Le théorème de Wedderburn

Gabriel Chênevert

Exposé final dans le cadre du cours MAT 7600
Novembre 2001

Ce texte se veut un bref aperçu historique et comparatif des différentes preuves ayant été trouvées, au cours du dernier siècle, du théorème suivant, qui est un bel exemple d'un résultat non trivial s'énonçant simplement.

Théorème 1 (Wedderburn, 1905) *Tout corps fini est commutatif.*

Mettons-nous tout d'abord dans le contexte de la découverte de ce théorème. W. R. Hamilton, au XIX^{e} siècle, conscient de l'interprétation des nombres complexes en tant que couples de nombres réels, s'est demandé pendant longtemps comment définir une multiplication sur $\mathbb{R}^3$ afin d'obtenir une structure de corps. Il s'est aperçu en 1843 que c'était impossible, et qu'il devait nécessairement passer en dimension 4 pour définir les **quaternions** comme l'ensemble $\mathbb{H}$ des nombres de la forme $a + bi + cj + dk$, où a, b, c et d sont des nombres réels et i, j, k vérifient les relations

$$i^2 = j^2 = k^2 = ijk = -1.$$

Il s'agit du premier exemple connu de corps non commutatif. D'autres exemples ont été découverts par la suite, et ils étaient tous infinis. E. H. Moore ayant prouvé quelques années plus tôt que tous les corps commutatifs finis étaient des corps de Galois, il était légitime au début du XX^{e} siècle de se demander s'il existait des corps finis non commutatifs. Cette question était également pertinente dans le contexte de l'introduction de coordonnées en géométrie projective, sujet assez en vogue à l'époque.

H. S. M. Wedderburn annonça son théorème à des collègues de l'université de Chicago en 1905, notamment à L. E. Dickson, qui doutait de la véracité du résultat. En lui cherchant un contre-exemple, il en trouva une preuve, qu'il publia [1] en attribuant la paternité du résultat à Wedderburn. Celui-ci, après avoir vu la preuve de son collègue, s'en est inspiré pour écrire deux nouvelles preuves utilisant la même idée, qu'il publia avec sa preuve originale [2]. Or, il s'avéra par la suite qu'il y avait une faille dans la preuve originale de Wedderburn, de sorte que c'est en fait Dickson qui a trouvé la première preuve correcte du théorème.

1 La preuve de Dickson

Soit K un corps fini (non nécessairement commutatif). Pour chaque élément $x \in K$, soit $C_x := \{\, y \in K \mid xy = yx \}$ le **centralisateur** de x dans K.

Lemme 1 *C_x est un sous-corps de K.*

Preuve: Il est clair que 0 et 1 sont dans C_x. Par ailleurs, si y, $z \in C_x$, on a

$$x(-y) = -(xy) = -(yx) = (-y)x,$$

$$x(y+z) = xy + xz = yx + zx = (y+z)x \quad \text{et}$$

$$x(yz) = (xy)z = (yx)z = y(xz) = y(zx) = (yz)x,$$

donc $-y$, $y+z$, $yz \in C_x$. De plus, si $y \neq 0$, puisque $xy = yx$, on trouve $y^{-1}xy = x$, et donc $y^{-1}x = xy^{-1}$, ce qui prouve que $y^{-1} \in C_x$. ■

Considérons maintenant $C := \{\, y \in K \mid \forall_{x \in K}\ xy = yx \}$ le **centre** de K. Remarquons que $C = \bigcap_{x \in K} C_x$ est un sous-corps de K qui est commutatif. On peut considérer K et chaque C_x comme espaces vectoriels sur C, de dimensions respectives n, n_x. On remarque donc que $|K| = q^n$ et $|C_x| = q^{n_x}$ où $q := |C| \geq 2$.

Par ailleurs, chaque n_x divise n, puisqu'on vérifie facilement en prenant des bases que $n = m_x n_x$, où m_x désigne la dimension de K considéré comme espace vectoriel (à gauche) sur le corps C_x.

