisibles par b_1, alors on passe à **l'étape 3**. Sinon, on recommence le procédé on remplaçant b_1 par b_2, puis b_2 par b_3 ... Ce procédé s'arrête nécessairement car la suite $\nu(b), \nu(b_1), \nu(b_2), ...$ est positive et strictement décroissante.

Étape 3. On utilise des opérations sur les lignes et sur les colonnes afin de faire apparaître des zéros et obtenir une matrice de la forme

$$\begin{pmatrix} d_1 & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & M_1 & \\ 0 & & & \end{pmatrix},$$

où $d \in A$ est non nul et normalisé.

1. Si d_1 divise tous les éléments de M_1, c'est fini.
2. Sinon, il existe une ligne L_i de M_1 contenant un élément non divisible par d_1. On fait l'opération $L_1 \leftarrow L_1 + L_i$, et on recommence à **l'étape 1**. On se ramène de nouveau à une matrice de la forme
$$\begin{pmatrix} d_2 & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & M_2 & \\ 0 & & & \end{pmatrix},$$
où $b_2 \in A$ est non nul, normalisé, et $\nu(b_2) < \nu(b_1)$. De la même manière que précédemment, on réitère l'opération jusqu'à qu'un élément d_k divise tous les éléments de la matrice M_k. Ce procédé termine nécessairement car $\nu(d_1) > \nu(d_2) > \cdots \geqslant 0$.

On peut alors conclure par récurrence, on recommençant l'algorithme avec la matrice M_k.

□

Comme affirmé précédemment, le résultat reste vrai pour les anneaux principaux. La démonstration utilise des matrices de Bézout, ie des matrices comportant les coefficients de Bézout de certains couples d'éléments, au lieu d'opérations élémentaires. Nous allons maintenant détailler deux exemples.

Exemple 36. On cherche la forme de Smith de la matrice $M = \begin{pmatrix} 10 & 14 \\ 6 & 7 \end{pmatrix} \in \mathcal{M}_2(\mathbf{Z})$. On applique l'algorithme de la preuve ci-dessus. On a

$$M = \begin{pmatrix} 10 & 14 \\ 6 & 7 \end{pmatrix} \sim \begin{pmatrix} 6 & 7 \\ 10 & 14 \end{pmatrix} \sim \begin{pmatrix} 6 & 1 \\ 10 & 4 \end{pmatrix} \sim \begin{pmatrix} 1 & 6 \\ 4 & 10 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 \\ 4 & -14 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 \\ 0 & -14 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 \\ 0 & 14 \end{pmatrix}.$$

Donc la forme de Smith de M est la matrice $\begin{pmatrix} 1 & 0 \\ 0 & 14 \end{pmatrix}$. On aurait aussi pu retrouver ce résultat à l'aide des relations entre les coefficients de la forme de Smith et les mineurs de M. En effet, si on voit M comme une matrice de $\mathcal{M}_2(\mathbf{Q})$, alors $\operatorname{rg}(M) = 2$, donc $M \sim \begin{pmatrix} a_1 & 0 \\ 0 & a_2 \end{pmatrix}$ où a_1 divise a_2. Or, en reprenant les notations du théorème 25, $a_1 = \mu_1(M)$ (car $\mu_0(M) = 1$). Donc $a_1 = \operatorname{pgcd}(10, 14, 6, 7) = 1$. De même $a_2 = \frac{\mu_2(M)}{\mu_1(M)} = \mu_2(M) = |\det(M)| = 14$. On retrouve donc bien la forme de Smith de M.

Exemple 37. On peut de même montrer que la forme de Smith de la matrice

$$M = \begin{pmatrix} X^3 + X^2 - 4X + 2 & X^3 + 2X^2 - 3X \\ 4X^3 - X^2 - 6X + 3 & 4X^3 + 3X^2 - 7X \end{pmatrix} \in \mathcal{M}_2(\mathbf{R}[X])$$

est

$$\begin{pmatrix} X - 1 & 0 \\ 0 & X^2 - X \end{pmatrix}.$$

4.3. **Algorithme de Berlekamp**

Pour finir, nous présentons ici l'algorithme de Berlekamp, qui permet de décomposer en facteurs irréductibles un polynôme sans facteurs carrés à coefficients dans un corps fini. L'algorithme de Berlekamp est une conséquence du théorème chinois, et sa mise en pratique nécessite des calculs de pgcd, donc de l'algorithme d'Euclide.

