35 Polygones réguliers constructibles

Note des auteurs. Un résultat classique assez important qui fait intervenir des notions d'algèbre très variées, ce qui lui confère un très bon recasage. La preuve est un peu technique, mais nous donnons ici une présentation originale assez élémentaire, en interprétant l'application comme une permutation circulaire des coordonnnées.

Contexte

Les mathématiciens de la Grèce antique s'intéressaient déjà aux polygones réguliers constructibles à l'aide d'une règle (non-graduée) et d'un compas. Ils savaient construire le triangle, le carré et le pentagone, et, étant donné un polygone régulier constructible à n côtés, ils savaient construire le polygone régulier à $2n$ côtés. Se pose donc la question : est il possible de construire tous les polygones réguliers à la règle et au compas ? C'est Gauss qui en 1801 donne une première condition suffisante pour la construction du polygone régulier à n côtés, et il prétend, sans toutefois le prouver, que cette condition est aussi nécessaire. Il faut attendre Wantzel en 1837 pour venir à bout de cette conjecture.

On commence par définir formellement la notion d'objet constructible à la règle et au compas :

Définition 35.1. *Pour une partie $X \subseteq \mathbb{R}^2$, on définit :*

- $\gamma_1(X) \overset{def}{=} \{(AB) : A, B \in X\}$ *l'ensemble des droites passant par deux points distincts de X.*
- $\gamma_2(X) \overset{def}{=} \{C(A, |AB|) : A, B \in X\}$ *l'ensemble des cercles dont un rayon a pour extrémité deux points distincts de X.*

On note $\gamma(X) = \gamma_1(X) \cup \gamma_2(X)$, et on dit qu'un point $M \in \mathbb{R}^2$ est constructible en un pas à partir de X s'il existe $u, v \in \gamma(X)$ distincts tels que $M \in u \cap v$.

On définit par récurrence l'ensemble B_n des points constructibles en n étapes à partir de $A \overset{\text{def}}{=} (0,0)$ et $B \overset{\text{def}}{=} (1,0)$. On a donc $B_0 = \{A, B\}$, et B_{n+1} est l'ensemble des points de P constructibles à partir de B_n en un pas. On dira que $M \in \mathbb{R}^2$ est constructible si $M \in \bigcup_{n\in\mathbb{N}} B_n$. De plus on dira que $x \in \mathbb{R}$ est constructible si $(x, 0)$ est constructible. On peut alors montrer que l'ensemble des nombres réels constructibles forme un corps dont les rationnels font partie.

Pour pouvoir construire le polygone régulier à n côtés, il faut et il suffit de savoir construire son sommet C d'affixe $\omega_n = e^{i\frac{2\pi}{n}}$. En effet, si on est capable d'obtenir ce point à partir de A et B, il suffit de répéter la suite d'opérations à partir de A et C pour obtenir le sommet suivant du polygone d'affixe w_n^2. En répétant cette opération n fois, on construit tous les sommets du polygone. Pour simplifier les notations, on

dira que $z \in \mathbb{C}$ est constructible si le point d'affixe z l'est. Le polygone régulier à n côtés est donc constructible si et seulement si ω_n est constructible.

Intuitivement, les nombres constructibles en un pas à partir d'un ensemble X sont solutions d'équations de degré au plus deux puisqu'ils correspondent à l'intersection d'une droite ou d'un cercle avec une autre droite ou un cercle. Wantzel formalise cette intuition à l'aide de la notion de tour d'extension quadratique qu'on définit maintenant.

Définition 35.2. *Une suite finie de corps $\mathbb{L}_0, \dots, \mathbb{L}_p$ est une* tour d'extension quadratique *si $\mathbb{L}_{i+1}$ est une extension finie de degré 2 de $\mathbb{L}_i$ pour tout $i \in [\![0, p-1]\!]$.*

Théorème 35.3 (Wantzel)**.** *Un nombre $t \in \mathbb{R}$ est constructible si et seulement si il existe $\mathbb{L}_0, \dots, \mathbb{L}_p$ une tour d'extension quadratique telle que $t \in \mathbb{L}_p$ et $\mathbb{L}_0 = \mathbb{Q}$.*

Comme $\mathbb{C}$ est une extension de $\mathbb{R}$ de degré 2, on en déduit aisément la version complexe du théorème de Wantzel.

