LE PETIT THÉORÈME DE WEDDERBURN (BROUILLON)

PAVLE MICHKO

Résumé. Le petit théorème de Wedderburn affirme que tous les corps finis sont commutatifs : un bien joli résultat qui mérite un détour.

Il y a peu, au hasard de la toile, je suis tombé sur une note fort intéressante de Gabriel Chênevert [6] présentant trois démonstrations du petit théorème de Wedderburn. Curieux d'en savoir un peu plus sur le sujet, je suis parti de la précieuse bibliographie de [13] pour faire le point, avec l'objectif, pourquoi pas, de terminer un jour ce document par une nouvelle preuve du théorème de Wedderburn. En effet, les corps de Galois sont au centre d'objets combinatoires remarquables, et je rêve parfois d'un monde ou le théorème de Wedderburn serait faux.

Table des matières

Date: Hiver 2014, 28 janvier 2014.

1. Introduction

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

Le théorème, connu sous le nom de petit théorème de Wedderburn, a été publié simultanément par Leonard Dickson et Joseph MacLagan-Wedderburn au tout début du 20e siècle. Il semble que l'énoncé fût proposé par Wedderburn et que, dans un premier temps, Dickson douta de sa véracité jusqu'à l'ouverture d'une voie par l'écossais. Aprés quoi l'américain découvrit rapidement une preuve presque élémentaire [4]. Un article fût publié par Wedderburn avec trois approches. Deux des démonstrations utilisent les arguments de divisibilités de Dickson. Plus tard [1], Emil Artin signale une erreur [1] dans celle de Wedderburn. Au final, le spécialiste des corps finis (Dickson) est bien le co-inventeur de ce joli théorème, il n'en revendiqua cependant jamais la paternité, bien au contraire.

En 1964, Théodore Kaczynski recense huit démonstrations : celle de Dickson, les deux de Wedderburn, une d'Artin, une de Ernst Witt, deux de Bartel Leendert van der Waerden et la sienne basée sur la théorie des groupes, il omet celle de Hans Zassenhaus [19] publiée une douzaine d'années plus tôt. Une autre preuve fondée exclusivement sur la théorie des groupes. Les cours d'algèbre de nos universités donnent la préférence à celle de Witt, nous verrons dans cette note que les arguments de van der Waerden, et ceux de Hernstein-Schue ne manquent pas d'intérêt pédagogique.

Pour le plaisir, cette note est parsemée de quelques digressions en direction de résultats profonds de la théorie des algèbres et corps gauches, le véritable point de vue de Wedderburn, le lecteur trouvera alors dans [3] la plupart des détails.

2. Corps de Galois

Dans la terminologie habituelle, un corps de Galois est une extension algébrique finie d'une corps premier. Un tel corps est par définition commutatif. Si p est sa caractéristique son cardinal q est une puissance de p.

Théorème 2. *Le groupe des inversibles d'un corps de Galois est cyclique.*

Démonstration. C'est un résultat général de Krönecker sur les sous groupes des finis du groupe des inversibles d'un corps commutatif. Il résulte du fait que, dans un corps commutatif, le polynôme $T^n - 1$ admet au plus n racines. □

Les générateurs du groupe des inversibles d'un corps de Galois sont des éléments primitifs trés particuliers : ceux sont les racines primitives du corps.

1. Ein weiterer Beweis von Herrn Wedderburn, der jene Teilbarkeitseigenschaften vermeidet, ist leider nicht stichhaltig. Die grosse Wichtigkeit dieses Satzes für die Arithmetik hyperkomplexer Zahlen hat kürzlich Herr Speiser gezeigt.

Théorème 3. *Soit q une puissance d'un premier p. Dans une clôture algébrique de $\mathbb{F}_p$, il existe un et un seul corps d'ordre q, c'est le corps de décomposition du polynôme $T^q - T$.*

Théorème 4. *Si K est un sous-corps d'ordre q d'un corps de Galois L alors l'extension L/K est cyclique de groupe de Galois engendré par l'automorphisme de Fröbenius $x \to x^q$.*

Terminons cette section, par deux petits lemmes. La preuve du second est volontairement tirée par les cheveux !

