Différentes preuves du théorème de Wedderburn

A.— Preuve utilisant la formule des classes pour l'action de conjugaison : Soit K un corps fini de centre Z. Si $q = \sharp Z$ alors il existe $n \geq 1$ tel que $\sharp K = q^n$. On fait agir K^* sur lui-même par conjugaison. Pour tout $x \in K^*$, l'ensemble $N(x)$ constitué du stabilisateur de x auquel on a rajouté $\{0\}$ est un sous-corps de K. Il existe donc un entier $\delta(x) \geq 1$ divisant n tel que $\sharp N(x) = q^{\delta(x)}$. Par définition de Z, les orbites ponctuelles de K^* correspondent biunivoquement aux éléments de Z^*, si bien que, si l'on considère $x_1, \cdots, x_h$ une classe de représentants dans K^* des orbites, alors la formule des classes donne

$$q^n - 1 = \sharp K^* = \sharp Z^* + \sum_{i=1}^{h} \frac{K^*}{N(x_i)^*} = q - 1 + \sum_{i=1}^{h} \frac{q^n - 1}{q^{\delta(x_i)} - 1}$$

On considère alors le polynôme $P(X) = X^n - 1 - \sum_{i=1}^{h} \frac{X^n - 1}{X^{\delta(x_i)} - 1}$. La formule précédente se traduit par $P(q) = q - 1$. Les propriétés classiques des polynômes cyclotomiques montrent que le polynôme cyclotomique $\Phi_n(X)$ divise dans $\mathbb{Z}$ le polynôme $\frac{X^n-1}{X^d-1}$ pour tout diviseur d de n. Ainsi, $\Phi_n(X)$ est un diviseur de $P(X)$ et donc $\Phi_n(q)$ divise $q - 1$. Cette dernière propriété n'est possible que si $n = 1$, car si $n \geq 2$ alors $|q - \xi| > |q - 1|$ pour toute racine primitive n-ième de l'unité ξ. Ainsi, $n = 1$ et $K = Z$ est commutatif.

B.— Preuve utilisant le théorème de Skolem-Noether : Rappelons le théorème en question,

Théorème.— *Soient A une algèbre simple de dimension finie sur son centre k et B_1, B_2 deux sous-algèbres simples de A, k-isomorphes. Tout k-isomorphisme de B_1 sur B_2 se relève en un automorphisme intérieur de A.*

Considérons un corps fini K et notons k son centre. Pour des raisons de cardinalité, K une algèbre simple de dimension finie sur k. Les sous-corps commutatif maximaux de K ont même dimension sur k, ils ont donc même nombre d'éléments et sont donc isomorphes, puisque commutatifs. Le théorème de Skolem-Noether assure alors qu'ils sont conjugués deux-à-deux dans K.

Remarquons maintenant que si $x \in K$ alors le corps $k(x)$ est commutatif. Ainsi, tout élément de K^* est contenu dans un sous-corps commutatif maximal de K. Ainsi, si l'on considère un sous-corps commutatif maximal L, on a

$$K^* = \bigcup_{x \in K^*} xL^*x^{-1}$$

Pour l'action de conjugaison de K^* sur l'ensemble des groupes multiplicatifs des sous-corps commutatifs maximaux, le normalisateur de L^* contient L^*. On en déduit que le nombre n de parties xL^*x^{-1} est majoré par $[K^* : L^*]$.

Considérons des éléments $x_1, \cdots, x_n \in K^*$ tels que $K^* = \bigcup_{i=1}^{n} x_i L^* x_i^{-1}$. Puisque $\sharp K^* = \sharp L^*.[K^* : L^*] \leq \sharp \sum_{i=1}^{n} x_i L^* x_i^{-1} = n\sharp L^*$, on en déduit que $n = [K^* : L^*]$ et que, pour tout $i \neq j$, $x_i L^* x_i^{-1} \cap x_i L^* x_i^{-1} =$

$\emptyset$ (i.e. $K^* = \bigsqcup_{i=1}^{n} x_i L^* x_i^{-1}$). Puisque $1 \in x_i L^* x_i^{-1}$ pour tout $i = 1, \cdots, n$, on en déduit finalement que $n = 1$ et donc que $K = L$.

