THEME: une démonstration du théorème de Wedderburn.

1 Introduction

Avant d'énoncer le théorème de Wedderburn, il faut effectuer une petite précision lexicale. La loi multiplicative d'un corps est généralement toujours supposée commutative. Ce ne sera pas le cas ici et on appellera corps un ensemble K muni de deux lois + et . telles que (K,+) ait une structure de groupe abélien et telles que (K\{0},.) ait une structure de groupe non nécessairement abélien. On dira alors qu'un corps est **commutatif** *si sa multiplication est commutative.*
Rappelons aussi qu'un corps est dit fini si son cardinal est fini.

Théorème de Wedderburn Tout corps fini est commutatif.

Afin d'établir la démonstration de ce théorème, il faut procéder à quelques rappels sur les racines de l'unité.

2 Racines de l'unité

Notons C le cercle trigonométrique, i.e.

$$C = \{z \in \mathbb{C} \ / \ |z| = 1\} = \left\{e^{i\theta} \ ; \ \theta \in \mathbb{R}\right\} = \left\{e^{i\theta} \ ; \ \theta \in [0\,;\,2\pi[\right\}.$$

Pour tout entier $n \geq 1$, on note R_n l'ensemble des racines n-ièmes de l'unité, à savoir

$$R_n = \{z \in \mathbb{C} \ / \ z^n = 1\}.$$

Bien sûr, $R_n \subset C$ et

$$R_n = \left\{e^{i\frac{2k\pi}{n}} \ ; \ k \in \{1, \cdots, n\}\right\}.$$

Ainsi, $card\,(R_n) = n$. Rappelons que R_n a une structure de groupe multiplicatif.

Définition On appelle **ensemble des racines entières de l'unité** l'ensemble $R = \bigcup_{n\geq 1} R_n$ où R_n désigne l'ensemble des racines n-ièmes de l'unité.

Proposition A toute racine entière de l'unité z, on peut associer l'idéal des entiers i tels que $z^i = 1$; cet idéal est non nul et son unique générateur strictement positif est le rang de z, noté ici $\rho\,(z)$.
Ainsi on a : $z \in R_n \ \Leftrightarrow \ \rho\,(z) \mid n$.

Démonstration Soit z une racine entière de l'unité. Il existe $n \in \mathbb{N}$ tel que $z^n = 1$. Par conséquent, l'ensemble $\mathcal{I}$ des entiers i tels que $z^i = 1$ est non vide. On vérifie facilement que c'est un idéal de $\mathbb{Z}$. Ce dernier étant principal, $\mathcal{I}$ est aussi principal et

donc monogène. Ceci permet d'être assuré que $\rho(z)$ est bien défini.

Rappelons aussi que, par définition, un élément de R est une racine primitive d$^{\text{ièmes}}$ de l'unité si et seulement si c'est un générateur de R_d. Enonçons la propriété:

Proposition Soit $d \geq 1$ un entier. Soit F_d désigne l'ensemble des racines primitives d$^{\text{ièmes}}$ de l'unité. Soit z une racine entière de l'unité et soit $\rho(z)$ son rang alors:

$$F_d = \{z \in R \ / \ \rho(z) = d\}.$$

On a, plus précisément,

$$F_d = \left\{ e^{i\frac{2k\pi}{d}} \ ; \ k \in \{1, \cdots, d\} \ et \ k \wedge d = 1 \right\}$$

où $k \wedge d$ désigne le pgcd de k et d.