Théorème 35.4. *Un nombre $z \in \mathbb{C}$ est constructible si et seulement si il existe $\mathbb{L}_0, \dots, \mathbb{L}_p$ une tour d'extension quadratique telle que $z \in \mathbb{L}_p$ et $\mathbb{L}_0 = \mathbb{Q}$.*

Corollaire 35.5. *Si $x \in \mathbb{C}$ est constructible, alors il existe un entier $n \in \mathbb{N}$ tel que $[\mathbb{Q}(x) : \mathbb{Q}] = 2^n$.*

Démonstration. Supposons que x soit constructible : il existe une tour d'extension quadratique $\mathbb{L}_0, \dots, \mathbb{L}_p$ de $\mathbb{Q}$ dans $\mathbb{C}$ telle que $x \in \mathbb{L}_p$. Comme $\mathbb{L}_p$ contient $\mathbb{Q}$ et x, alors $\mathbb{L}_p$ contient aussi $\mathbb{Q}(x)$. Ainsi $\mathbb{Q}(x)$ est un sous-corps de $\mathbb{L}_p$ donc son degré sur $\mathbb{Q}$ divise celui de $\mathbb{L}_p$ sur $\mathbb{Q}$. D'après le théorème des bases télescopiques, $\mathbb{L}_p$ est de degré 2^p sur $\mathbb{Q}$, donc $\mathbb{Q}(x)$ est de degré 2^n sur $\mathbb{Q}$ avec $n \leq p$. □

On rappelle la définition et quelques propriétés importantes des polynômes cyclotomiques.

Définition 35.6. *Soit $n \in \mathbb{N}^*$. Le polynôme cyclotomique Φ_n est défini par*

$$\Phi_n(X) \overset{def}{=} \prod_{0 \leq k < n, k \wedge n = 1} \left(X - \exp\left(\frac{2ik\pi}{n} \right) \right).$$

On rappelle que l'indicatrice d'Euler $\varphi(n)$ d'un entier n est défini comme le nombre d'entiers k tels que $0 \leq k < n$ et k est premier avec n. La propriété suivante peut constituer un développement en lui-même.

Proposition 35.7. *Soit $n \in \mathbb{N}^*$, alors $\Phi_n \in \mathbb{Q}[X]$ est de degré $\varphi(n)$ et est irréductible sur $\mathbb{Q}$. De plus*

$$X^n - 1 = \prod_{d \mid n} \Phi_d(X).$$

Développement

Théorème 35.8. *Soit p un nombre premier impair et $a \in \mathbb{N}^*$. Alors le polygone régulier à p^a côtés est constructible si et seulement si $a = 1$ et s'il existe $n \in \mathbb{N}$ tel que $p = 2^n + 1$.*

Démonstration. Supposons que le polygone régulier à $m \overset{\text{def}}{=} p^a$ côtés soit constructible, donc $\omega_m = e^{2i\pi/m}$ est constructible. Or, ω_m est racine du polynôme cyclotomique Φ_m, qui est unitaire et irréductible sur $\mathbb{Q}$. Ainsi, ω_m est algébrique sur $\mathbb{Q}$ de degré $\deg(\Phi_m) = \varphi(m) = p^{a-1}(p-1)$. Comme ω_m est constructible, le théorème de Wantzel implique que $p^{a-1}(p-1)$ est une puissance de 2. On a donc nécessairement $a = 1$, et $p - 1$ est une puissance de 2.

Supposons qu'il existe $n \geq 1$ tel que $p = 1 + 2^n$. On pose $\omega \overset{\text{def}}{=} e^{2i\pi/p}$ et $\mathbb{K} = \mathbb{Q}(\omega)$ le corps cyclotomique. Là aussi, le polynôme minimal de ω est Φ_p, d'où $[\mathbb{K} : \mathbb{Q}] = p - 1 = 2^n$ et donc une base de $\mathbb{K}$ comme $\mathbb{Q}$-espace vectoriel est $\mathcal{B} = \{\omega, \omega^2, \ldots, \omega^{p-1}\}$. Pour construire la tour d'extension quadratique de $\mathbb{Q}$ dans $\mathbb{K}$ de longueur n, on s'intéresse à $G = \mathrm{Aut}(\mathbb{K})$ l'ensemble des automorphismes de corps de $\mathbb{K}$ qui sont $\mathbb{Q}$-linéaires : on commence par montrer que G est isomorphe à $(\mathbb{Z}/p\mathbb{Z})^\times$, puis on construit des sous-ensembles de $\mathbb{K}$ invariants par des sous-groupes de G qui nous fourniront les corps intermédiaires.