Rappelons que dans un groupe fini G, on obtient, en considérant la partition de G en classes de conjugaison, l'**équation de classes**

$$|G| = |C(G)| + \sum_x \frac{|G|}{|C_G(x)|}$$

où $C(G)$ désigne le centre de G, $C_G(x)$ le centralisateur dans G d'un élément x, et où la somme est prise sur l'ensemble des classes de conjugaison des éléments x non centraux.

En appliquant cette équation au groupe multiplicatif $K^* = K \backslash \{0\}$ de K, pour lequel $C(K^*) = C^*$ et $C_{K^*}(x) = C_x^*$, on obtient la formule

$$q^n - 1 = q - 1 + \sum_x \frac{q^n - 1}{q^{n_x} - 1} \tag{1}$$

dans laquelle chaque n_x est un diviseur propre de n (en effet, on sait déjà que n_x divise n, et il est impossible que $n_x = n$, car on aurait alors $C_x = K$, ce qui est impossible puisque x est un élément qui n'est pas dans le centre). Pour montrer que K est commutatif, i.e. que $K = C$, il suffit de montrer que l'équation (1) ne peut être satisfaite que pour $n = 1$.

Pour ce faire, Dickson a invoqué le résultat suivant, dont on peut trouver une preuve dans [3].

Théorème 2 (Zsigmondy, 1882) *Sauf si $q = 2^k - 1$, $n = 2$ ou si $q = 2$, $n = 6$, il existe un nombre premier p tel que p divise $q^n - 1$ mais ne divise aucun des entiers $q^m - 1$ pour $m < n$.*

Si on peut trouver un tel nombre premier p, on remarque qu'il doit diviser chacun des termes $(q^n - 1)/(q^{n_x} - 1)$ apparaissant dans (1), et puisque p divise $q^n - 1$, (1) implique que p doit également diviser $q - 1$. Or, d'après le choix de p, ceci implique que $n = 1$.

Pour terminer la preuve du théorème de Wedderburn, il ne reste plus qu'à vérifier que les cas exceptionnels $q = 2^k - 1$, $n = 2$ et $q = 2$, $n = 6$ ne peuvent pas se produire.

Tout d'abord, si $n = 2$, K serait un espace vectoriel de dimension 2 sur C, et puisque tout ensemble libre peut être étendu à une base, on trouverait une base $\{1, \alpha\}$ de K en tant que C-espace vectoriel. Mais alors chaque élément de K s'écrirait (uniquement) de la forme $a + b\alpha$ avec a, $b \in C$, et on vérifie facilement que deux éléments de cette forme commutent. Ceci voudrait dire que K est commutatif, donc que $K = C$, ce qui est impossible puisqu'on a supposé $n = 2$.

Maintenant, si on suppose que $q = 2$ et $n = 6$, alors les n_x ne peuvent prendre que les valeurs 1, 2 ou 3, et dans ce cas l'équation (1) prend la forme

$$62 = 63x + 21y + 9z$$

où x, y et z sont des entiers, ce qui est impossible puisque 63, 21 et 9 sont divisibles par 3, mais 62 ne l'est pas.

Ceci termine la preuve du théorème de Wedderburn en admettant le théorème de Zsigmondy. La preuve de Dickson souffre donc du fait qu'elle dépend lourdement de ce théorème

non trivial de théorie des nombres, et aussi du fait qu'on doive traiter certains cas séparément. Soulignons que les deux preuves correctes de Wedderburn, basées sur celle de Dickson, utilisent également le résultat de Zsigmondy.

2 La preuve de Witt

Certains algébristes, fascinés par le théorème de Wedderburn, tentèrent dans les années suivantes de simplifier cette preuve ou d'en trouver une autre plus élégante. E. Artin [4] en trouva une en 1927 qui n'utilisait pas d'argument de divisibilité, mais elle était relativement technique. Il fallu attendre 1930 pour que E. Witt publie [5] la preuve du théorème de Wedderburn considérée encore aujourd'hui comme la plus élégante, et que l'on retrouve notamment dans [6] et dans la plupart des livres standards d'algèbre (souvent en exercice !).