Démonstration

- Démontrons l'inclusion de F_d dans $\{z \in R \ / \ \rho(z) = d\}$. Soit $z \in F_d$. z est donc un générateur de R_d. Rappelons que R_d est un groupe cyclique à d éléments. Par conséquent, pour tout élément $z' \neq 1$ de R_d, il existe $0 \leq i < d$ tel que $z' = z^i$ et $z^d = 1$. On a ainsi montré que $\rho(z) = 1$ et donc l'inclusion demandée. Démontrons l'inclusion réciproque. Soit z une racine entière de l'unité de rang d. Le sous groupe de R engendré par z est un sous groupe cyclique de R d'ordre d. Ce sous groupe contient alors toutes les racines du polynômes $X^d - 1 = 0$ car pour chaque élément z' de ce sous groupe, $z'^d = 1$. Ce sous groupe est par conséquent le groupe des racines d-ième de l'unité et z est bien un générateur de ce groupe.
- Montrons la seconde égalité. Soit z un élément de F_d. z est une racine entière de l'unité, donc il existe k et $n \in \mathbb{N}$ tels que $z = e^{i\frac{2k\pi}{n}}$. Comme $z^d = 1$, n est un diviseur de d. En particulier n≤d. Mais $z^n = 1$ donc n est élément de l'idéal engendré par d et donc $n \geq d$. En conclusion $n = d$ et $z = e^{i\frac{2k\pi}{d}}$. Montrons maintenant que $k \wedge d$=1. Si ce n'est pas le cas alors il existe un élément p de $\mathbb{N}$ tel que d=k.p et p<d. Mais $z^p = 1$, et le rang de z ne peut être d. Ceci est contraire à nos hypothèses. Donc forcément $k \wedge d = 1$. Pour démontrer l'inclusion réciproque, choisissons un élément $z = e^{i\frac{2k\pi}{d}}$ tel que $k \in \{1,...,d\}$ et tel que $k \wedge d = 1$. Montron que le rang m de cette racine entière de l'unité est égal à d. Il est évident que m est au plus égal à d. Supposons que m<d. Alors $z^m = 1$ implique $e^{i\frac{2k.m\pi}{d}} = 1$. Donc d divise k.m, mais comme d est premier avec k, en vertu du lemme de Gauss, d divise m ce qui est contraire au choix fait pour m. Donc d=m et z est de rang d. Par conséquent, comme les éléments de rang d sont les racines primitives d-ièmes de l'unité, l'inclusion réciproque est prouvée.

Définition Soit F_d l'ensemble des racines primitives d$^{\text{ièmes}}$ de l'unité. Le polynôme

$$\Phi_d(X) = \prod_{z \in F_d} (X - z)$$

est appelé **d$^{\text{ièmes}}$ polynôme cyclotomique**.

Etablissons maintenant quelques propriétés préalables à la démonstration du théorème de Weddenburn.

3 Propriétés préléminaires

Proposition (P1) Soient K un corps commutatif, $A \subset K$ un sous-anneau de K et $\Phi \in K[X]$. S'il existe un polynôme $Q \in A[X]$ unitaire tel que $\Phi.Q \in A[X]$, alors $\Phi \in A[X]$.

Démonstration Cette propriété se démontre assez simplement par récurrence sur $d^\circ\Phi$; néanmoins nous préférons une preuve plus " élégante ".

Notons $P = \Phi.Q \in A[X]$. Comme $Q \in A[X]$ est unitaire, il existe une unique division euclidienne de P par Q dans $A[X]$, i.e. il existe un unique couple (Q_1,R_1)de $A[X]^2$ tel que $P = Q_1Q + R_1$ et $d^\circ R_1 < d^\circ Q$.

D'autre part, K étant un corps, il existe une unique division euclidienne de P par Q dans $K[X]$, i.e. il existe un unique couple (Q_2,R_2)de $K[X]^2$ tel que $P = Q_2Q + R_2$ et $d^\circ R_2 < d^\circ Q$.

Comme $(Q_1,R_1) \in A[X]^2$ et que A est sous-anneau de K, on a $(Q_1,R_1) \in K[X]^2$; alors l'unicité du couple de division euclidienne de P par Q dans $K[X]$ implique que $(Q_1,R_1) = (Q_2,R_2)$.

Enfin, comme $P = \Phi.Q$, cette même unicité implique : $(Q_2,R_2) = (\Phi,0)$.

On a donc $(Q_1,R_1) = (\Phi,0)$, donc $\Phi = Q_1$, i.e. $\Phi \in A[X]$.

Proposition (P2) Soient L un corps fini, $K \subset L$ un sous-corps de L. Alors il existe $s \in IN^*$ tel que $card(L) = (card(K))^s$.

Démonstration

L'opération de $K \times L$ dans L définie par $k * l = kl$ (le produit dans L) induit sur L une structure de K-espace vectoriel. L est fini, donc de dimension finie s, et on a bien classiquement $card(L) = (card(K))^s$.

