Lucas Isenmann
Timothée Pecatte

Agrégation

L'oral à l'agrégation de mathématiques

Une sélection de développements

2e édition

ellipses

1 Décomposition des groupes abéliens finis

Note des auteurs. Le théorème de décomposition des groupes abéliens finis est un résultat important des mathématiques à connaître. Dans ce développement, on manie les caractères de groupes ainsi que les groupes cycliques, ce qui a pour conséquence un bon recasage.

Contexte

Comme pour la décomposition en nombres premiers d'un entier, on peut décomposer un groupe abélien fini en produit de groupes plus petits. Ce sont les groupes cycliques $\mathbb{Z}/n\mathbb{Z}$ qui joueront le rôle des nombres premiers. Le développement qui suit propose de démontrer ce résultat important qui permet de travailler plus facilement sur les groupes après les avoir décomposés, et en particulier de les classifier. Ce théorème est aussi connu sous le nom de théorème de Kronecker mais il ne faut pas le confondre avec l'autre théorème du même nom que l'on prouve aussi dans ce livre (voir « Théorème de Kronecker » (p. 277)).

On aura besoin des résultats suivant sur les ordres des éléments d'un groupe abélien fini. Étant donné un groupe fini G, le ppcm des ordres des éléments est appelé *l'exposant* du groupe et est noté $\exp(G)$.

Lemme 1.1. *Soit G un groupe abélien fini, et x, y deux éléments de G d'ordres respectifs n et m. Si $\mathrm{pgcd}(n, m) = 1$, alors xy est d'ordre nm.*

Démonstration. Comme $(xy)^{nm} = (x^n)^m(y^m)^n = ee = e$, alors, si on note r l'ordre de xy, on a $r|nm$. On a $x^{mr} = (x^r)^m = (y^{-r})^m = (y^m)^{-r} = e$, donc $n|\ mr$ et comme n et m sont premiers entre eux, on a $n|r$. De même on a $m|r$, d'où par le lemme de Gauss $nm|r$, et donc $r = nm$. □

Proposition 1.2. *Soit G un groupe abélien fini. Il existe un élément dont l'ordre est l'exposant de G.*

Démonstration. On pose $\exp(G) = \prod_{i=1}^{r} p_i^{a_i}$ la décomposition en facteurs premiers de l'exposant de G. Par définition de l'exposant et du ppcm, pour tout $i \in [\![1, r]\!]$, il existe un élément g_i tel que la p_i-valuation de son ordre soit a_i et on définit $u_i \in \mathbb{N}$ tel que l'ordre de g_i soit $p_i^{a_i} u_i$. Ainsi, $g_i^{u_i}$ est d'ordre $p_i^{a_i}$, et donc d'après le lemme précédent, l'élément $g = \prod_{i=1}^{r} g_i^{u_i}$ est d'ordre $\prod_{i=1}^{n} p_i^{a_i} = \exp(G)$. □

Définition 1.3. *Soit G un groupe. Un caractère χ de G est un morphisme de G dans $\mathbb{C}^*$. L'ensemble des caractères de G est noté $\widehat{G}$. En considérant la multiplication de caractères, $\widehat{G}$ est un groupe.*

Développement

On prouve d'abord qu'on peut toujours prolonger un caractère d'un sous-groupe abélien fini en un caractère défini sur le groupe complet.

Lemme 1.4. *Soient G un groupe abélien fini et H un sous-groupe de G. Soit un caractère χ de H, alors il existe un caractère τ de G tel que $\tau_{|H} = \chi$.*

Démonstration. On démontre ce résultat par récurrence sur l'indice de H. Si H est un sous-groupe de G d'indice 1, alors $H = G$ et le résultat est clair. Soit K un sous-groupe d'indice $[G : K] \geq 2$ tel que le résultat soit vrai pour tous les sous-groupes H de G tels que $[G : H] < [G : K]$. Comme $K \subsetneq G$, il existe $x \in G \setminus K$, et on pose $H = \langle x, K\rangle$ qui vérifie $[G : H] < [G : K]$. Il suffit alors de prolonger les caractères de K à H, puis d'utiliser l'hypothèse de récurrence pour les prolonger à G.