La preuve de Witt débute comme celle de Dickson en établissant l'équation de classes (1) pour le groupe multiplicatif K^*. Pour montrer que cette équation implique que $n = 1$, il utilise certains résultats de base sur les polynômes cyclotomiques que nous allons maintenant développer.

Soit $W_n := \{\, x \in \mathbb{C} \,|\, x^n = 1\}$ l'ensemble des racines complexes n^{e} de l'unité. On sait que W_n est un groupe cyclique d'ordre n, engendré par $e^{2\pi i/n}$. Soit maintenant W_n^* l'ensemble des éléments d'ordre n dans W_n, i.e. l'ensemble des générateurs de W_n. Définissons maintenant le n^{e} **polynôme cyclotomique** Φ_n comme étant le polynôme monique dont les racines sont exactement les éléments de W_n^*, i.e.

$$\Phi_n(x) := \prod_{\zeta \in W_n^*} (x - \zeta).$$

Le théorème de Lagrange pour les groupes finis nous apprend que W_n est l'union disjointe des différents W_d^* où d divise n, ce qui nous donne la relation suivante entre les Φ_d :

$$x^n - 1 = \prod_{\zeta \in W_n} (x - \zeta) = \prod_{d|n} \prod_{\zeta \in W_d^*} (x - \zeta) = \prod_{d|n} \Phi_d(x). \tag{2}$$

Le fait remarquable à propos des polynômes cyclotomiques est que, bien qu'ils soient définis en terme de racines complexes de l'unité, ce sont en fait tous des polynômes sur $\mathbb{Z}$.

Lemme 2 *Chaque Φ_n est un polynôme à coefficients entiers dont le terme constant est ± 1.*

Preuve: Montrons ceci par induction sur n. L'énoncé est certainement vrai pour $n = 1$ puisque $\Phi_1(x) = x - 1$. Pour $n > 1$, l'équation (2) nous donne

$$x^n - 1 = \Phi_n(x) \prod_{\substack{d|n \\ d<n}} \Phi_d(x) \tag{3}$$

où $\prod_d \Phi_d(x)$ est un polynôme à coefficients entiers dont le terme constant est ± 1 par l'hypothèse d'induction. Si on écrit $\Phi_n(x) = \sum_i a_i x^i$ et $\prod_d \Phi_d(x) = \sum_j b_j x^j$, où chaque $b_j \in \mathbb{Z}$ et $b_0 = \pm 1$, on trouve $a_0 b_0 = -1$, d'où $a_0 = \mp 1$, et pour chaque $1 \leq k \leq n$, en posant $\epsilon_k := 0$ si $k < n$ et $\epsilon_n := 1$, on a :

$$\sum_{i=0}^{k} a_i b_{k-i} = \epsilon_k, \quad \text{d'où} \quad a_k = \mp \left(\epsilon_k - \sum_{i=0}^{k-1} a_i b_{k-i} \right) \in \mathbb{Z}.$$

■

Utilisons maintenant les propriétés des polynômes cyclotomiques pour montrer qu'il est impossible que l'équation (1) soit vérifiée si $n > 1$.

Remarquons que le lemme nous assure que $\Phi_n(q)$ est un entier, qui de plus divise $q^n - 1$ d'après l'équation (3). De même, pour chaque n_x, qui est un diviseur propre de n, on a

$$q^n - 1 = \Phi_n(q) \prod_{d|n_x} \Phi_d(q) \prod_{\substack{d|n \\ d\nmid n_x}} \Phi_d(q) = \Phi_n(q)(q^{n_x} - 1) \prod_{\substack{d|n \\ d\nmid n_x}} \Phi_d(q)$$

ce qui prouve que $\Phi_n(q)$ divise chaque $(q^n - 1)/(q^{n_x} - 1)$.