Lemma 1. *Soit D un corps fini. Si D est de dimension 2 sur son centre alors D est un corps de Galois.*

Le centre K de D est un corps de Galois. Prenons x un élément dans $D \setminus K$, $K[x]$ est un corps de Galois et pour des raisons de dimension c'est D.

Lemma 2. *Un corps fini de dimension 6 sur $\mathbb{F}_2$ est un corps de Galois.*

Démonstration. D'aprés le lemme de Cauchy, il existe un élément x d'ordre 7 dans D. Considérons le corps de Galois $K := \mathbb{F}_2[x]$. Si $D = K$ alors il n'y a rien à faire. On peut donc supposer que $K^\times$ est d'ordre 7. Un argument de Sylow nous dit que c'est le seul sous-groupe d'ordre 7 de $D^\times$. Pour tout $y \in D^\times$, l'automorphisme intérieur associé s'envoie dans le groupe de Galois de K. Il en résulte un morphisme dans un groupe d'ordre 3 qui ne peut-être surjectif car le noyau d'ordre 21 est aussi le centralisateur de x donc le groupe multipicatif d'un corps fini d'ordre : 3, 7, 15, 31. □

Les deux lemmes qui précèdent constituent l'argument final de Dickson. Bien évidemment, contrairement à ce que l'on peut lire dans une récente note publiée dans un journal de mathématiques américain, une nouvelle preuve d'un de ces lemmes ne constitue pas une nouvelle preuve du théorème de Wedderburn !

3. La preuve de Dickson

Considérons donc un corps non commutatif D, son centre Z est commutatif de cardinal de q. Le centralisateur d'un élément $x \in D$ est :

$$C(x) = \{y \in D \mid xy = yx\},$$

c'est un corps qui contient Z, un Z-espace vectoriel, son cardinal est de la forme $q^{d(x)}$, où $d(x)$ est la dimension de $C(x)$ sur Z. Quand le groupe multiplicatif de D agit par automorphismes intérieurs, $C(x) \setminus \{0\}$ est justement fixateur de x, l'équation aux classes donne :

$$q^n - 1 = q - 1 + \sum_{x \in X} \frac{q^n - 1}{q^{d(x)} - 1}, \quad n := [D : K]$$

où la somme porte sur un ensemble de représentants. Il s'agit alors de prouver l'existence d'un diviseur de $q^n - 1$ qui ne soit pas un diviseur des $q^d - 1$

pour tout diviseur propre d de n. Pour cela, Dickson s'appuie sur un ancien résultat de Zsigmondy [20],

Proposition 1. *Soit n et q deux entiers. Il existe un premier p qui divise $q^n - 1$ sans diviser aucun des $q^k - 1$ avec $k < n$. Sauf si $q = 2$ et $n = 6$, ou bien, $q = 2^r - 1$ et $n = 2$.*

On remarque que la non commuativité implique $n \neq 2$. La proposition (1) permet de couvrir tous les cas sauf celui de $n = 6$ et $q = 2$.

Mezalor, la non-commutativité conduirait à une une congruence impossible modulo 3

$$0 \equiv 63 = 1 + 9X + 21Y \equiv 1$$

Il en résulte une démonstration complète concentrant la difficulté sur la proposition (1), le lecteur trouvera une démonstration de ce point dans [2].

4. Argument cyclotomique

La preuve de Dickson fût synthétisée par Ernst Witt au moyen d'un argument d'intégralité de la théorie des nombres. Nous en donnons ici le fil conducteur, les détails sont dans bien des manuels d'algèbre.