Soit $\chi \in \widehat{K}$ un caractère. Comme G est fini, on note $p < \infty$ l'ordre de x. Soit $r = \min\{i \geq 1 : x^i \in K\}$ qui est bien défini car $x^p = 1 \in K$. On a alors $\chi(x^r)^p = \chi(x^{rp}) = \chi(e) = 1$, donc $|\chi(x^r)| = 1$ et on note $u \in \mathbb{U}$ une racine r-ième de $\chi(x^r)$. Comme G est abélien, pour tout $z \in H$ il existe $s \in K$ et $0 \leq k < r$ tels que $z = sx^k$. De plus si $sx^k = tx^l$ avec $s, t \in K$ et $0 \leq k \leq l < r$, alors $x^{l-k} = st^{-1} \in K$ et donc $k = l$ par minimalité de r, d'où $s = t$ et donc l'écriture $z = sx^k$ est unique. On définit donc le candidat suivant pour le prolongement de χ sur H :

$$\begin{array}{rccc} \tau : & H & \longrightarrow & \mathbb{C} \\ & sx^k & \longmapsto & \chi(s)u^k. \end{array}$$

Pour sx^k et tx^l deux éléments de H, on a $\tau(sx^k tx^l) = \tau((st)x^{k+l})$.

- Si $k + l < r$: $\begin{aligned} \tau((st)x^{k+l}) &= \chi(st)\, u^{l+k} \\ &= \chi(s)\, u^k\, \chi(t)\, u^l \\ &= \tau(sx^k)\, \tau(tx^l) \end{aligned}$
- Si $r \leq k + l < 2r$: $\begin{aligned} \tau((st)x^{k+l}) &= \tau((stx^r)x^{l+k-r}) \\ &= \chi(stx^r)\, u^{k+l-r} \\ &= \chi(s)\chi(t)u^r\, u^{k+l-r} \\ &= \tau(sx^k)\, \tau(tx^l)\ . \end{aligned}$

Ainsi $\tau \in \widehat{H}$ et τ prolonge χ à H, ce qui prouve le résultat par récurrence. □

Théorème 1.5. *Soient G un groupe abélien fini non trivial. Il existe un entier $r \geq 1$ et des entiers $n_1, \ldots, n_r \geq 2$ tels que n_i divise n_{i-1} pour tout $i \geq 2$ et tels qu'on ait l'isomorphisme $G \cong \mathbb{U}_{n_1} \times \cdots \times \mathbb{U}_{n_r} \cong \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z}$.*

Démonstration. On démontre le résultat par récurrence sur l'ordre du groupe. Si $|G| = 2$, alors $G \cong \mathbb{U}_2$ donc le résulat est vrai. Soit G un groupe d'ordre supérieur

ou égal à 3 tel que le résultat soit vrai pour tout groupe abélien d'ordre strictement inférieur. On note m l'exposant de G et x un élément d'ordre m, qui existe d'après la Proposition 1.2 car G est abélien fini. Comme le groupe $\langle x \rangle$ est cyclique, alors il existe un isomorphisme $\chi : \langle x \rangle \to \mathbb{U}_m$, et en particulier on a $\chi \in \widehat{\langle x \rangle}$. D'après le lemme il existe donc $\tau \in \widehat{G}$ tel que τ prolonge χ à G. Tout élément de G est d'ordre divisant m donc τ est à valeurs dans $\mathbb{U}_m$. On peut alors définir l'application

$$\begin{array}{rccc} f : & G & \longrightarrow & \langle x \rangle \times (G/\langle x \rangle) \\ & g & \longmapsto & (\chi^{-1} \circ \tau(g), \overline{g}). \end{array}$$