Soient p un nombre premier et $s \in \mathbf{N}^*$. On note $q := p^s$ et $\mathbf{F}_q$ le corps à q éléments. On commence par prouver un lemme utile pour la suite.

Lemme 38. Soit $R \in \mathbf{F}_q[X]$. Alors l'application

$$\left| \begin{array}{rccc} S_R : & \mathbf{F}_q[X]/(R) & \longrightarrow & \mathbf{F}_q[X]/(R) \\ & Q \mod R & \longmapsto & Q(X^q) \mod R \end{array} \right.$$

est bien définie et coïncide avec l'élévation à la puissance q dans $\mathbf{F}_q[X]/(R)$.

Démonstration. Soit δ_1 le morphisme d'anneaux défini par

$$\left| \begin{array}{rccc} \delta_1 : & \mathbf{F}_q[X] & \longrightarrow & \mathbf{F}_q[X] \\ & Q & \longmapsto & Q(X^q). \end{array} \right.$$

Comme $a^q = a$ pour tout $a \in \mathbf{F}_q$, on remarque que pour $Q \in \mathbf{F}_q[X]$, $\delta_1(Q) = Q(X^q) = Q^q$. Soient $\pi : \mathbf{F}_q[X] \longrightarrow \mathbf{F}_q[X]/(R)$ la projection canonique et $\delta := \pi \circ \delta_1$. L'application π est un morphisme d'anneaux, donc $\delta(R) = \pi(R)^q = 0$. Ainsi $(R) \subset \operatorname{Ker}\delta$, δ passe donc au quotient par (R) et l'on obtient S_R. De plus S_R coïncide bien avec l'élévation à la puissance q dans $\mathbf{F}_q[X]/(R)$ car pour tout $Q \in \mathbf{F}_q[X]$, on a

$$S_R(Q \mod R) = S_R(\pi(Q)) = \pi(Q(X^q)) = \pi(Q^q) = \pi(Q)^q.$$

□

Théorème 39 (Algorithme de Berlekamp)**.** Soit $P \in \mathbf{F}_q[X]$ un polynôme dont la décomposition en polynômes irréductibles est sans facteurs carrés. On note x l'image de X dans $\mathbf{F}_q[X]/(P)$, et on considère la base $\mathcal{B} = \{1, x \ldots, x^{\deg(P)-1}\}$ de $\mathbf{F}_q[X]/(P)$. Alors le processus suivant s'arrête au bout d'un nombre fini d'étapes et donne la décomposition en facteurs irréductibles de P.

Étape 1. On calcule la matrice de $S_P - \mathrm{Id}$ dans la base $\mathcal{B}$.

Étape 2. Le nombre de facteurs irréductibles de P est

$$r = \dim(\mathrm{Ker}\,(S_p - \mathrm{Id})) = \deg(P) - \mathrm{rg}\,(S_P - \mathrm{Id}).$$

Si $r = 1$, P est irréductible et on arrête. Sinon, on passe à **l'étape 3**.

Étape 3. On calcule un polynôme $V \in \mathbf{F}_q[X]$ tel que $V \mod P$ soit non constant et tel que $V \mod P \in \mathrm{Ker}\,(S_p - \mathrm{Id})$. On a alors

$$P = \prod_{\alpha \in \mathbf{F}_q} \mathrm{pgcd}(P, V - \alpha).$$

On retourne ensuite à **l'étape 1** avec chacun des facteurs non triviaux de ce produit.

Remarque. Le calcul du rang à l'étape 2 peut se faire avec un pivot de Gauss, donc ce calcul est faisable algorithmiquement.