Proposition (P3) Soient m et n deux entiers avec $1 \leq m \leq n$, $T \in \mathbb{Z}(X)$ la fraction rationnelle définie par : $T(X) = \frac{X^n-1}{X^m-1}$, et Φ_n le n-ième polynôme cyclotomique.

Alors on a:

1. $X^n - 1 = \prod_{d \mid n} \Phi_d(X)$;
2. $\Phi_n \in \mathbb{Z}[X]$;

3. $m \mid n \Rightarrow T \in \mathbb{Z}[X]$;
4. $m \mid n \ et \ m < n \Rightarrow$ Φ_n divise le polynôme T dans $\mathbb{Z}[X]$.

Démonstration

1. Rappelons que l'ensemble des racines primitives d[ièmes] de l'unité F_d vérifie

$$F_d = \left\{ e^{i\frac{2k\pi}{d}} \ ; \ k \in \{1, \cdots, d\} \ et \ k \wedge d = 1 \right\}.$$

Un corollaire immédiat de cette égalité est, φ étant la fonction indicatrice d'Euler ($\varphi(d) = card\{k \in \{1,...,d\}, k \wedge d = 1\}$), $card(F_d) = \varphi(d)$.
D'autre part, l'ensemble des définitions implique aisément que $\{F_d\}_{d \mid n}$ forme une partition de R_n ; cela donne deux résultats intéressants :

$$card(R_n) = \sum_{d \mid n} card(F_d),$$

i.e.

$$n = \sum_{d \mid n} \varphi(d);$$

Identité des polynômes

$$\prod_{z \in R_n} (X - z) \text{ et } \prod_{d \mid n} \prod_{z \in F_d} (X - z).$$

En notant

$$\Phi_d(X) = \prod_{z \in F_d} (X - z),$$

le d-ième polynôme cyclotomique, et en développant $\prod_{z \in R_n} (X - z)$, cette identité donne :

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

Ceci est le 1/ de la propriété.

2. $\Phi_n \in \mathbb{Z}[X]$; montrons-le par récurrence sur n :
Pour $n = 1$, $\Phi_1(X) = X - 1$, donc $\Phi_1 \in \mathbb{Z}[X]$.
Supposons démontré jusqu'à n ; on a

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

ce qui entraîne que

$$X^{n+1} - 1 = \Phi_{n+1}(X) \cdot \prod_{\substack{d \mid n+1 \\ d \leq n}} \Phi_d(X).$$

La récurrence s'applique aux Φ_d avec $d \leq n$, et donc le polynôme

$$\prod_{\substack{d \,|\, n+1 \\ d \leq n}} \Phi_d(X)$$

appartient à $\mathbb{Z}[X]$. De plus il est clairement unitaire, et comme $\left(X^{n+1}-1\right) \in \mathbb{Z}[X]$, la propriété (P1) nous dit que $\Phi_{n+1} \in \mathbb{Z}[X]$: la récurrence est achevée.

3. $m \mid n \;\Rightarrow\; T \in \mathbb{Z}[X]$; montrons cela : $m \mid n$, donc l'ensemble des diviseurs de n est la réunion disjointe de l'ensemble des diviseurs de m et de l'ensemble Q des diviseurs de n ne divisant pas m ; par suite, on a

$$\prod_{d \,|\, n} \Phi_d(X) = \prod_{\delta \,|\, m} \Phi_\delta(X) \cdot \prod_{q \in Q} \Phi_q(X).$$

D'après 1/, cela donne

$$X^n - 1 = (X^m - 1) \cdot \prod_{q \in Q} \Phi_q(X).$$

La propriété (P1) nous dit alors que

$$\left(\prod_{q \in Q} \Phi_q(X) \right) \in \mathbb{Z}[X],$$

et par suite $T \in \mathbb{Z}[X]$ (car $T = \prod_{q \in Q} \Phi q$).

4. $m \mid n$ implique que

$$T = \prod_{q \in Q} \Phi_q \;\in \mathbb{Z}[X]$$

(c'est le point 3/), et $m < n$ implique que $n \in Q$, et par suite,

$$T = \Phi_n \cdot \prod_{q \in Q - \{n\}} \Phi_q,$$

puis (P1) implique que

$$\left(\prod_{q \in Q - \{n\}} \Phi_q \right) \in \mathbb{Z}[X],$$

et donc Φ_n divise le polynôme T dans $\mathbb{Z}[X]$.