qui est bien un morphisme de groupes comme produit et composée de morphismes de groupes. Si $g \in \mathrm{Ker}(f)$, alors $\overline{g} = \overline{e}$ et $g \in \langle x \rangle$. De là, puisque $\tau = \chi$ sur ce sous-groupe, on a $\chi^{-1} \circ \tau(g) = \chi^{-1} \circ \chi(g) = g$, d'où $g = e$ et donc f est injective. Comme G et $\langle x \rangle \times (G/\langle x \rangle)$ ont même cardinal, f est un isomorphisme.

Comme $|G/\langle x \rangle| < |G|$, d'après l'hypothèse de récurrence il existe des entiers $n_2, \ldots, n_r$ tels que $n_i | n_{i-1}$ pour tout $i \geq 2$ et $G/\langle x \rangle \cong \mathbb{U}_{n_2} \times \cdots \times \mathbb{U}_{n_r}$. D'où $G \cong \mathbb{U}_m \times \mathbb{U}_{n_2} \times \cdots \times \mathbb{U}_{n_r}$ et il ne reste plus qu'à montrer que $n_2 | m$. On considère pour cela l'élément $(1, e^{2i\pi/n_2}, 1, \ldots, 1) \in \mathbb{U}_m \times \mathbb{U}_{n_2} \times \cdots \times \mathbb{U}_{n_r}$ qui est d'ordre n_2. Donc n_2 divise m par définition de l'exposant, ce qui achève la preuve par récurrence du résultat. □

Approfondissements

Ce théorème de décomposition permet de classifier les groupes finis. Par exemple les seuls groupes d'ordre p^2 sont $\mathbb{Z}/p^2\mathbb{Z}$ et $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ où p est un nombre premier. On peut en fait prouver qu'une telle décomposition est unique, et on appelle alors les entiers $n_1, \ldots, n_r$ les facteurs invariants du groupe G. Pour prouver l'unicité, nous aurons besoin du lemme suivant :

Lemme 1.6. *Soit $n_1, \ldots, n_r$ des entiers et k un entier. Alors le nombre d'éléments de $\mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z}$ dont l'ordre divise k vaut*

$$\mathrm{pgcd}(k, n_1) \cdots \mathrm{pgcd}(k, n_r).$$

Démonstration. Par produit, il suffit de montrer que le nombre le nombre d'éléments dans $\mathbb{Z}/n\mathbb{Z}$ dont l'ordre divise k vaut $u \overset{\text{def}}{=} \mathrm{pgcd}(k, n)$. On pose k' et n' les entiers premiers entre eux tels que $k = uk'$ et $n = un'$. Soit a un élément dont l'ordre divise k : on a $ak = 0 \mod n$. Ainsi n' divise ak', et donc, par le lemme de Gauss, n' divise a. Réciproquement, si a est divisible par n', alors n divise ak et donc l'ordre de a divise k. L'ensemble des éléments dont l'ordre divise k est donc engendré par n'. Il reste à calculer l'ordre de n' : si $vn' = 0 \mod n$, alors n divise vn', donc u divise v. Réciproquement, on a bien $un' = n = 0 \mod n$, d'où n' est d'ordre u. Ainsi il y a $\mathrm{pgcd}(k, n)$ éléments dont l'ordre divise k dans $\mathbb{Z}/n\mathbb{Z}$. □

Théorème 1.7. *Soient $n_1, \dots, n_r$ et $m_1, \dots, m_s$ des entiers tels que $n_i | n_{i-1}$ et $m_i | m_{i-1}$ pour tout i. Si $\mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z} \cong \mathbb{Z}/m_1 \times \cdots \times \mathbb{Z}/m_s\mathbb{Z}$, alors $s = r$ et $n_i = m_i$ pour tout i.*