Démonstration. Si $P \in \mathbf{F}_q[X]$ est sans facteurs carrés, alors il s'écrit $P = \prod_{i=1}^{r} P_i$ où les P_i sont des polynômes irréductibles deux à deux premiers entre eux. On considère les $\mathbf{F}_q$-espaces vectoriels de dimension finie $K_i := \mathbf{F}_q[X]/(P_i)$. Les P_i étant irréductibles, les K_i sont des corps. De plus, le théorème chinois nous fournit l'isomorphisme de $\mathbf{F}_q$-algèbres suivant, que l'on note φ :

$$\left| \begin{array}{rccc} \varphi : & \mathbf{F}_q[X]/(P) & \longrightarrow & K_1 \times \cdots K_r \\ & [Q] & \longmapsto & ([Q]_1, \ldots, [Q]_r) \end{array} \right.$$

où $[Q] = Q \mod P$ et $[Q]_i = Q \mod P_i$. Montrons que $r = \dim(\mathrm{Ker}\,(S_P - \mathrm{Id}))$. On pose

$$\widetilde{S_P} := \varphi \circ S_P \circ \varphi^{-1}$$

l'élévation à la puissance q dans l'anneau produit $K_1 \times \cdots \times K_r$. Soit $(x_1, \ldots x_r) \in K_1 \times \cdots \times K_r$. Alors

$$\begin{aligned} (x_1, \ldots, x_r) \in \mathrm{Ker}\,(\widetilde{S_P} - \mathrm{Id}) &\Leftrightarrow (x_1^q, \ldots, x_r^q) = (x_1, \ldots, x_r) \\ &\Leftrightarrow \forall\, i \in [\![1, r]\!], x_i^q = x_i \text{ dans } K_i. \end{aligned}$$

Considérons K une extension de corps de $\mathbf{F}_q$. Alors l'image de $\mathbf{F}_q$ dans K est l'ensemble des éléments x de K vérifiant $x^q = x$. En effet :

- Si $x \in \mathbf{F}_q^\times$, alors par le théorème de Lagrange $x^{q-1} = 1$, donc pour tout $x \in \mathbf{F}_q$, $x^q = x$ (l'égalité étant également vraie pour $x = 0$).
- Le polynôme $X^q - X \in K[X]$ est de degré q et admet déjà q racines, il n'y a donc pas d'autres éléments dans K vérifiant l'équation $X^q = X$.

Ainsi

$$(x_1, \ldots, x_r) \in \mathrm{Ker}\,(\widetilde{S_P} - \mathrm{Id}) \Leftrightarrow \forall\, i \in [\![1, r]\!], x_i^q = x_i \text{ dans } \mathbf{F}_q \hookrightarrow K_i,$$

donc $\mathrm{Ker}\,(\widetilde{S_P} - \mathrm{Id}) = (\mathbf{F}_q)^r$. Or $\mathrm{Ker}\,(\widetilde{S_P} - \mathrm{Id}) = \varphi(\mathrm{Ker}\,(S_P - \mathrm{Id})$ et φ est un isomorphisme, donc

$$\dim \mathrm{Ker}\,(S_P - \mathrm{Id}) = \dim(\mathrm{Ker}\,(\widetilde{S_P} - \mathrm{Id})) = \dim((\mathbf{F}_q)^r) = r.$$

Si $r = 1$, alors P est irréductible et l'algorithme s'arrête. On suppose donc que $r > 1$. Il existe alors $V \in \mathbf{F}_q[X]$ tel que $[V]$ est non constant et $[V] \in \mathrm{Ker}\,(S_P - \mathrm{Id})$. Par ce qui précède, on

sait alors que $([V]_1, \dots, [V]_r) \in (\mathbf{F}_q)^r$. Pour tout $i \in [\![1, r]\!]$, on note donc $\alpha_i := [V]_i \in \mathbf{F}_q \subset K_i$. Montrons maintenant que

$$\forall\, \alpha \in \mathbf{F}_q, \quad \operatorname{pgcd}(P, V - \alpha) = \prod_{\{i : \alpha_i = \alpha\}} P_i.$$