En observant (1), on remarque que ceci implique que $\Phi_n(x)$ divise $q - 1$. Nous allons maintenant montrer que ceci est impossible si $n > 1$.

En effet, soit $\zeta \in W_n^*$. Puisque $n > 1$, on sait que $\zeta \neq 1$. Si on écrit $\zeta = a + bi$ avec a, $b \in \mathbb{R}$, on sait donc que $a < 1$. Mais alors

$$\begin{aligned} |q - \zeta|^2 &= (q - a)^2 + b^2 = q^2 - 2aq + a^2 + b^2 \\ &= q^2 - 2aq + |\zeta|^2 = q^2 - 2aq + 1 \\ &> q^2 - 2q + 1 = (q - 1)^2 \end{aligned}$$

et donc $|q - \zeta| > q - 1$.

Puisque $n \geq 2$, on trouve donc

$$|\Phi_n(q)| = \prod_{\lambda \in W_n^*} |q - \lambda| \geq |q - \zeta| > q - 1$$

ce qui est bien sûr impossible puisque $\Phi_n(q)$ divise $q - 1$.

Cet argument permet donc de conclure que $n = 1$, et donc que $K = C$ est un corps commutatif. Malgré le fait qu'elle nécessite l'introduction des polynômes cyclotomiques, la preuve de Witt est donc une preuve élémentaire du théorème de Wedderburn qui n'utilise aucun résultat externe.

3 La preuve de van der Waerden

Quelques années plus tard, en 1949, on trouve dans le livre classique de B. L. van der Waerden [7] une autre preuve du théorème de Wedderburn, qui apparaît également dans un livre de Jacobson publié en 1956 [8]. Cet argument repose sur le lemme suivant, dont la preuve demande une bonne compréhension des extensions de corps.

Lemme 3 *Tous les sous-corps commutatifs maximaux de K sont conjugués, i.e. si F et F' sont deux sous-corps commutatifs maximaux de K, alors il existe un élément $x \in K^*$ tel que $F' = xFx^{-1}$.*

Si on admet ce résultat, dont une preuve élémentaire n'utilisant que la diagonalisation des opérateurs linéaires est donnée dans [9], il est aisé de terminer la preuve de van der Waerden en utilisant l'affirmation suivante.

Lemme 4 *Un groupe G fini ne peut pas être décomposé en conjugués d'un de ses sous-groupes propres, i.e. si $H < G$ est un sous-groupe propre de G, alors $G \neq \bigcup_{g \in G} gHg^{-1}$.*

Preuve: D'après le théorème de Lagrange, $|G| = (G : H)|H|$. Or, remarquons que si deux éléments g, g' de G sont dans le même translaté de H, alors il existe un $h \in H$ tel que $g' = gh$, et alors

$$g'H(g')^{-1} = (gh)H(gh)^{-1} = (gh)H(h^{-1}g^{-1}) = g(hHh^{-1})g^{-1} = gHg^{-1}$$

et donc les conjugués de H par g et g' sont les mêmes. Il ne peut donc y avoir au maximum que $(G : H)$ conjugués distincts de H dans G. Or, puisqu'ils contiennent tous exactement $|H|$

éléments, pour que leur union donne le groupe G au complet, il faudrait qu'ils soient tous distincts, ce qui n'est pas le cas puisqu'ils contiennent tous le neutre. ■

Puisque le corps fini K contient des sous-corps commutatifs (par exemple son centre C), il contient certainement au moins un sous-corps commutatif maximal F. De plus, chaque élément $x \in K$ est contenu dans un sous-corps commutatif maximal, puisque $C[x]$ est un anneau intègre fini, donc un corps commutatif; il est donc contenu dans un sous-corps commutatif maximal F_x de K. On obtient donc $K = \bigcup_{x \in K} F_x$, et puisque chaque F_x est conjugué à F dans K, le groupe fini K^* s'écrit donc comme l'union des conjugués de F^*, ce qui implique d'après le lemme précédent que $F^* = K^*$, d'où $K = F$ est commutatif.