Démonstration. D'après le lemme précédent on a donc

$$\forall k \in \mathbb{N}, \quad \prod_{i=1}^{r} \operatorname{pgcd}(k, n_i) = \prod_{j=1}^{s} \operatorname{pgcd}(k, m_j).$$

Supposons sans perte de généralité que $r \geq s$. On prend alors $k = n_r$ pour obtenir l'égalité suivante : $(n_r)^r = \prod_{j=1}^{s} \operatorname{pgcd}(n_r, m_j)$. Comme $\operatorname{pgcd}(n_r, m_j) \leq n_r$, on a nécessairement $s = r$ et $\operatorname{pgcd}(n_r, m_j) = n_r$ pour tout j. Un argument symétrique permet de montrer que $\operatorname{pgcd}(m_s, n_i) = m_s$ pour tout i. Ainsi, on a donc prouvé que $m_s = \operatorname{pgcd}(m_s, n_r) = n_r$, et on montre de même par récurrence que $n_i = m_i$ pour tout i. □

Ce schéma de preuve permet d'aboutir au critère suivant pour montrer que deux groupes sont isomorphes.

Proposition 1.8. *Soient G et H deux groupes abéliens finis qui ont, pour tout entier k, le même nombre d'éléments d'ordre k. Alors G et H sont isomorphes.*

Démonstration. Il est immédiat que pour tout k, le nombre d'éléments dont l'ordre divise k est le même dans G et dans H. D'après le Théorème 1.5, il existe $a_1, \dots, a_r$ et $b_1, \dots, b_s$ tels que $G \cong \mathbb{U}_{a_1} \cdots \mathbb{U}_{a_r}$, $H \cong \mathbb{U}_{b_1} \cdots \times \mathbb{U}_{b_s}$ et a_i divise a_{i-1} pour tout i et b_i divise b_{i-1} pour tout i. On a donc $\prod_{i=1}^{r} \operatorname{pgcd}(k, n_i) = \prod_{j=1}^{s} \operatorname{pgcd}(k, m_j)$ pour tout entier k. D'où $s = r$ et $a_i = b_i$ pour tout i, et donc $G \cong H$. □

Le théorème de décomposition permet entre autre de dénombrer le nombre de groupes abéliens d'ordre n.

Proposition 1.9. *Soit $n = \prod_{i=1}^{r} p_i^{k_i}$ un entier et sa décomposition en nombres premiers. Alors il existe, à isomorphisme près,*

$$p(k_1) \cdots p(k_r)$$

groupes abéliens d'ordre n où $p(a)$ désigne le nombre partition de l'entier a.

Cette décomposition est aussi la base de l'analyse harmonique des groupes qui, pour définir la transformée de Fourier d'une fonction sur G à valeurs dans $\mathbb{C}$, va utiliser le dual du groupe.

Proposition 1.10. *Le dual d'un groupe abélien est isomorphe au groupe lui-même.*

Ce théorème peut aussi être étendu pour décomposer les groupes abéliens d'ordre infini de type fini (c'est-à-dire engendré par un nombre fini d'éléments).

Théorème 1.11. *Soit G un groupe abélien de type fini. Alors il existe un entier l, un entier $r \geq 1$ et des entiers $n_1, \dots, n_r \geq 2$ tels que n_i divise n_{i-1} pour tout $i \geq 2$ et*

$$G \cong \mathbb{Z}^l \times \mathbb{U}_{n_1} \times \cdots \times \mathbb{U}_{n_r}.$$

Recasages

★★★★★ **102 :** *Groupe des nombres complexes de module* 1. *Racines de l'unité. Applications.*

★★★★★ **104 :** *Groupes finis. Exemples et applications.*

★★★★ **108 :** *Exemples de parties génératrices d'un groupe. Applications.*

★★★ **120 :** *Anneaux Z/nZ. Applications.*

★★★★★ 110 : *(Ancienne leçon de 2019) Structure et dualité des groupes abéliens finis. Applications.*

★★★★ 107 : *(Ancienne leçon de 2021) Représentations et caractères d'un groupe fini sur un $\mathbb{C}$-espace vectoriel. Exemples.*

Références

[1] Pierre COLMEZ : *Éléments d'analyse et d'algèbre (et de théorie des nombres)*. École Polytechnique, 2011.