Un élément $g \in G$ est complétement déterminé par l'image de ω. Comme Φ_p annule ω, on a $\Phi_p(g(\omega)) = g(\Phi_p(\omega)) = g(0) = 0$ donc l'image de ω par g est encore une racine de Φ_p : il existe un unique $k \in \mathbb{Z}/p\mathbb{Z}$ tel que $g(\omega) = \omega^k$. De plus, comme ω est une racine primitive, on a nécessairement $k \in (\mathbb{Z}/p\mathbb{Z})^\times$. On a ainsi défini une application injective $\varphi : G \to (\mathbb{Z}/p\mathbb{Z})^\times$ qui est un morphisme puisque $g \circ h(\omega) = g(\omega^{\varphi(h)}) = (g(\omega))^{\varphi(h)} = \omega^{\varphi(h)\varphi(g)}$.

Montrons que φ est surjective : soit $k \in (\mathbb{Z}/p\mathbb{Z})^\times$ et construisons $g \in G$ tel que $g(\omega) = \omega^k$. Remarquons qu'il suffit de définir g sur les éléments de $\mathcal{B}$ pour définir g sur $\mathbb{K}$ tout entier par $\mathbb{Q}$-linéarité, qui sera donc compatible avec l'addition et la multiplication par un scalaire. On définit donc l'application linéaire $g : \mathbb{K} \to \mathbb{K}$ du $\mathbb{Q}$-espace vectoriel $\mathbb{K}$ par son image sur la base $\mathcal{B}$:

$$g(\omega^i) = \omega^{ik} \quad \text{pour tout } i \in [\![1, p-1]\!].$$

C'est le seul candidat pour être un automorphisme de corps puisqu'on doit avoir $g(\omega^i) = g(\omega)^i$. Montrons maintenant qu'il s'agit bien d'un automorphisme du corps $\mathbb{K}$. Dans la base $\mathcal{B}$, la décomposition de 1 est donnée par $1 = \sum_{j=1}^{p-1} -\omega^j$, et donc la $\mathbb{Q}$-linéarité de g permet de montrer que

$$g(1) = \sum_{j=1}^{p-1} g(-\omega^j) = \sum_{j=1}^{p-1} -\omega^{kj} = 1.$$

De même, pour $i \geq p$, on a $g(\omega^i) = g(\omega^{i \mod p}) = \omega^{k(i \mod p)} = \omega^{ki}$. Ainsi, on a $g(\omega^i) = \omega^{ki}$ pour tout $i \in \mathbb{N}$. Il reste donc à vérifier la compatibilité de g avec la multiplication et, quitte à développer par $\mathbb{Q}$-linéarité, il suffit de considérer le cas de la multiplication de deux éléments de la base. Pour $i, j \in [\![1, p-1]\!]$, on a bien $g(\omega^i\omega^j) = g(\omega^{i+j}) = \omega^{k(i+j)} = \omega^{ki}\omega^{kj} = g(\omega^i)g(\omega^j)$ et donc g est bien un automorphisme du corps $\mathbb{K}$ tel que $g(\omega) = \omega^k$.

On a donc montré que l'application $\varphi : G \to (\mathbb{Z}/p\mathbb{Z})^\times$, qui à $g \in G$ associe l'unique $k \in (\mathbb{Z}/p\mathbb{Z})^\times$ tel que $g(\omega) = \omega^k$, est un isomorphisme. Comme $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique, alors G l'est également : il existe un élément $g \in G$ d'ordre $p-1$, et donc $B = \{\omega, g(\omega), g^2(\omega), \dots, g^{p-2}(\omega)\}$ est une base. On définit alors les ensembles $\mathbb{K}_i \overset{\text{def}}{=} \{z \in \mathbb{K} : g^{2^i}(z) = z\}$ pour $i \in [\![0, n]\!]$, qui sont des sous-corps de $\mathbb{K}$ tels que $\mathbb{K}_i \subseteq \mathbb{K}_{i+1}$, et $\mathbb{K}_n = \mathbb{K}$ car $g^{2^n} = \mathrm{Id}$. Nous allons montrer que les $\mathbb{K}_i$ forment la tour d'extension quadratique souhaitée. Pour cela, nous allons voir l'application de g à $z \in \mathbb{K}$ comme une permutation circulaire des coordonnées de z dans la base B. En effet, décomposons z dans la base B : $z = \sum_{i=0}^{p-2} z_i g^i(\omega)$ où $z_i \in \mathbb{Q}$ pour tout i. On a alors