C.— Preuve utilisant la cohomologie des groupes cycliques : Considérons un corps fini K et notons k son centre. En tant que k-algèbre simple centrale, K possède un corps neutralisant L, qui est une extension commutative finie de k. Puisque L est un corps neutralisant de K, la classe de K dans le groupe de Brauer de k est dans le noyau de l'application canonique $\mathrm{Br}(k) \longrightarrow \mathrm{Br}(L)$. La théorie du groupe de Brauer assure que le noyau de ce morphisme est isomorphe au groupe de cohomologie $\mathrm{H}^2(\mathrm{Gal}(L/k), L^*)$. Nous allons montrer que ce dernier est nul, ce qui prouvera que la classe de K dans $\mathrm{Br}(k)$ est trivial, c'est-à-dire que $K = k$.

La théorie de Galois assure que $\mathrm{Gal}(L/k)$ est un groupe cyclique, le groupe L^* est lui aussi cyclique et le théorème 90 d'Hilbert assure que $\mathrm{H}^1(\mathrm{Gal}(L/k), L^*) = 0$. La preuve s'achève en considérant le résultat classique de cohomologie des groupes cycliques :

Proposition.— *Soit C un groupe cyclique et G un C-groupe abélien. Si G est fini, alors $\mathrm{H}^1(C, G)$ et $\mathrm{H}^2(C, G)$ sont des groupes finis de même ordre (i.e. le quotient de Herbrand vaut 1).*

Les preuves qui suivent visent à montrer que le groupe de Brauer d'un corps fini (commutatif) est trivial. Cette propriété équivaut en fait au théorème de Wedderburn. En effet, si K est un corps fini, dire que K est commutatif équivaut à dire qu'il est égal à son centre k, ce qui équivaut bien à dire que $\mathrm{Br}(k)$ est trivial pour tout corps commutatif fini k.

D.— Preuve utilisant théorème de Chevalley-Waring : Rappelons le théorème en question,

Théorème.— *Soient k un corps fini (commutatif), un ensemble fini d'indices I et pour tout $i \in I$, $f_i(X_1, \cdots, X_n) \in k[X_1, \cdots, X_n]$ un polynôme sans terme constant. Si $\sum_{i \in I} d^\circ f_i < n$, alors les f_i possèdent un zéro non trivial en commun.*

En particulier, les corps finis (commutatifs) sont C^1, c'est-à-dire qu'ils vérifient que *toute forme de degré d en n variables possède un zéro non trivial dés que $d < n$.* Les corps C^1 ont toujours un groupe de Brauer trivial. Donnons quelques explications sur ce dernier point :

Soient k est un corps C^1 et L/k une extension finie de degré n. Si l'on choisit une k-base $(e_1, \cdots, e_n)$ de L, alors pour tout $z \in k^*$, l'application $f : k^{n+1} \longrightarrow k$ définie par

$$f(x_1, \cdots, x_n, x_{n+1}) = N_{L/k}(x_1 e_1 + \cdots + x_n e_n) - x_{n+1}^n z$$

est une forme de degré n en $n+1$ variable. Elle possède donc un zéro $(x_1, \cdots, x_n, x_{n+1})$ non trivial et ce dernier ne peut pas vérifier que $x_{n+1} = 0$. On a donc $z = N_{L/k}(\frac{x_1}{x_{n+1}} e_1 + \cdots + \frac{x_n}{x_{n+1}} e_n)$. On vient donc de montrer que la norme $N_{L/k}$ est surjective pour tout extension finie L/k. Cette dernière propriété est équivalente au fait que le groupe de Brauer de toute extension algébrique de k est trivial (voir [Serre, Cohomologie galoisienne, 3.1. Proposition 5.]). En particulier, $\mathrm{Br}(k) = 0$.

E.— Preuve utilisant la dimension cohomologique : Soit k un corps fini (commutatif). On sait que $k \simeq \mathbb{F}_q$ avec $q = p^a$ une puissance d'un nombre premier. La théorie de Galois montre que, pour tout $n \geq 1$, k possède une et une seule extension de degré n : $\mathbb{F}_{q^n}$. L'extension $\mathbb{F}_{q^n}/\mathbb{F}_q$ est cyclique

et comme on a l'extension $\mathbb{F}_{q^m}/\mathbb{F}_{q^n}$ si et seulement si $n|m$, on en déduit que

$$\mathrm{Gal}(\bar{k}/k) = \varprojlim \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) \simeq \varprojlim \mathrm{Gal}\mathbb{Z}/n\mathbb{Z} = \widehat{\mathbb{Z}}$$

Le groupe profini $\widehat{\mathbb{Z}}$ est prolibre (de rang 1), il est donc projectif (i.e. sa dimension cohomologique est ≤ 1). D'après [Serre, Cohomologie galoisienne, 3.1. Proposition 5.], cette propriété équivaut aussi à dire que le groupe de Brauer de toute extension algébrique de k est trivial.