[2] Gabriel PEYRÉ : *L'algèbre discrète de la transformée de Fourier*. Ellipses, 2004.

2 Algorithme de Berlekamp

Note des auteurs. Il s'agit d'un résultat classique de calcul formel qui fait intervenir polynômes, corps finis et algèbre linéaire. Le recasage est bon bien que le développement soit un peu technique. Cette procédure fait partie d'un algorithme plus général qui décompose tout polynôme à coefficients entiers en polynômes irréductibles.

Contexte

Pour un polynôme $P \in \mathbb{K}[X]$, où $\mathbb{K}$ est un corps, on dit que P est irréductible si $P \notin \mathbb{K}^*$ et si pour toute factorisation $P = QR$, on a $Q \in \mathbb{K}^*$ ou $R \in \mathbb{K}^*$. Les polynômes irréductibles jouent un rôle central dans l'étude de $\mathbb{K}[X]$ puisque tout polynôme se décompose de manière unique (à un facteur inversible près) en un produit de polynômes irréductibles puisque $\mathbb{K}[X]$ hérite de la factorialité de $\mathbb{K}$. Le théorème fondamental de l'algèbre permet de prouver que les irréductibles de $\mathbb{C}[X]$ sont précisemment les polynômes de degré 1 (qui sont toujours irréductibles par propriété du degré). Sur $\mathbb{R}$, il faut aussi rajouter aux polynômes de degré 1 les polynômes de degré 2 de la forme $X^2 + bX + c$ avec b, c des réels tels que $b^2 - 4c < 0$. En revanche, sur un corps fini, il n'y a pas de caractérisation complète des polynômes irréductibles. Néanmoins, il existe des algorithmes capables de calculer la factorisation d'un polynôme $P \in \mathbb{F}_q[X]$ en produit d'irréductibles. Dans ce développement, on présente un de ces algorithmes, découvert par Berlekamp en 1967.

On rappelle et prouve ici quelques résultats nécessaires au développement. En fonction du temps pris pour présenter le résultat principal, vous pouvez présenter certains des résultats suivants (en particulier le deuxième).

Lemme 2.1. *Soit p un nombre premier. Alors p divise $\binom{p}{k}$ si $1 \leq k \leq p-1$.*

En utilisant la formule du binôme de Newton et ce lemme, on obtient l'égalité $(a+b)^p = a^p + b^p \ [p]$. Plus généralement, pour $q = p^n$, on montre que l'application $x \longmapsto x^q$ est un endomorphisme de corps de $\mathbb{F}_q$, également connue sous le nom de morphisme de Frobenius. Dans ce développement, nous utiliserons un prolongement de cet endomorphisme défini sur les polynômes de $\mathbb{F}_q[X]$.

Proposition 2.2. *L'application $S : \mathbb{F}_q[X] \to \mathbb{F}_q[X]$ définie par $S(Q) = Q^p$ est un $\mathbb{F}_q$-endomorphisme de l'espace vectoriel $\mathbb{F}_q[X]$.*

Démonstration. Pour tout $\lambda \in \mathbb{F}_q$, on a $\lambda^q = \lambda$ et donc, pour tout $R \in \mathbb{F}_q[X]$, on a $S(\lambda R) = (\lambda R)^q = \lambda S(R)$. Soient $Q, R \in \mathbb{F}_q[X]$. Comme $\mathbb{F}_q$ est de caractéristique p, on a $(Q+R)^p = Q^p + R^p$. Ainsi, on montre par récurrence sur $k \in \mathbb{N}$ que

$(Q+R)^{p^k} = Q^{p^k} + R^{p^k}$, et donc en particulier

$$S(Q+R) = (Q+R)^{p^n} = Q^{p^n} + R^{p^n} = S(Q) + S(R),$$

ce qui achève la preuve que S est $\mathbb{F}_q$-linéaire. □

La proposition suivante est une propriété importante des corps finis qui découle du lien avec les polynômes.