$$g(z) = \sum_{i=0}^{p-2} z_i g^{i+1}(\omega) = \sum_{i=1}^{p-2} z_{i-1} g^i(\omega) + z_{p-2}\,\omega.$$

On peut donc écrire $g \cdot (z_0, z_1, \dots, z_{p-2}) = (z_{p-2}, z_0, \dots, z_{p-1})$. De cette manière, on a $g^a(z) = z$ si et seulement si $z_{i+a} = z_i$ pour tout i, où les indices sont pris modulo p. En particulier, si a est premier avec $p-1$, alors il engendre $(\mathbb{Z}/(p-1)\mathbb{Z}, +)$ donc on a $g^a(z) = z$ si et seulement si $z_i = z_0$ pour tout i. Dans ce cas, on aurait $z = z_0 \sum_{i=0}^{p-2} g^i(\omega) = z_0 \sum_{i=1}^{p-1} \omega^i = -z_0 \in \mathbb{Q}$, doù $g^a(z) = z$ si et seulement si $z \in \mathbb{Q}$. Le cas $a = 1$ assure que $\mathbb{K}_0 = \mathbb{Q}$, et cette remarque motive la définition des $\mathbb{K}_i$.

Pour $i \in [\![0, n]\!]$, on a $z \in \mathbb{K}_i$ si et seulement si $z_{j+2^i} = z_j$ pour tout j. Notons e l'élément de $\mathbb{K}$ dont la décomposition dans la base B est donné par

$$e = (1, \underbrace{0, \dots, 0}_{2^i-1}, 1, \underbrace{0, \dots, 0}_{2^i-1}, \dots) = \sum_{j=0}^{2^{n-j}-1} g^{j \cdot 2^i}(\omega).$$

L'ensemble $C = \{e, g(e), \dots, g^{2^i-1}(e)\}$ est une famille linéairement indépendante. On a $z \in \mathbb{K}_i$ si et seulement si $z_{j+2^i} = z_j$ pour tout j, ce qui équivaut à dire que z se décompose en $z = \sum_{j=0}^{2^i-1} z_j g^j(e)$. On a donc $\mathbb{K}_i = \langle C \rangle$, d'où $[\mathbb{K}_i : \mathbb{Q}] = 2^i$. Et comme $\mathbb{K}_i \subseteq \mathbb{K}_{i+1}$, le théorème de la base télescopique nous donne l'égalité $[\mathbb{K}_{i+1} : \mathbb{K}_i] = \frac{[\mathbb{K}_{i+1} : \mathbb{Q}]}{[\mathbb{K}_i : \mathbb{Q}]} = 2$. On a donc une tour d'extension quadratique de $\mathbb{K}$ sur $\mathbb{Q}$, d'où w est constructible par le théorème de Wantzel.

□

Approfondissements

Le théorème précédent énonce donc que si un polygone régulier à p côtés est constructible avec p premier impair, alors il existe n un entier tel que $p = 2^n + 1$. Les nombres premiers de la forme $2^n + 1$ s'appelle les nombres premiers de Fermat. Il est facile de montrer que dans ce cas, n doit nécessairement être une puissance de deux, c'est pourquoi on note $F_k = 2^{2^k} + 1$ les nombres de Fermat. Ce dernier conjectura que tous les nombres F_k étaient premiers, en s'appuyant sur le fait que $F_0 = 3, F_1 = 5, F_2 = 17, F_3 = 257$ et $F_4 = 65537$ sont effectivement premiers. Néanmoins la conjecture est prouvé fausse par Euler en 1732 qui montre que F_5 est composé. De nos jours, il a été prouvé que les nombres suivants jusqu'à F_{32} sont aussi composés mais on ne sait en revanche pas encore si les nombres de Fermat F_{33} et les suivants sont premiers ou non.

Revenons en aux polygones en prouvant le théorème suivant qui achève la classification des polynônes réguliers constructibles.