Démonstration. Witt [18] considère le n-ème polynôme cyclotomique défini à partir de la racine n-ième principale de l'unité $\zeta_n = \exp(2i\pi/n)$:

$$\Phi_n(T) = \prod_{(i,n)=1} (T - \zeta_n^i).$$

Les ζ_n sont des entiers algébriques, le polynôme cyclotomique est à coefficients entiers. On obtient la factorisation dans $\mathbb{Z}[T]$:

$$T^n - 1 = \prod_{d|n} \Phi_d(T).$$

L'équation au classe montre alors que $\Phi_n(q)$ divise $q - 1$ ce qui est impossible car le module de $q - \zeta_n$, et de ses conjugués, sont tous supérieurs à $q - 1$. □

Notons que l'argument d'intégralité peut-être éludé par l'utilisation des transformations de Möbius multiplicatives [12].

5. Le point de vue d'Artin

La méthode d'Artin demande un investissement dans les anneaux de polynômes sur des corps non commutatifs.

Soit D un corps. L'ensemble des polynômes à une indéterminée qui s'écrivent :

$$f(t) = \sum_{i=0}^{n} a_i t^i, \quad a_i \in D$$

muni des opérations usuelles forme une algèbre de centre K. La division euclidienne de f par g s'obtient par l'algoritme habituel, en particulier,

$$f(t) = g(t)q(t) + r(t), \quad \deg r < \deg g.$$

en conséquence les idéaux à droites sont tous principaux.

Lemma 3 (Hilfssatz 1)**.** *Soit $h(t)$ une fonction non constante. Soit $g(t) \neq 0$ ayant vérifiant la propriété : pout tout $a \in D$, $h(t)$ est un diviseur à gauche de $ag(t)a^{-1}$. Alors, il existe une fonction non constante $F(t)$ du centre qui divise $g(t)$.*

Démonstration. Les $g(t)$ vérifiants la condition de divisibilité forme un idéal à droite.

$$a^{-1}h(t)Q_a(t)a = g(t) \Longrightarrow h(t)Q_a(t)ax(t)a^{-1} = ag(t)x(t)a^{-1}$$

Soit $F(t)$ le générateur unitaire de cet idéal à droite, par définition :

$$aF(t)a^{-1} = F.$$

Notons que $F(t)$ divisible à gauche par $h(t)$ n'est pas constant. □

Lemma 4 (Hilfssatz 2)**.** *Si $t-\xi$ est un diviseur à gauche du produit $f(t)g(t)$ sans diviser $f(t)$ alors $ag(t)a^{-1}$ est divisible à gauche pour un certain $a \in D$.*

Démonstration. Par la division euclidienne, il existe une constante a tel que

$$f(t) = (t - \xi)q(t) + a$$

par suite $(t - \xi)$ est un diviseur gauche de $ag(t)a^{-1}$. □

6. L'erreur de Wedderburn

7. Algèbre linéaire

L'argument de comptage sur les classes de conjugaison bien que suffisant n'est pas totalement satisfaisant pour qui s'intéresse aux propriétés cachés des corps gauches. Notamment l'énoncé ci-dessous qui, d'une part, se généralise aux corps infini et, d'autre part, conduit à une preuve purement linéaire ou presque du théorème de Wedderburn.

Théorème 5. *Soit K un sous-corps commutatif maximal de D*

$$[D : Z] = [K : Z]^2.$$

où Z est le centre de D.

Démonstration. Soit ω une racine primitive de K, $f \in Z[T]$ le polynôme minimal de ω sur Z. La multiplcation à droite par ω est un K-automorphisme Ω de D. Nous notons Λ le spectre de ω. On remarque $\omega \in \Lambda$ car 1 est un vecteur propre. De plus, si $\lambda \in \Lambda$ alors c'est une racine conjuguée de ω car la relation $x\omega = \lambda x$ conduit à $x\omega^i = \lambda^i x$ et donc

$$0 = xf(\omega) = f(\lambda)x.$$

L'ensemble des vecteurs propres coincide avec le normalisateur de $K^\times$ dans D. La maximalité de K montre que