Proposition (P4) Soit G un groupe fini (non nécessairement commutatif) agissant sur un ensemble E non vide fini ; soient $\{s_1, \cdots, s_r\} \subset E$ un système de représentants des orbites, et $G_1, \cdots, G_r$ les stabilisateurs respectifs de $s_1, \cdots, s_r$. Alors on a :

1. Pour tout i, $1 \leq i \leq r$, $card(G_i)$ divise $card(G)$;

2. Formule des classes:

$$card\,(E) = \sum_{1\leq i\leq r} \frac{card\,(G)}{card\,(G_i)}.$$

Démonstration

Ici aussi, rappel des faits... On dit qu'un groupe G (noté ici multiplicativement et d'élément neutre noté 1) agit sur un ensemble E (non vide) s'il existe une opération $(\cdot * \cdot)$ de $G \times E$ dans E telle que :

$$\forall x \in E,\ 1 * x = x$$

$$\forall x \in E,\ \forall\,(g,g') \in G \times G,\ g' * (g * x) = (g'g) * x.$$

On note alors, pour tout x de E :

– $G * x = \{g * x\}_{g\in G}$, sous-ensemble de E appelé orbite de x .

– $G_x = \{g \in G\ /\ g * x = x\}_{g\in G}$, sous-ensemble de G appelé stabilisateur de x .

– s_x l'application de G dans $G * x$ qui à $g \in G$ associe $g * x$.

G_x est un sous-groupe de G; d'autre part, on constate que la relation d'équivalence factorisant l'application s_x coïncide avec la relation de quotient $\frac{G}{G_x}$; comme il est clair que s_x est surjective, on en déduit que les ensembles $\frac{G}{G_x}$ et $G * x$ sont équipotents.

Enfin, il est aisé de vérifier que l'ensemble des orbites, $\{G * x\}_{x\in E}$, forme une partition de E.

Dans le cas où E et G sont finis, tout cela implique la formule des classes : en effet, soient $G * x_1, \cdots, G * x_r$ les orbites, alors elles forment une partition de E, donc

$$card\,(E) = \sum_{1\leq i\leq r} card\,(G * x_i).$$

Comme $G * x_i$ est équipotent à $\frac{G}{G_{x_i}}$, cela donne

$$card\,(E) = \sum_{1\leq i\leq r} card\left(\frac{G}{G_{x_i}}\right)$$

La démonstration s'achève en remarquant que

$$card\left(\frac{G}{G_{x_i}}\right) = \frac{card\,(G)}{card\,(G_{x_i})}.$$

Nous pouvons passer désormais à la démonstration du théorème.

4 Démonstration du théorème de Wedderburn

Démonstration Soit K un corps fini. On note Z le centre de K, i.e. l'ensemble des éléments de K qui commutent avec tous les autres. Z est un sous-corps de K.

Notons q le cardinal de Z ; la propriété (P2) nous dit alors qu'il existe un entier naturel non nul n tel que $card\,(K) = q^n$.

Nous allons supposer désormais que K n'est pas commutatif ;

Cela implique que $Z \neq K$, et donc que $n \geq 2$.

Pour tout $x \in K$, on note Z_x l'ensemble des éléments de K qui commutent avec x.

Alors Z_x est un sous-corps de K, et une extension de Z.

Z est un sous-corps de Z_x, donc d'après la propriété (P2) il existe un entier naturel non nul $d\,(x)$ tel que

$$card\,(Z_x) = q^{d(x)}.$$

Z_x est un sous-corps de K, donc la propriété (P2) nous dit qu'il existe un entier naturel non nul m tel que $card\,(K) = (card\,(Z_x))^m$.

Mais comme $card\,(K) = q^n$, donc on obtient

$$q^n = \left(q^{d(x)}\right)^m,$$

et donc $n = m\,d\,(x)$.

Retenons de cela que $d\,(x)$ **divise n pour tout x de K**.