4 La preuve de Kaczynski

Plusieurs autres arguments purement algébriques ont été trouvés par la suite. En particulier, H. J. Zassenhaus donna en 1952 une preuve n'utilisant que des notions de théorie des groupes [10]. Il prouva d'abord le théorème suivant.

Théorème 3 (Zassenhaus, 1952) *Un groupe fini est abélien si et seulement le normalisateur de chacun de ses sous-groupes abéliens coïncide avec le centralisateur de ce sous-groupe.*

La preuve de ce théorème est relativement technique et nécessite la discussion de plusieurs cas. Par la suite, il faut également vérifier que le groupe multiplicatif K^* d'un corps fini vérifie la condition du théorème, ce qui est également passablement technique.

Par la suite, I. N. Herstein [11] a trouvé en 1961 une preuve du théorème de Wedderburn n'utilisant que des manipulations algébriques élémentaires en théorie des anneaux avec les éléments de K, mais qui est, tout comme celle d'Artin, relativement technique et tortueuse.

Quelques années plus tard, en 1964, T. J. Kaczynski [12] (mieux connu sous le surnom tristement célèbre de Unabomber) trouva une preuve n'utilisant que des résultats de théorie des groupes finis. Esquissons ici les grandes lignes de cette preuve. Il est intéressant de noter qu'elle dépend du fait que le groupe multiplicatif K^* ne peut contenir aucun sous-groupe isomorphe au **groupe des quaternions** $Q := \{\pm 1, \pm i, \pm j, \pm k\} < \mathbb{H}^*$. Pour prouver ceci, nous avons besoin du lemme suivant.

Lemme 5 *L'équation $x^2 + y^2 = -1$ admet toujours une solution dans le corps de Galois $\mathbb{F}_p$ à p éléments.*

Preuve: On peut trouver la preuve suivante dans [6]. Les carrés distincts dans $\mathbb{F}_p$ sont les éléments 0^2, 1^2, ..., h^2 où $h := \lfloor p/2 \rfloor + 1$. On le vérifie facilement en utilisant le fait que pour $x, y \in \mathbb{F}_p$, $x^2 = y^2$ si et seulement si $x^2 - y^2 = (x-y)(x+y) = 0$, i.e. si et seulement si $x = \pm y$. Par ailleurs, il y a aussi dans $\mathbb{F}_p$ exactement h éléments de la forme $-1 - x^2$ puisqu'il y en a le même nombre que de carrés. Or

$$2h = 2\left(\left\lfloor \frac{p}{2} \right\rfloor + 1\right) = 2\left\lfloor \frac{p}{2} \right\rfloor + 2 \geq (p-1) + 2 = p + 1 > p = |\mathbb{F}_p|,$$

donc l'ensemble des carrés et celui des éléments de la forme $-1 - x^2$ n'ont pas assez de place dans $\mathbb{F}_p$ pour être disjoints, il doit donc nécessairement y avoir dans $\mathbb{F}_p$ un élément qui est à la fois de la forme y^2 et de la forme $-1 - x^2$, donnant la solution (x, y) cherchée. ■

Lemme 6 *Si K est un corps fini, K^* ne contient aucun sous-groupe isomorphe à Q.*