$$x\omega x^{-1} = y\omega y^{-1} \in K^\times \iff y \in Kx$$

Ce dernier point montre que les valeurs propres Ω sont simples, et que le polynôme minimal $\pi(T)$ de Ω est scindé sur K. Il s'en suit que Ω est diagonalisable, et que

$$[D : Z] = \deg \pi \times [K : Z]$$

Si x et y sont deux vecteurs propores xy en est un autre. En particulier, pour chaque vecteur propre x l'automorphisme intérieur associé à x permute l'ensemble des valeurs propres. On déduit de cela que le polynôme de $K[T]$

$$g(T) = \prod_{\lambda \in \Lambda} (T - \lambda)$$

est à coefficient dans Z. Il s'annule en ω et des considérations de graduation montrent que $\pi = f$. □

Proposition 2. *Soit D un corps de dimension finie sur son centre K. La dimension $[D : K]$ est un carré parfait parfait.*

L'énoncé et la preuve complète sont dans le petit livre de André Blanchard [3] sur les corps non commutatifs.

On réalise une preuve par induction. Si $D = K$ alors il n'y a rien à faire. Dans le cas contraire, on part d'un élément x non central de D. L'extension algébrique $E := K(x)$ est un corps commutatif intermédiaire. L'algèbre $D \otimes_K E$ est simple de centre E, sa dimension sur E est égale à celle de D sur K. Une telle algèbre est isomorphe à une algèbre de matricielle sur un corps E' contenant E, d'où

$$[D : K] = [D \otimes_K E : E] = k^2.[E' : E]$$

Notons bien que $D \otimes_K E$ n'est pas un corps, donc $k > 1$, et ainsi, par induction $[D : K]$ est bien un carré.

8. L'argument de Van der Waerden

Il s'agit de partir du lemme suivant démontré par Van der Waerden dans le cas d'un corps de dimension finie sur son centre. L'adaptation au cas fini est tirée de [13].

Lemma 5. *Les corps commutatifs maximaux d'un corps fini D sont conjugués.*

Démonstration. Le lemme (5) montre que les sous corps maximaux sont de même cardinalité. Soit $Z[\omega]$ et $Z[\omega']$ deux corps commutatifs maximaux. Soit ω' l'image de ω par un K-isomorphisme. Le polynôme minimal de ω annule la multiplication par ω et par isomorphie celle par ω'. Il suit que ω est une valeur propre de Ω'.

$$x\omega' = \omega x \Longrightarrow K' = x^{-1}Kx$$

□

Lemma 6. *Un groupe fini n'est jamais une union de conjugés d'un sous-groupe propre.*

Démonstration. En effet, soit H un sous-groupe propre d'un groupe G. Le nombre de conjugués est inférieur au nombre de classes latérales. Les relations

$$G = \cup_x xHx^{-1}, \quad \sharp G = \sharp H \times [G : H]$$

montrent que les conjugués devraient être disjoints. □

9. La preuve de Schue

Dans cette approche récente de John Schue [10], on mélange les idées des approches précédentes. Il s'agit d'utiliser l'équation aux classes en cernant avec précisions les dimensions des centralisateurs.

Sans perdre en généralité, on peut supposer que tous les sous-corps propres de D sont des corps de Galois.

On note p la caractéristique de D. Dans sa note [10], utilise un lemme de Hernstein [**?**] concernant les commutateurs de $[x, y] = xy - yx$ de D.

Lemma 7. *Soit a un élément de D. L'endomorphisme $D_a \colon x \mapsto [a, x]$ satisfait à $D_a^p = D_{a^p}$.*

Démonstration. □

Soit t un élément non central de D. Les éléments qui commutent avec t forment un corps commutatif K dont le groupe multiplicatif est cyclique engendré par une racine primitive ω.