Proposition 2.3. *Soit L une extension de $\mathbb{F}_q$. Alors $x \in L$ vérifie $x^q = x$ si et seulement si $x \in \mathbb{F}_q$.*

Démonstration. D'après le théorème de Lagrange, pour tout $x \in \mathbb{F}_q^*$, on a $x^{q-1} = 1$, d'où $x^q = x$ pour tout élément $x \in \mathbb{F}_q$. On a donc exhibé q racines distinctes du polynômes $P = X^q - X$ sur L. Or, comme L est un corps et que P est de degré q, P possède au plus q racines, donc ce sont les seules. □

On utilisera aussi le théorème des restes chinois appliqué à l'algèbre $\mathbb{F}_q[X]$, qui s'énonce alors de la manière suivante.

Théorème 2.4. *Soient $P_1, \dots, P_r \in \mathbb{F}_q[X]$ des polynômes premiers entre eux, et soit $P = \prod_{i=1}^r P_i$. Alors, l'application suivante est un isomorphisme de $\mathbb{F}_q$-algèbres :*

$$\begin{array}{rccc} f: & \mathbb{F}_q[X]/(P) & \longrightarrow & \mathbb{F}_q[X]/(P_1) \times \cdots \times \mathbb{F}_q[X]/(P_r) \\ & x \mod P & \longmapsto & (x \mod P_1, \dots, x \mod P_r). \end{array}$$

Développement

Théorème 2.5. *Soient $q = p^n$ avec p premier, $n \in \mathbb{N}^*$ et $P \in \mathbb{F}_q[X]$ sans facteur carré. On pose $P = \prod_{i=1}^r P_i$ la décomposition de P en produit d'irréductibles sur $\mathbb{F}_q[X]$. Si $r = 1$, alors P est irréductible. Sinon, il existe $a \in \mathbb{F}_q$ et $V \in \mathbb{F}_q[X]$ tels que $\operatorname{pgcd}(P, V - a)$ soit un facteur non trivial de P.*

Démonstration. On considère l'application

$$\begin{array}{rccc} T: & \mathbb{F}_q[X] & \longrightarrow & \mathbb{F}_q[X]/(P) \\ & Q & \longmapsto & Q^q \mod P. \end{array}$$

Comme $S : Q \to Q^q$ et la projection canonique sont toutes les deux $\mathbb{F}_q$-linéaires, alors T est $\mathbb{F}_q$-linéaire par composition. Pour tout polynôme $Q \in \mathbb{F}_q[X]$, on a l'égalité suivante : $T(QP) = (QP)^q\ [P] = 0$ et donc $(P) \subseteq \operatorname{Ker}(T)$. On peut alors factoriser T pour obtenir un $\mathbb{F}_q$-endomorphisme φ de $\mathbb{F}_q[X]/(P)$ défini par $\varphi(\overline{Q}) = \overline{Q^q}$.

Les P_i sont premiers entre eux ; d'après le Théorème 2.4, il existe donc un isomorphisme de $\mathbb{F}_q$-algèbres