Preuve: Supposons que K^* contienne un sous-groupe

$$Q = < \sigma, \tau \mid \sigma^4 = \tau^4 = 1, \sigma^2 = \tau^2, \tau\sigma = \sigma^3\tau >$$

isomorphe au groupe des quaternions. Puisque σ^2, τ^2 et $(\sigma\tau)^2$ sont des éléments d'ordre 2 dans Q, et que le seul élément qui peut être d'ordre 2 dans le groupe multiplicatif d'un corps est -1, on trouve $\sigma^2 = \tau^2 = (\sigma\tau)^2 = -1$, de sorte que $Q = \{\pm 1, \pm\sigma, \pm\tau, \pm\sigma\tau\}$. Puisque ces éléments sont tous distincts, on en conclut au passage que la caractéristique de K est différente de 2. Notons p la caractéristique de K et $\mathbb{F}_p \subseteq C$ son corps caractéristique. Si x et y sont les éléments de $\mathbb{F}_p$ dont l'existence est assurée par le lemme précédent, on trouve

$$(x\sigma + y\tau)^2 = x^2\sigma^2 + xy\sigma\tau + xy\tau\sigma + y^2\tau^2 = -x^2 + xy(\sigma\tau + \tau\sigma) - y^2 = -(x^2 + y^2) = 1$$

puisque $\tau\sigma = -\sigma\tau$, d'où $x\sigma + y\tau = \pm 1$. Or ceci implique que $x\sigma + y\tau$ commute avec σ, ce qui force $y = 0$, et avec τ, ce qui force $x = 0$, et on obtient donc $0 = x\sigma + y\tau = \pm 1$, une contradiction. ■

L'idée de la preuve de Kaczynski consiste à remarquer que chaque p-Sylow-sous-groupe non trivial de K^* contient un unique sous-groupe cyclique d'ordre p. Or, un théorème sur les p-groupes nous apprend que ceci ne peut être le cas que si chaque p-Sylow-sous-groupe est cyclique ou bien est un groupe de quaternions généralisé. Puisque les groupes de quaternions généralisés contiennent tous Q comme sous-groupe, le lemme précédent permet d'écarter cette possibilité, de sorte que tous les sous-groupes de Sylow de K^* sont cycliques, ce qui en fait un groupe **métacyclique**. Après quelques manipulations, on peut conclure qu'il est en fait cyclique, donc abélien, et donc que K est commutatif.

Quelques années plus tard, en 1969, S. Ebey et K. Sitaram publièrent [13] une preuve semblable invoquant des résultats sur les groupes de Frobenius pour certaines étapes de l'argument.

Par la suite, quelques autres preuves firent leur apparition, notamment celle de J. Carcanague en 1971 [14] utilisant la théorie de Galois, et la très belle preuve élémentaire de J. Schue [15] en 1988 qui mélange certains ingrédients des preuves de Hernstein et de Witt, en utilisant l'équation de classes et la correspondance de Galois.

5 Généralisations

Le théorème de Wedderburn a suscité à partir des années 40 beaucoup de recherche sur la commutativité des anneaux, dont le résultat le plus connu est probablement celui-ci.

Théorème 4 (Jacobson, 1945) *Soit A un anneau pour lequel pour chaque élément $x \in A$, il existe un entier $n_x > 1$ tel que $x^{n_x} = x$. Alors A est commutatif.*

On obtient facilement le théorème de Wedderburn comme corollaire du théorème de Jacobson, puisque si K est un corps fini, chaque élément $0 \neq x \in K$ est un élément du groupe fini K^*, donc il est d'ordre fini m_x. En posant $n_x := m_x + 1$ pour $x \neq 0$ et $n_0 := 2$, on vérifie que K satisfait l'hypothèse du théorème de Jacobson, donc K est commutatif.

Voici une autre généralisation qu'on peut déduire facilement du théorème de Wedderburn, mentionnée dans [16].

Théorème 5 *Soit G un sous-groupe fini du groupe multiplicatif d'un corps K de caractéristique $p \neq 0$. Alors G est cyclique.*

Preuve: Soit F un sous-corps commutatif fini de K (par exemple, on peut prendre son corps primitif $\mathbb{F}_p$). Considérons l'ensemble

$$L := \left\{ \sum_i a_i g_i \;\middle|\; a_i \in F, g_i \in G \right\}.$$

On vérifie aisément que L est un sous-anneau fini de K contenant 1, c'est donc un sous-corps de K. Par le théorème de Wedderburn, L est un corps commutatif fini, et puisque G est un sous-groupe de L^*, on conclut que G est cyclique. ■

Remarquons que ce résultat n'est pas vrai en caractéristique 0, puisque le groupe multiplicatif $\mathbb{H}^*$ des quaternions contient Q comme sous-groupe, qui n'est pas cyclique.