Notons N le normalisateur de $K^\times$ dans $D^\times$. Nous noterons q l'ordre du quotient $N/K^\times$, c'est aussi le nombre de classes $[N : K^\times]$. Dans ce cas,

$$x \in N \iff x\omega x^{-1} \in K.$$

De plus,

$$x\omega x^{-1} = y\omega y^{-1} \iff y \in Kx$$

Le lemme montre que le polynôme minimal de opérateur D_ω est un diviseur de $T^{[K:\mathbb{F}_p]} - T$, il est scindé sur K, et D_ω est diagonalisable. Pour $\lambda \in K$, on note E_λ l'espace propre correspondant à λ,

$$x \in E_\lambda, \quad \omega x - x\omega = \lambda x, \quad \lambda - \omega = x^{-1}\omega x \in K.$$

Autrement dit, les valeurs propres non nulles sont des élémemnts du normalisateur de $K^\times$ dans $D^\times$.

$$[D : K] = [N : K^\times]$$

L'extension K/Z est Galoisienne. Le groupe $G := N/K^\times$ s'identifie à un sous-groupe des automorphismes de K. Un élément z du corps fixe de G

vérifie $xzx^{-1} = z$, en particulier D_z est nul sur N, et donc sur les E_λ ce qui montre que $z \in F$ i.e.

$$[K : F] = [N : K^\times] = q.$$

Au final, la dimension de D sur son centre est un carré q^2 et la dimension d'un centralisateur non trivial est q. L'équation au classe apporte la divisibilité de $q - 1$ par $q + 1$.

Au cours de la preuve deux faits importants sont apparus : conjugaison des corps commutatif maximaux et dimension quadratique de K sur son centre.

10. L'argument de Zassenhaus

L'article de Zassenhauss [19] fourni une démonstration autocomplète du théorème qui nous intéressent : théorie de Galois des corps finis commutatifs et argument de commutativité sur la théorie des groupes.

Théorème 6. *Soit G un groupe fini. Si dans G, pour tous sous-groupe abélien A, les notions normalisateurs et centralisateurs coïncident, alors G est abélien.*

Démonstration. Non triviale ! □

Lemma 8. *Si G est un sous-groupe abélien de $D^\times$, le normalisateur de G coincide avec le centralisateur de G.*

Démonstration. La preuve de Zassenhaus est plutôt longue (3 pages). □

11. Algèbre de quaternion

Pour tout corps commutatif K de caractéristique impaire, on peut définir une algèbre de dimension 4 contenant une base 1, i, j et k satisfaisant :

$$i^2 = j^2 = k^2 = ijk = -1. \tag{1}$$

L'algèbre des quaternions [2] ainsi formée sur K est simple. La relation

$$\forall a, b, c, d \in K \quad (a + bi + cj + dk)(a - bi - cj - dk) = a^2 + b^2 + c^2 + d^2$$

montre que c'est un corps si et seulement si la somme de 4 carrés non nuls est non nulle.

Lemma 9. *Si K est un corps de Galois alors $\mathbb{H}(K)$ est n'est pas un corps.*

Démonstration. Dans un corps de Galois, le théorème de Chevalley-Warning (par exemple) montre la forme quadratique $X^2 + Y^2 + Z^2 + T^2$ représente 0. □

2. On peut lire sur le pont de Broom à Dublin : "Ici, le 16 octobre 1843, alors qu'il se promenait, Sir William Rowan Hamilton découvrit dans un éclair de génie la formule fondamentale sur la multiplication des quaternions i2 = j2 = k2 = ijk = –1 et la grava sur une pierre du pont."

Lemma 10 (Chevalley-Warning)**.** *Dans un corps de Galois K de caractéristique p. Le nombre de solutions d'un système d'équations polynomiales $P_j(x_1, \ldots, x_n)$ est multiple de p dès que :*

$$n > \sum_j \deg(P_j).$$

Théorème 7 (Froebenius)**.** *Il n'y en a que trois corps de centre $\mathbb{R}$: le corps des réels, celui des complexes et le corps non commutatif $\mathbb{H}(\mathbb{R})$ des quaternions.*

Démonstration. □

12. La preuve de Kaczynski

Il s'agit d'une preuve utilisant exclusivement des argument de la théorie des groupes. Assez difficile à suivre dans les détails, elle a l'avantage de nous renseigner sur des outils assez rarement utilisés dans la théorie des corps finis.