Théorème 35.9 (Gauss-Wantzel)**.** *Un polygone régulier à n côtés est constructible à la règle et au compas si et seulement si n est le produit d'une puissance de 2 et de nombres premiers de Fermat distincts.*

Démonstration. Si le polygone régulier à n côtés est constructible, alors le polygone régulier à $2n$ côtés est aussi constructible. En effet, il suffit de construire la bissectrice de l'angle de mesure $2\pi/n$ du premier polygone, ce qui peut se faire à la règle et au compas.

Soient n et m deux entiers premiers entre eux tels que les polygones réguliers à n côtés et m côtés soient tous les deux constructibles. D'après le théorème de Bezout, il existe deux entiers u et v tels que $un+vm = 1$. À partir des angles $2\pi/n$ et $2\pi/m$, on peut donc construire l'angle de mesure $2\pi/nm = v2\pi/n+u2\pi/m$ et donc construire le polygone régulier à nm côtés.

Ainsi, si n est le produit d'une puissance de 2 et de nombres premiers de Fermat distincts, alors le polygone régulier à n côtés est constructible.

Pour la réciproque, il suffit de remarquer que si le polygone régulier P à n côtés est constructible, alors pour tout diviseur d de n, le polygone régulier à d côtés étant contenu dans P, il est donc lui aussi constructible. □

Le théorème de Wantzel permet aussi de résoudre le problème datant de l'Antiquité de la duplication du cube : étant donné un cube de référence, est il possible de construire un cube ayant un volume deux fois plus grand ? Le rapport entre les côtés des deux cubes valant $\sqrt[3]{2}$, cela revient à se demander si $\sqrt[3]{2}$ est constructible. Or, le polynôme minimal de $\sqrt[3]{2}$ étant $X^3 - 2$ qui est de degré 3, le Corollaire 35.5 permet de répondre négativement à la question de départ.

Recasages

★★★★★ **102 :** *Groupe des nombres complexes de module* 1*. Sous-groupes des racines de l'unité. Applications.*

★★★★★ **125 :** *Extensions de corps. Exemples et applications.*

★★★★★ **151 :** *Dimension d'un espace vectoriel (on se limitera au cas de la dimension finie). Rang. Exemples et applications.*

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

★★★★ **141 :** *Polynômes irréductibles à une indéterminée. Corps de rupture. Exemples et applications.*

★★★★ **144 :** *Racines d'un polynôme. Fonctions symétriques élémentaires. Exemples et applications.*

★★★ **121 :** *Nombres premiers. Applications.*

★★★ **182 :** *Applications des nombres complexes à la géométrie.*

★★ **183 :** *Utilisation des groupes en géométrie.*

Références

[1] Jean-Claude CARRÉGA : Théorie des corps. *In Formation des enseignants*. Hermann, 2001.

[2] Patrice TAUVEL : *Corps commutatifs et théorie de Galois*. Calvage et Mounet, 2008.

36 Générateurs des isométries vectorielles et affines

Note des auteurs. Il s'agit d'un résultat classique concernant les générateurs des isométries qui possède un bon recasage. La preuve présentée ici est naturelle et assez élémentaire.

Contexte

Les *isométries* sont les transformations de l'espace qui conservent les distances, comme par exemple les rotations ou les translations de l'espace. Ces transformations interviennent notamment lorsque l'on s'intéresse aux symétries d'un objet de l'espace : ce sont les isométries qui fixent cet objet. Pour manipuler des groupes d'isométries, il est utile de trouver un système de générateurs « simples ». Pour démontrer une propriété sur ces groupes, il suffira alors de la démontrer uniquement sur ces générateurs. Dans ce développement, on montre que les réflexions jouent en quelque sorte le rôle des transpositions dans le groupe des permutations : ce sont des isométries faciles à étudier, involutives, qui engendrent le groupe des isométries.

On rappelle d'abord les notions de géométrie vectorielle et affine qui nous seront utiles.