$$\psi : \mathbb{F}_q[X]/(P) \to K_1 \times \cdots \times K_r,$$

où $K_i = \mathbb{F}_q[X]/(P_i)$ est un corps car P_i est irréductible. On pose alors l'application linéaire $\tilde{\varphi} = \psi \circ \varphi \circ \psi^{-1}$, qui vérifie $\tilde{\varphi}(Q) = (Q_1^q, \ldots, Q_r^q)$ pour tout $Q = (Q_1, \ldots, Q_r) \in K_1 \times \cdots \times K_r$ car l'application ψ préserve la multiplication. Ainsi, on a $Q \in \mathrm{Ker}(\tilde{\varphi} - \mathrm{Id})$ si et seulement $Q_i^q = Q_i$ pour tout $i \in [\![1, r]\!]$. Or, pour tout $i \in [\![1, r]\!]$, K_i est une extension de $\mathbb{F}_q$, donc on a, d'après la Proposition 2.3, $Q_i^q = Q_i$ si et seulement si $Q_i \in \mathbb{F}_q$. On a donc $|\mathrm{Ker}(\tilde{\varphi} - Id)| = q^r$ et donc $\dim(\mathrm{Ker}(\varphi - \mathrm{Id})) = \dim(\mathrm{Ker}(\tilde{\varphi} - \mathrm{Id})) = r$.

Supposons que r soit supérieur ou égal à 2. Les polynômes constants modulo P forment un sous-espace vectoriel de $\mathbb{F}_q[X]/(P)$ de dimension 1 engendré par 1. Comme $\dim(\mathrm{Ker}(\varphi - \mathrm{Id})) = r \geq 2$, il existe donc $V \in \mathbb{F}_q[X]$ non constant modulo P tel que $V^q = V[P]$. En particulier, pour tout $i \in [\![1, r]\!]$, on a $V^q = V[P_i]$ et on pose donc $\alpha_i \overset{\text{def}}{=} V[P_i]$ qui appartient à $\mathbb{F}_q$ d'après la Proposition 2.3. Si pour tout $i, j \in [\![1, r]\!]$, on avait $\alpha_i = \alpha_j$, alors il existerait $\alpha \in \mathbb{F}_q$ tel que $V = \alpha[P_i]$ pour tout $i \in [\![1, r]\!]$, et donc $V = \alpha[P]$ (par injectivité de ψ), ce qui est impossible car on a supposé que V n'était pas constant modulo P. Ainsi il existe $i, j \in [\![1, r]\!]$ distincts tels que $\alpha_i \neq \alpha_j$. On pose alors $Q \overset{\text{def}}{=} \mathrm{pgcd}(P, V - \alpha_i)$. Comme P_i divise P et $V - \alpha_i$, il divise aussi Q. De plus, P_j ne divise pas Q car il ne divise pas $V - \alpha_i$ puisque $\alpha_i \neq \alpha_j$. Ainsi, $Q \neq 1$ et $Q \neq P$, donc Q est un facteur non trivial de P. □

La preuve de ce théorème est constructive puisqu'elle fournit une manière de trouver un tel V : il suffit de calculer le noyau de l'application linéaire $\varphi - \mathrm{Id}$. On en déduit un algorithme itératif puisque pour trouver un nouveau facteur, il suffit de recommencer ce procédé avec $P/(V - \alpha)$ à la place de P. L'algorithme s'arrête lorsque $\dim(\mathrm{Ker}(\varphi - \mathrm{Id})) = 1$, ce qui signifie que le polynôme est irréductible.

Remarque 2.6. *Si P possède des facteurs carrés et $P' \neq 0$, on peut les récupérer en calculant $Q = \mathrm{pgcd}(P, P')$. On peut alors utiliser l'algorithme décrit précédemment pour factoriser P/Q qui est bien sans facteur carré. En réitérant le processus pour factoriser Q, on obtient ainsi la factorisation complète de P.*

Dans le cas dégénéré où $P' = 0$, il existe alors un polynôme $Q \in \mathbb{F}_q[X]$ tel que $P(X) = Q(X^p)$. D'après l'isomorphisme de Frobenius, il existe un polynôme $R \in \mathbb{F}_q[X]$ tel que $Q(X^p) = R(X)^p$: les coefficients de R sont les racines p-ièmes des coefficients de Q. Il suffit alors de factoriser R pour obtenir la factorisation de P.