Théorème 8. *Un p-groupe qui contient un et un seul sous-groupe d'ordre p est soit groupe cyclique, soit un groupe de quaternions généralisés.*

Démonstration. Une page de démonstration dans [7], page 189. □

Un résultat classique de représentation par des formes quadratiques sur les corps finis

$$\exists x, y \in \mathbb{F}_p, \quad x^2 + y^2 = 1 \tag{2}$$

permet une première observation

Lemma 11. *Le groupe multiplicatif d'un corps fini ne contient pas le groupe des quaternions.*

Démonstration. Soit K un corps fini contenant le groupe Q des quaternions engendré par deux éléments a et b d'ordre 4 vérifiant la relation $aba = b$.

$$a^2 = -1, \quad b^2 = -1, \quad ab = -ba.$$

Notons p la caractéristique de K, (u, v) une solution de (2). Ici Kaczynski prend un chemin étrange, en divergeant un peu :

$$(1 + ua + vb)(1 - ua - vb) = (1 - (ua + bv)^2) = 1 - u^2 - v^2 = 0$$

Il suit que l'un des facteurs de gauche est nul, au final b commute avec a. □

Lemma 12. *Le groupe multiplicatif d'un corps fini D est métacyclique : tous ses sous-groupe de Sylow sont cycliques.*

Démonstration. En effet, soit S un ℓ-sous-groupe de Sylow de $D^\times$, son centre contient un élément g d'ordre ℓ. C'est le seul sous-groupe d'ordre ℓ dans S. En effet, si h est d'ordre ℓ hors de G alors g et h engendre un corps de Galois contenant trop d'éléments d'ordre ℓ !

Il découle de (8) que S est soit cyclique soit un groupe de quaternion généralisés. La seconde possibilité ayant été écartée, tous les sous-groupes de Sylow sont cycliques. □

Il ne reste plus qu'à tirer les marrons du feu mais c'est chaud.

Démonstration. Le groupe $D^\times$ est résoluble. Notons Z le centre que nous supposons propre. Le quotient D/Z est résoluble et ses sous-groupes de Sylow sont résolubles. Notons A un sous-groupe normal minimal, le quotient A/Z est cyclique et donc A est abélien.

Kaczynski utilise un fil calculatoire pour montrer que A et Z commutent.

Soient x dans $D^\times$ et $y \in A$, on a $xyx^{-1} \in A$ et, de même, il existe un élément $z \in A$ tel que $(1+x)y = z(1+x)$.

Un calcul direct donne

$$y - z = zx - xy = (z - xyx^{-1})x$$

$$\begin{aligned} y(y-z) = y(z-xyx^{-1})x &= (z-xyx^{-1})yx \\ (y-z)y = y(y-z) &= (z-xyx^{-1})xy \end{aligned}$$

Si $(z - xyx^{-1}) = 0$ alors x et y commutent, et sinon... c'est idem ! □

ouf !

13. Automorphisme

14. Simplicité

Une algèbre qui ne contient que des idéaux bilatères triviaux est dite simple. Isotypiquement, l'algèbre $\mathrm{mat}_n(K)$ des matrices carrées $n \times n$ à coefficient dans un corps k est simple.

Théorème 9. *Toute K-algèbre simple est isomorphe à une algèbre matricielle sur un corps L contenant K.*

La preuve n'est pas immédiate, c'est une conséquence de l'étude des structures des modules simples et semi-simple.

Etant donné un corps commutatif K, chaque corps D de dimension finie sur K définit une classe d'algèbre simple, celle des matrices carrées à coefficients dans D.

Le produit tensoriel de K-algèbre est compatible avec cette notion de classe. L'ensemble des classes de K-algèbre muni du produit tensoriel forme un monoide associatif, commutatif, unifère. En fait, toute classe est inversible car la classe d'un corps gauche D n'est autre que le corps inverse de D.

Définition 1. *Le groupe des classes d'un corps commutatif K, noté* $\mathrm{Br}(K)$*, s'appelle le groupe de Brauer de K.*

Par exemple, le groupe de Brauer d'un corps algébriquement clos est trivial. Le groupe de Brauer du corps des réels contient 2 classes celle des réels et celle des quaternions. Le théorème de Wedderburn se résume par l'implication :

$$K \text{ fini} \implies \mathrm{Br}(K) = 1$$

15. Méthode Cohomologique

16. Approche naïve

Références

[1] Emil Artin. Über einen Satz von Herrn J. H. Maclagan Wedderburn. *Abh. Math. Sem. Univ. Hamburg*, 5(1) :245–250, 1927.

[2] Geo. D. Birkhoff and H. S. Vandiver. On the integral divisors of $a^n - b^n$. *Ann. of Math. (2)*, 5(4) :173–180, 1904.

[3] André Blanchard. *Les corps non commutatifs*. Collection SUP. Presses Universitaires de France, Paris, 1972.

[4] Leonard Eugene Dickson. On finite algebras. *Nachrichten von der Gesellschaft der Wissenschaften zu Göttingen, Mathematisch-Physikalische Klasse*, 1905 :358–393, 1905.

[5] S. W. Dolan. A proof of Jacobson's theorem. *Canad. Math. Bull.*, 19(1) :59–61, 1976.

[6] Chênevert Gabriel. Le théorème de wedderburn, 2001.

[7] Marshall Jr Hall. *The Theory of Groups*. 2nd edition. Macmillan, New York, 1976.

[8] I. N. Herstein. Wedderburn's theorem and a theory of Jacobson. *Amer. Math. Monthly*, 68 :249–251, 1961.

[9] Jürgen G. Hinz. Einige Bemerkungen zum Beweis eines Satzes von J. H.Maclagan-Wedderburn. *J. Reine Angew. Math.*, 290 :109–112, 1977.

[10] Schue John. The Wedderburn theorem of finite division rings. *Amer. Math. Monthly*, 95(5) :436–437, 1988.

[11] T. J. Kaczynski. Mathematical Notes : Another Proof of Wedderburn's Theorem. *Amer. Math. Monthly*, 71(6) :652–653, 1964.

[12] W. Klobe. Über eine untere Abschätzung der n-ten Kreisteilungspolynome $g_n(z) = \prod_{d|n}(z^d - 1)^{\mu(n/d)}$. *J. Reine Angew. Math.*, 187 :68–69, 1949.

[13] Rudolf Lidl and Harald Niederreiter. *Finite fields*. Encyclopaedia of mathematics and its applications. Cambridge University Press, New York, 1997.

[14] Jiang Luh. On the commutativity of J-rings. *Canad. J. Math.*, 19 :1289–1292, 1967.

[15] J. H. Maclagan-Wedderburn. A theorem on finite algebras. *Trans. Amer. Math. Soc.*, 6(3) :349–352, 1905.

[16] Takasi Nagahara and Hisao Tominaga. Elementary proofs of a theorem of Wedderburn and a theorem of Jacobson. *Abh. Math. Sem. Univ. Hamburg*, 41 :72–74, 1974.

[17] D. E. Taylor. Some classical theorems on division rings. *Enseignement Math. (2)*, 20 :293–298, 1974.

[18] Ernst Witt. Über die kommutativität endlicher schiefkörper. *Abh. Math. Sem. Univ. Hamburg*, 8(1) :413, 1931.

[19] Hans J. Zassenhaus. A group-theoretic proof of a theorem of Maclagan-Wedderburn. *Proc. Glasgow Math. Assoc.*, 1 :53–63, 1952.

[20] K. Zsigmondy. Zur Theorie der Potenzreste. *Monatsh. Math. Phys.*, 3(1) :265–284, 1892.