# Le théorème de Wedderburn

Mars 2005

## 1 Rappels sur les actions de groupes

On considère ici un groupe $G$ noté multiplicativement. Si $X$ est un ensemble quelconque, une action de $G$ dans $X$ est une application $G \times X \to X$, $(g, x) \longmapsto g.x$ vérifiant :

1. $\forall g, g' \in G, \forall x \in X, g.(g'.x) = (gg').x$,
2. $\forall x \in X, x.1 = x$.

On dit que le groupe $G$ agit sur $X$. A une telle action correspond une relation $\mathcal{R}$ d'équivalence dans $X$ définie par

$$x \mathcal{R} y \iff \exists g \in G, y = g.x.$$

On note $\omega(x)$ la classe d'un élément $x \in X$ et on l'appelle l'orbite de $x$, on a donc $\omega(x) = \{g.x \in X, g \in G\}$. Les classes d'une relation d'équivalence formant une partition de l'ensemble considéré, on peut considérer pour chaque orbite $\omega$ un $t \in X$ tel que $\omega = \omega(t)$ ; l'ensemble $T$ de ces $t$ est une transversale. On a donc

$$X = \bigcup_{t \in T} \omega(t),$$

cette réunion étant disjointe.

On vérifie facilement que l'ensemble $G_x = \{g \in G, g.x = x\}$ des éléments $g$ laissant invariant $x \in X$ est un sous-groupe de $G$ appelé stabilisateur de $x$.

On peut maintenant énoncer le résultat suivant, connu sous le nom d'équation aux classes.

**Proposition 1** *Soit $G$ un groupe fini agissant sur un ensemble fini $X$ et soit $T$ une transversale. Alors on a l'équation aux classes*

$$|X| = \sum_{t \in T} \omega(t) = \sum_{t \in T} \frac{|G|}{|G_t|}. \tag{1}$$

DEMONSTRATION : La première égalité est claire (puisque les orbites forment une partition). Nous voulons montrer maintenant $\omega(t) = |G|/|G_t|$.
Soit $x = g_0.t$ un élément de l'orbite $\omega(t)$. L'ensemble des $g$ tels que $x = g.t$ est la classe à gauche $g_0G_t$. Elle a même cardinal que $G_t$. Regroupons tous les éléments de $G$ qui appliquent $t$ sur un même élément $x$ de $\omega(t)$. On partage ainsi $G$ en $|\omega(t)|$ parties disjointes qui ont toutes pour cardinal $|G_t|$. On a donc $|G| = |G_t|.|\omega(t)|$. □

On considère maintenant le cas où l'ensemble $X$ est le groupe $G$ et on définit une action de $G$ sur lui-même par

$$\forall x, y \in G, \quad x.y = xyx^{-1}.$$

On dit alors que $G$ agit sur lui-même par automorphisme intérieur.
Pour cette action, le stabilisateur de $x \in G$ est l'ensemble des éléments qui commutent avec $x$ : $G_x = \{y \in G, xy = yx\}$.
Soit $T$ une transversale et $P$ l'ensemble des $t \in T$ tels que $\omega(t)$ soit réduit au singleton $\{t\}$. Autrement dit $P$ est le centre $Z(G)$ de $G$, c'est-à-dire $\{x \in G, \forall y \in G, xy = yx\}$. La formule 1 donne alors immédiatement

$$|G| = |Z(G)| + \sum_{t \in T \setminus P} \frac{|G|}{|G_t|}.$$

## 2 Le théorème de Wedderburn

La dernière formule de la section précédente va nous aider à démontrer le

**Théorème 2 (Wedderburn)** *Tout corps fini est commutatif.*

DEMONSTRATION : Soit $K$ un corps fini de centre $Z(K) = \{x \in K, \forall y \in K, xy = yx\}$. Il est clair que $Z$ est un sous-corps de $K$ et en tant que tel, $K$ est muni d'une structure de $Z$-espace vectoriel de dimension finie $n$. En dénombrant ses bases, on voit tout de suite que $|K| = q^n$ où $q$ est le cardinal de $Z$. Le théorème sera démontré lorsqu'on aura prouvé que $n = 1$ ; le raisonnement qui suit suppose que $n > 1$.

Faisons agir le groupe multiplicatif $K^*$ sur lui-même par automorphisme intérieur. Pour $x \in K^*$, on note $\omega(x)$ son orbite et $\text{Stab}(x) = \{y \in K^*, xy = yx\}$ son stabilisateur.
On vérifie que $\text{Stab}(x) \cup \{0\}$ est un sous-corps de $K$ contenant $Z$ et donc pour les même raisons que ci-dessus, il existe un entier $d(x)$ tel que $|\text{Stab}(x) \cup \{0\}| = q^{d(x)}$, c'est-à-dire tel que $|\text{Stab}(x)| = q^{d(x)} - 1$. De plus, il existe $k$ tel que $|K| = |\text{Stab}(x)|^k = q^{d(x)k} = q^n$ et c'est donc que $d(x)$ divise $n$. Il vient par

l'équation aux classes

$$|\omega(x)| = \frac{|K^*|}{|\text{Stab}(x)|} = \frac{q^n - 1}{q^{d(x)} - 1}.$$

Soit $\Phi_n$ le $n^{\text{ième}}$ polynôme cyclotomique définit par

$$\Phi_n(X) = \prod_{\xi \in \Delta_n} (X - \xi)$$

où $\Delta_n$ est l'ensemble des racines $n^{\text{ième}}$ primitives de l'unité. On rappelle que $\Phi_n$ est un polynôme unitaire à coefficients entiers et qu'on a la formule

$$X^n - 1 = \prod_{m|n} \Phi_m(X).$$

Puisque $d(x)$ divise $n$, cette formule entraîne

$$|\omega(x)| = \frac{\prod_{m|n} \Phi_m(q)}{\prod_{m|d(x)} \Phi_m(q)} = \prod_{\substack{m|n \\ m \not| d(x)}} \Phi(q).$$

En particulier pour $d(x) \neq n$, on voit que $\Phi_n(q)$ divise $\omega(x)$.L'équation aux classes nous donne

$$|K^*| = |Z^*| + \sum_{x \in T} |\omega(x)|$$

où $T$ est une transversale ne contenant pas les éléments dont l'orbite est ponctuelle. Cette formule s'écrit aussi

$$q^n - 1 = q - 1 + \sum_{x \in T} \frac{q^n - 1}{q^{d(x)} - 1}.$$

Mais dire que $x$ est dans $T$ implique que $d(x) \neq n$ de sorte que $\Phi_n(q)$ divise chaque terme de la somme et puisqu'il divise aussi $q^n - 1$,

$$\Phi_n(q) | q - 1. \tag{2}$$

Si $\xi$ désigne une racine $n^{\text{ième}}$ primitive de l'unité, un calcul simple donne

$$|\Phi_n(q)| = \Big| \prod_{\substack{m \leq n \\ m \wedge n = 1}} (q - \xi^m) \Big| > (q - |\xi^m|)^{\varphi(n)} \geq q - 1$$

où on a noté $\varphi$ la fonction d'Euler. Cette dernière inégalité combinées avec 2 fournie la contradiction recherchée. □