Par définition du pgcd, $\operatorname{pgcd}(P, V - \alpha)$ divise P, donc $\operatorname{pgcd}(P, V - \alpha)$ est de la forme

$$\prod_{i \in I_\alpha} P_i$$

où $I_\alpha \subset [\![1, r]\!]$. Les P_i sont deux à deux premiers entre eux, donc par le théorème de Gauss

$$I_\alpha = \{i \in [\![1, r]\!] : P_i \,|\, V - \alpha\}.$$

Or, pour $i \in [\![1, r]\!]$,

$$P_i \,|\, V - \alpha \Leftrightarrow [V - \alpha]_i = 0 \Leftrightarrow \alpha_i = \alpha,$$

donc $I_\alpha = \{i \in [\![1, r]\!] : \alpha_i = \alpha\}$ et on obtient finalement le résultat annoncé. De là il vient

$$P = \prod_{i=1}^{r} P_i = \prod_{\alpha \in \mathbf{F}_q} \left(\prod_{\{i : \alpha_i = \alpha\}} P_i \right) = \prod_{\alpha \in \mathbf{F}_q} \operatorname{pgcd}(P, V - \alpha).$$

On obtient la forme annoncée, mais il nous reste à vérifier la terminaison de l'algorithme, ie que r diminue strictement. Le polynôme $[V]$ est non constant, donc il existe nécessairement $i, j \in [\![1, r]\!]$ tel que $\alpha_i \neq \alpha_j$. Ainsi, le produit $\prod_{\alpha \in \mathbf{F}_q} \operatorname{pgcd}(P, V - \alpha)$ admet au moins deux facteurs non triviaux. Ils sont de plus sans facteurs carrés. La terminaison de l'algorithme est donc vérifiée. □

L'algorithme de Berlekamp permet de factoriser un polynôme sans facteurs carrés, mais qu'en est-il des polynômes quelconques ? Pour répondre à cette question, l'outil adéquat est le polynôme dérivé : on détecte si un polynôme P a des facteurs carrés en calculant $\operatorname{pgcd}(P, P')$. C'est l'objet de la proposition suivante, dont on peut trouver la preuve dans [1], aux pages 247-248. On pourra noter la différence avec les corps de caractéristique nulle.

Proposition 40. Soit $P \in \mathbf{F}_q[X]$. Alors
- $\operatorname{pgcd}(P, P') = P \iff P' = 0 \iff \exists\, R \in \mathbf{F}_q[X],\ R^p = P$;
- $\operatorname{pgcd}(P, P') = 1 \iff P$ est sans facteurs carrés.

On peut alors établir un algorithme de factorisation des polynômes sur $\mathbf{F}_q$.

Théorème 41 (Algorithme de factorisation de polynômes sur les corps fini.)**.** Soit $P \in \mathbf{F}_q[X]$. L'algorithme suivant donne la factorisation de P en polynômes irréductibles :

1. Si P est constant, fin.
2. Sinon on calcule $\operatorname{pgcd}(P, P')$.
   (a) Si $\operatorname{pgcd}(P, P') = 1$, on applique l'algorithme de Berlekamp.
   (b) Si $\operatorname{pgcd}(P, P') = P$, on calcule R tel que $R^p = P$ et retourner en 1. avec R.
   (c) Sinon $\operatorname{pgcd}(P, P') = P_1$, et $P_2 := P / \operatorname{pgcd}(P, P')$ sont deux facteurs non triviaux de P, retourner en 1. avec P_1 et P_2.

Références

[1] V. Beck, J. Malick, and G. Peyré. *Objectif Agrégation.* H&K, 2005.

[2] G. Berhuy. *Algèbre : le grand combat.* Calvage et Mounet, 2018.

[3] F. Combes. *Algèbre et géométrie.* Bréal, 2003.

[4] X. Gourdon. *Algèbre.* Ellipses, 2021.

[5] P. Ortiz. *Exercices d'algèbre.* Ellipses, 2004.

[6] D. Perrin. *Cours d'algèbre.* Ellipses, 1996.

[7] P. Saux Picart. *Cours de calcul formel. Algorithmes fondamentaux.* Ellipses, 1999.