Le groupe (multiplicatif) K^* agit sur l'ensemble K^* via l'opération de conjugaison $k * x = kxk^{-1}$. Vérifions cela :

$$1 * x = 1x1^{-1} = x,$$

$$k' * (k * x) = k'\,(k * x)\,k'^{-1} = k'\left(kxk^{-1}\right)k'^{-1} = (k'k)\,x\left(k^{-1}k'^{-1}\right) = (k'k)\,x\,(k'k)^{-1} = (k'k) * x.$$

Pour tout x de K^*, on note $K^* * x$ l' orbite de x, et $stab\,(x)$ le stabilisateur de x.

Pour tout y de K^*, on a

$$Z_y = stab\,(y) \ \cup \ \{0\}.$$

Ainsi,

$$card\,(stab\,(y)) = q^{d(y)} - 1.$$

On a de plus, pour x dans K^* :

$$card\,(K^* * x) = 1 \quad \Leftrightarrow \quad K^* * x = \{x\} \quad \Leftrightarrow \quad stab\,(x) = K^* \quad \Leftrightarrow \quad x \in Z^*.$$

Notons $z_0, \cdots, z_{q-1}$ les éléments de Z (avec $z_0 = 0$); d'après les équivalences ci-dessus, les orbites qui coupent Z^* sont exactement $K^* * z_1, \cdots, K^* * z_{q-1}$. Soient $K^* * y_1, \cdots, K^* * y_r$ les autres orbites ; alors la formule des classes nous donne :

$$card\,(K^*) = \sum_{1 \leq i \leq q-1} \frac{card\,(K^*)}{card\,(stab\,(z_i))} + \sum_{1 \leq i \leq r} \frac{card\,(K^*)}{card\,(stab\,(y_i))}.$$

Comme $stab\,(z_i) = K^*$, que $card\,(stab\,(y_i)) = q^{d(y_i)} - 1$, et que $card\,(K^*) = q^n - 1$, cela donne :

$$q^n - 1 = (q-1) + \sum_{1 \leq i \leq r} \frac{q^n - 1}{q^{d(y_i)} - 1},$$

et donc enfin :

$$q - 1 = (q^n - 1) - \sum_{1 \leq i \leq r} \frac{q^n - 1}{q^{d(y_i)} - 1}.$$

Considérons la fraction rationnelle

$$F\,(X) = (X^n - 1) - \sum_{1 \leq i \leq r} \frac{X^n - 1}{X^{d(y_i)} - 1}.$$

On a vu que pour tout i, $d\,(y_i)$ divise n, et la propriété (P3) nous permet alors de dire que $F \in \mathbb{Z}[X]$.

Mieux, il est clair que $d\,(y_i) < n$, en effet, $d\,(y_i) = n$ impliquerait $orb\,(y_i) = K^*$, et donc $y_i \in Z$, ce qui est faux.

Alors la propriété (P3) permet d'affirmer que le polynôme cyclotomique Φ_n divise le polynôme

$$\frac{X^n - 1}{X^{d(y_i)} - 1}$$

dans $\mathbb{Z}[X]$. Comme Φ_n divise aussi $(X^n - 1)$ dans $\mathbb{Z}[X]$, on obtient que Φ_n divise le polynôme F dans $\mathbb{Z}[X]$. Autrement dit :

Il existe un polynôme $Q \in \mathbb{Z}[X]$ tel que $F = Q\,\Phi_n$.

En particulier, cela implique

$$F\,(q) = Q\,(q)\ \Phi_n\,(q)\,.$$

Or (3) $F\,(q) = q - 1$, donc

$$q - 1 = Q\,(q)\ \Phi_n\,(q)\,.$$

Comme $Q \in \mathbb{Z}[X]$, $Q\,(q)$ est un entier, non nul car $q \neq 1$ (Z contient au moins 0 et 1). Ainsi cette dernière égalité implique que $|\Phi_n\,(q)| \leq q - 1$. Par conséquent il existe (au moins) une racine complexe u de Φ_n telle que $|q - u| \leq q - 1$.

Or u est racine primitive n-ième de l'unité, et comme $n \geq 2$, $u \neq 1$; comme la distance de q au cercle trigonométrique est atteinte en 1, on a facilement $|q - u| > q - 1$. Mais on vient de prouver l'inverse !

D'où l'absurdité, et la preuve que K est bien commutatif.