On peut aussi utiliser les techniques développées pour prouver le théorème de Wedderburn afin d'obtenir des théorèmes sur la commutativité de groupes finis, comme l'a fait Grundhöfer [17].

Par ailleurs, on peut obtenir le théorème de Wedderburn comme un corollaire de résultats plus généraux sur la structure des algèbres.

6 Mot de la fin

Les preuves exposées ici utilisent toutes de façon astucieuse les rapports entre les différentes structures en jeu: groupe multiplicatif, groupe additif, espace vectoriel sur certains sous-corps, en plus de la structure imposée par les cardinalités des ensembles. Chaque preuve utilise également certains résultats non triviaux provenant de différentes parties de l'algèbre: théorie des nombres, polynômes cyclotomiques, théorie des groupes finis, algèbre linéaire, théorie des anneaux, illustrant bien le principe de conservation de la difficulté en mathématiques.

Références

[1] L. E. Dickson, *On finite algebras*, Göttingen Nachr., 1905, pp. 358-393.

[2] J. H. M. Wedderburn, *A theorem on finite algebras*, Trans. Amer. Math. Soc., vol. 6, 1905, pp. 349-352.

[3] G. D. Birkhoff et H. S. Vandiver, *On the integral divisors of $a^n - b^n$*, Annals Math. (2), vol. 5, 1904, pp. 173-180.

[4] E. Artin, *Über einen Satz von Herrn J. H. MacLaglan Wedderburn*, Abh. Math. Sem. Univ. Hamburg, vol. 5, 1927, pp. 245-250.

[5] E. Witt, *Über die Kommutativität endlicher Schiefkörkper*, Abh. Math. Sem. Univ. Hamburg, vol. 8, 1931, p. 413.

[6] M. Aigner et G. M. Ziegler, *Proofs from the Book*, Springer, Berlin, New York, 1999.

[7] B. L. van der Waerden, *Modern algebra*, Ungar, New York, 1949.

[8] N. Jacobson, *Structure of rings*, AMS Colloq. Publ. 37, 1956.

[9] R. Lidl et H. Niederreiter, *Introduction to finite fields and their applications*, édition révisée, Cambridge University Press, 1994.

[10] H. J. Zassenhaus, *A group-theoretic proof of a theorem of MacLaglan-Wedderburn*, Proc. Glasgow Math. Assoc., vol. 1, 1952, pp. 53-63.

[11] I. N. Hernstein, *Wedderburn's theorem and a theorem of Jacobson*, Amer. Math. Monthly, vol. 68, 1961, pp. 249-251.

[12] T. J. Kaczynski, *Another proof of Wedderburn's theorem*, Amer. Math. Monthly, vol. 71, 1964, pp. 652-653.

[13] S. Ebey et K. Sitaram, *Frobenius groups and Wedderburn's theorem*, Amer. Math. Monthly, vol. 76, 1969, pp. 526-528.

[14] J. Carcanague, *Une démonstration du théorème de Wedderburn*, Bull. Sci. Math. 2, vol. 95, 1971, pp. 379-381.

[15] J. Schue, *The Wedderburn theorem of finite division rings*, Amer. Math. Monthly, vol. 95, 1988, pp. 436-437.

[16] I. N. Hernstein, *Noncommutative rings*, Carus Math. Monographs, 1968.

[17] T. Grundhöfer, *Commutativity of finite groups according to Wedderburn and Witt*, Arch. Math., vol. 70, 1998, pp. 425-426.