

Zeitschrift: L'Enseignement Mathématique
Herausgeber: Commission Internationale de l'Enseignement Mathématique
Band: 19 (1973)
Heft: 1-2: L'ENSEIGNEMENT MATHÉMATIQUE

Artikel: ÉQUATIONS ET VARIÉTÉS ALGÈBRIQUES SUR UN CORPS FINI
Autor: Joly, Jean-René
Kapitel: §1. Le théorème de Chevalley- Warning.
DOI: <https://doi.org/10.5169/seals-46287>

Nutzungsbedingungen

Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. [Siehe Rechtliche Hinweise.](#)

Conditions d'utilisation

L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. [Voir Informations légales.](#)

Terms of use

The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. [See Legal notice.](#)

Download PDF: 20.02.2025

ETH-Bibliothek Zürich, E-Periodica, <https://www.e-periodica.ch>

CHAPITRE 3

THÉORÈMES DE CHEVALLEY ET WARNING

Ce chapitre est centré sur la propriété suivante: si un polynôme sans terme constant sur un corps fini k a un nombre de variables strictement supérieur à son degré, alors il admet sur k un zéro *non trivial* (c'est-à-dire autre que le point $(0, \dots, 0)$); ce résultat, conjecturé par Artin vers 1934, a été démontré par Chevalley en 1935, puis précisé par Warning la même année (pour plus amples détails, voir les Notes en fin de chapitre).

On conserve ici les conventions adoptées au début du chapitre 2.

§ 1. *Le théorème de Chevalley-Warning.*

1.1. Il s'agit du résultat suivant:

THÉORÈME 1. — *Soit F_1, \dots, F_s une famille de s polynômes appartenant à $k[X]$, de degrés respectifs d_1, \dots, d_s , et soit V l'ensemble des solutions dans k^n du système d'équations*

$$(1.1.1) \quad F_1 = 0, \dots, F_s = 0;$$

soient enfin $N = \text{card}(V)$ le nombre de solutions de (1.1.1) dans k^n , et $d = d_1 + \dots + d_s$ la somme des degrés des polynômes F_j . Alors, si $n > d$, le nombre N est divisible par p (la caractéristique de k).

Démonstration. — Introduisons les deux polynômes suivants:

$$(1.1.2) \quad \bar{F} = (1 - F_1^{q-1}) \dots (1 - F_s^{q-1});$$

$$(1.1.3) \quad F_V = \sum_{\mathbf{a} \in V} (1 - (X_1 - a_1)^{q-1}) \dots (1 - (X_n - a_n)^{q-1});$$

(avec les notations du chap. 2, sect. 2.1, on a donc $F_V = \sum_{\mathbf{a} \in V} F_{\mathbf{a}}$). On voit immédiatement que \bar{F} et F_V prennent la valeur 1 en tout point de V , et la valeur 0 partout ailleurs; le polynôme $G = \bar{F} - F_V$ est donc identiquement nul; comme F_V est manifestement réduit, et que $\bar{F} = F_V + G$, F_V n'est autre que le polynôme réduit associé à \bar{F} (chap. 2, sect. 1.4), ce qui implique (chap. 2, th. 2) $\deg(F_V) \leq \deg(\bar{F})$, donc, en utilisant l'hypothèse $n > d$, $\deg(F_V) \leq d(q-1) < n(q-1)$. Mais F_V comporte a priori un monôme

en $X_1^{q-1} \dots X_n^{q-1}$, de degré $n(q-1)$; le coefficient de ce monôme, égal à $(-1)^n N$, doit donc être nul dans le corps k , de caractéristique p : en d'autres termes, N doit être divisible par p , C.Q.F.D.

On verra (§ 4) que l'hypothèse $n > d$ ne peut pas être affaiblie: on peut en effet, quels que soient k et n , construire un polynôme de degré n , à n variables et à coefficients dans k , et pour lequel on ait $N = 1$.

COROLLAIRE 1 (théorème de Chevalley). — *Mêmes données et hypothèses (notamment $n > d$) que dans le théorème 1. Si de plus chacun des polynômes F_j ($j=1, \dots, s$) est sans terme constant, alors le système (1.1.1) admet dans k^n une solution autre que la solution triviale $(0, \dots, 0)$.*

Démonstration. — L'absence de termes constants implique que $(0, \dots, 0)$ est solution du système (1.1.1): d'où $N \geq 1$; mais N est divisible par p (th. 1); on a donc $N \geq p$, et le nombre $N - 1$ de solutions non triviales est donc $\geq p - 1 \geq 2 - 1 = 1$, C.Q.F.D.