Définition 36.1. *Étant donné un espace euclidien E, une* isométrie *de E est un endomorphisme u de E tel que $\|u(x)\| = \|x\|$ pour tout $x \in E$. L'ensemble des isométries de E forme un groupe, noté $\mathrm{O}(E)$.*

Une isométrie positive *de E est une isométrie de E de déterminant 1. L'ensemble des isométries positives de E forme un sous-groupe de $\mathrm{O}(E)$, noté $\mathrm{SO}(E)$.*

Définition 36.2. *Étant donné un sous-espace vectoriel H de E, la* symétrie orthogonale *par rapport à H, notée s_H, est l'endomorphisme de E qui vérifie pour tout $x \in H$ et $y \in H^\perp$ que*

$$s_H(x + y) = x - y.$$

Une réflexion *de E est une symétrie orthogonale par rapport à un espace de codimension 1. Un* retournement *de E est une symétrie orthogonale par rapport à un espace de codimension 2.*

Les symétries orthogonales sont des isométries mais toutes ne sont pas des symétries positives. En effet, une symétrie orthogonale par rapport à un sous-espace vectoriel H est une isométrie positive si et seulement si $\dim(H^\perp)$ est pair. En particulier, une réflexion n'est pas une isométrie positive, et son déterminant vaut donc -1.

Dans le cas d'un espace affine, il faut aussi prendre en compte le fait que des applications affines peuvent n'avoir aucun point fixe.

Définition 36.3. *Soit E un espace euclidien et $\mathcal{E}$ un espace affine euclidien sur E. Une* transformation affine *est un endomorphisme affine qui est bijectif. Une* translation affine *est une transformation affine dont la partie linéaire est l'identité. Une* réflexion affine *(resp.* retournement affine*) est une transformation affine dont la partie vectorielle est une réflexion (resp. retournement) et qui admet un point fixe.*

Lemme 36.4. *Soit $f \in \mathrm{Isom}(\mathcal{E})$. Alors il existe $g \in \mathrm{Isom}(\mathcal{E})$ et une translation affine t tels que g admette un point fixe et $f = t \circ g$.*

Lemme 36.5. *Soient u et v deux applications affines d'un espace affine $\mathcal{E}$. Alors $\overrightarrow{u \circ v} = \overrightarrow{u} \circ \overrightarrow{v}$.*

On utilisera également à plusieurs reprises des formules qui impliquent la dimension, comme le théorème du rang et la formule de Grassmann. En particulier, cette formule implique le lemme suivant :

Lemme 36.6. *Soient E un espace vectoriel de dimension finie et $H_1, \dots, H_p$ des hyperplans. Alors $\dim(H_1 \cap \cdots \cap H_p) \geq \dim(E) - p$.*

Démonstration. Ce résultat se montre par récurrence sur le nombre p d'hyperplans : si $p = 1$, alors $\dim(H_1) = \dim(E) - 1$ par définition d'un hyperplan. Supposons le résultat vrai à l'ordre p, et soient $H_1, \dots, H_{p+1}$ des hyperplans de E. On pose $F = \cap_{i=1}^{p} H_i$ et, d'après la formule de Grassman, on a

$$\dim(F) + \dim(H_{p+1}) = \dim(F + H_{p+1}) + \dim(F \cap H_{p+1}).$$

Par hypothèse de récurrence, et par définition d'un hyperplan, on obtient donc

$$\dim(E) - p + \dim(E) - 1 \leq \dim(F + H_{p+1}) + \dim(F \cap H_{p+1}).$$

Finalement, comme $F + H_{p+1} \subseteq E$, on a $\dim(F + H_{p+1}) \leq \dim(E)$ et on obtient bien que $\dim(E) - (p+1) \leq \dim(F \cap H_{p+1})$, ce qui achève la preuve. □

Développement

Théorème 36.7. *Soient E un $\mathbb{R}$-espace vectoriel euclidien et $u \in \mathrm{O}(E)$ une isométrie de E. En notant $r \overset{def}{=} \mathrm{rg}(u - \mathrm{Id})$, on a alors :*

- (i) *u est produit de r réflexions, mais pas moins ;*
- (ii) *si $u \in \mathrm{SO}(E)$ et $\dim(E) \geq 3$, alors u est produit d'au plus r retournements.*

Démonstration. (i) On montre d'abord l'existence d'une décomposition par récurrence sur r. Si $r = 0$, alors $u = \mathrm{Id}$ qui est produit de zéro réflexion. Soit $r \geq 1$ tel que la propriété soit vérifiée pour tout $u \in \mathrm{O}(E)$ avec $\mathrm{rg}(u - \mathrm{Id}) < r$, et soit