Le théorème 1 et son corollaire 1 s'appliquent en particulier au cas $s = 1$ d'un seul polynôme de degré d , à n variables et tel que $n > d$. Ainsi, toute forme quadratique à trois variables ou plus sur un corps fini k admet un zéro non trivial sur k ; en langage géométrique, toute conique, quadrique, ... projective, définie sur un corps fini k , admet au moins un point rationnel sur k . On aura l'occasion de revenir fréquemment sur ce genre de propriété. Notons par ailleurs qu'un polynôme satisfaisant à $n > d$ peut être tel que $N = 0$; ainsi, si $p \neq 2$, le polynôme $(X_1 + \dots + X_n)^{q-1} + 1$, de degré $q - 1$, ne peut prendre que les valeurs 1 et $2 \neq 0$ (chap. 1, sect. 1.1): donc, si grand que soit n , et en particulier si $n > d = q - 1$, ce polynôme donne lieu à $N = 0$. Pour un autre exemple, voir le chapitre 4 (sect. 2.3).

1.2. Le théorème de Chevalley fournit une démonstration du théorème de Wedderburn autre que celles mentionnées au chapitre 1. Soient en effet K un corps commutatif et r un nombre réel positif; on dit que K possède la propriété (C_r) si tout polynôme homogène, de degré d , à n variables, à coefficients dans K , et tel que $n > d^r$, admet dans K^n un zéro non trivial (voir par exemple [7], p. 6); avec cette terminologie, le théorème 1 (ou son corollaire 1) implique:

COROLLAIRE 2. — *Tout corps fini (commutatif) possède la propriété (C_1) .*

Convenons d'autre part, toujours pour un corps commutatif K , de désigner par (B_0) la propriété suivante: tout corps gauche de centre K et de degré fini sur K est égal à K . On a alors le résultat suivant:

PROPOSITION 1. — *Si un corps commutatif K possède la propriété (C_1) , alors il possède la propriété (B_0) .*

Démonstration. — Soit en effet L un corps gauche de centre K et de degré fini n sur K . On sait que n est un carré (soit $n = d^2$) et que si e_1, \dots, e_n est une base de L sur K (en tant qu'espace vectoriel), la norme réduite $Nrd_{L/K}(x)$ d'un élément quelconque $x = x_1e_1 + \dots + x_n e_n$ de L est un polynôme homogène et de degré d , à coefficients dans K , par rapport aux composantes x_1, \dots, x_n de x , qui sont dans K (voir par exemple Bourbaki, Algèbre, chap. VIII, § 12; dans le cas bien connu du corps \mathbf{H} des quaternions ordinaires sur \mathbf{R} , rapporté à la base canonique $1, i, j, k$, on a $n = 4 = 2^2$ et $Nrd_{\mathbf{H}/\mathbf{R}}(x) = x_1^2 + x_2^2 + x_3^2 + x_4^2$); cette norme réduite ne s'annule que pour $x = 0$, donc pour $x_1 = \dots = x_n = 0$; comme K est supposé posséder la propriété (C_1) , on a nécessairement $n = d^2 \leq d$, donc $d = 1$, $n = 1$ et $L = K$, C.Q.F.D.

Redémontrons alors le théorème de Wedderburn; soit L un corps fini, non supposé commutatif, et soit k son centre; k est un corps fini commutatif, et il possède la propriété (C_1) (cor. 2), donc la propriété (B_0) (prop. 1); mais comme L est évidemment de degré fini sur k , on a alors $L = k$ (par définition de (B_0)), et par conséquent L est commutatif, C.Q.F.D.

§ 2. *Seconde démonstration du théorème de Chevalley-Waring.*

2.1. Cette seconde démonstration, indépendante de la théorie des polynômes réduits, repose sur le théorème suivant (dont on aura également besoin au § 3):

THÉORÈME 2. — *Soit $F \in k[X]$ un polynôme à n variables, et de degré d . Alors, si $d < n(q-1)$, on a*

$$(2.1.1) \quad \sum_{\mathbf{x} \in k^n} F(\mathbf{x}) = 0.$$

Démonstration. — Par linéarité, on peut se ramener au cas où F est un monôme $X_1^{u_1} \dots X_n^{u_n}$, avec $d = u_1 + \dots + u_n < n(q-1)$; on a alors

$$(2.1.2) \quad \sum_{\mathbf{x} \in k^n} F(\mathbf{x}) = \prod_{i=1}^n \left(\sum_{x_i \in k} x_i^{u_i} \right);$$

l'inégalité relative à d montre que pour un i au moins, $u_i < q-1$, et il suffit évidemment de prouver que, dans (2.1.2), le i -ème facteur du membre de droite est alors nul, ce qui résulte du lemme suivant: