§1. Classification des corps finis.

Objekttyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **19 (1973)**

Heft 1-2: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **22.09.2024**

Nutzungsbedingungen

Die ETH-Bibliothek ist Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Inhalten der Zeitschriften. Die Rechte liegen in der Regel bei den Herausgebern.
Die auf der Plattform e-periodica veröffentlichten Dokumente stehen für nicht-kommerzielle Zwecke in Lehre und Forschung sowie für die private Nutzung frei zur Verfügung. Einzelne Dateien oder Ausdrucke aus diesem Angebot können zusammen mit diesen Nutzungsbedingungen und den korrekten Herkunftsbezeichnungen weitergegeben werden.
Das Veröffentlichen von Bildern in Print- und Online-Publikationen ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Die systematische Speicherung von Teilen des elektronischen Angebots auf anderen Servern bedarf ebenfalls des schriftlichen Einverständnisses der Rechteinhaber.

Haftungsausschluss

Alle Angaben erfolgen ohne Gewähr für Vollständigkeit oder Richtigkeit. Es wird keine Haftung übernommen für Schäden durch die Verwendung von Informationen aus diesem Online-Angebot oder durch das Fehlen von Informationen. Dies gilt auch für Inhalte Dritter, die über dieses Angebot zugänglich sind.

Ein Dienst der *ETH-Bibliothek*
ETH Zürich, Rämistrasse 101, 8092 Zürich, Schweiz, www.library.ethz.ch

http://www.e-periodica.ch

CHAPITRE PREMIER

CORPS FINIS (RAPPELS)

Ce chapitre résume les propriétés générales des corps finis. Rappelons que d'après le *théorème de Wedderburn*, tout corps fini est commutatif (pour une démonstration, voir par exemple [**1**], pp. 35-37, ou [**19**], p. 1).

§ 1. *Classification des corps finis.*

1.1. Soit k un corps fini. Sa caractéristique est certainement différente de 0; c'est un nombre premier p, et le sous-corps premier de k s'identifie à $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$. Notons f le degré de l'extension $k/\mathbf{F}_p$; k est isomorphe, en tant qu'espace vectoriel sur $\mathbf{F}_p$, au produit direct de f exemplaires de $\mathbf{F}_p$; en particulier:

PROPOSITION 1. — *Si q désigne le nombre d'éléments de k, on a $q = p^f$.*

Considérons alors k^*, groupe multiplicatif de k; il est d'ordre $q - 1$; on a donc, pour tout élément a de k^*, $a^{q-1} = 1$, et a fortiori $a^q = a$; comme cette égalité reste vraie pour $a = 0$, elle est vérifiée par tout élément de k; en conséquence:

PROPOSITION 2. — *Si Ω désigne une clôture algébrique de k (donc aussi de $\mathbf{F}_p$), k est égal à l'ensemble des racines dans Ω du polynôme $X^q - X$. En particulier, k est le corps de décomposition dans Ω du polynôme $X^q - X$, et tout corps fini ayant même nombre d'éléments q (donc même caractéristique p) que k est nécessairement isomorphe à k.*

Pour $k = \mathbf{F}_p$, l'identité $a^q = a$ s'écrit $a^p = a$, et constitue le *petit théorème de Fermat* sur les restes modulo p. Pour k quelconque, la proposition 2 permet d'écrire

$$X^{q-1} - 1 = \prod_{a \in k^*} (X - a); \quad X^q - X = \prod_{a \in k} (X - a);$$

la première de ces deux égalités montre que les fonctions symétriques élémentaires des éléments de k^* *autres que le produit* sont toutes nulles, et que le produit de tous les éléments de k^* est égal à -1; pour $k = \mathbf{F}_p$, cette dernière propriété constitue le *théorème de Wilson* sur les restes modulo p.

1.2. Soient maintenant p un nombre premier, f un entier $\geqslant 1$, et posons $q = p^f$. Désignons par Ω une clôture algébrique de $\mathbf{F}_p$, et notons k l'ensemble des racines dans Ω du polynôme $X^q - X$. Ce polynôme ayant toutes ses racines simples (son dérivé vaut -1), on voit que card $(k) = q$; de plus, q étant une puissance de la caractéristique, on a, quels que soient a et b dans k, $(a+b)^q = a^q + b^q = a + b$; on a évidemment aussi $(ab)^q = a^q b^q = ab$, et k est un sous-corps de Ω; en particulier:

PROPOSITION 3. — *Quels que soient p premier et $f \geqslant 1$, il existe un corps fini possédant exactement $q = p^f$ éléments.*

Ce corps est unique à isomorphisme près (prop. 2); on le note généralement $\mathbf{F}_q$.

1.3. Mêmes données que dans la section précédente. Soient f_1 et f_2 deux entiers $\geqslant 1$, et posons, pour $i = 1, 2$,

$$q_i = q^{f_i}; \qquad k_i = \mathbf{F}_{q_i} \subset \Omega;$$

on a alors évidemment $[k_i : \mathbf{F}_q] = f_i$. Si $k_1 \subset k_2$, la multiplicativité du degré montre que f_1 divise f_2. Inversement, supposons que f_1 divise f_2; on peut écrire $f_2 = mf_1$, donc $q_2 = {q_1}^m$; si $a \in k_1$, on a alors $a^{q_1} = a$ (prop. 2), donc $a^{{q_1}^m} = a^{q_2} = a$, et par conséquent $a \in k_2$ (prop. 2); ainsi, $k_1 \subset k_2$. Au total (et en conservant ces notations):

PROPOSITION 4. — *L'inclusion $k_1 \subset k_2$ équivaut à la relation f_1 divise f_2, donc à la relation q_2 est une puissance de q_1.*

COROLLAIRE 1. — *Soient respectivement f' et f'' le p.g.c.d. et le p.p.c.m. de f_1 et f_2. Posons $q' = q^{f'}$, $q'' = q^{f''}$, $k' = \mathbf{F}_{q'}$, $k'' = \mathbf{F}_{q''}$. Alors l'intersection et le composé de k_1 et k_2 sont respectivement k' et k''.*

§ 2. *Groupe additif et groupe multiplicatif d'un corps fini.*

Soit k un corps fini à $q = p^f$ éléments.

2.1. L'extension $k/\mathbf{F}_p$ étant de degré f, k est isomorphe, en tant qu'espace vectoriel sur $\mathbf{F}_p$, et a fortiori en tant que groupe additif, au produit direct de f exemplaires de $\mathbf{F}_p$; en conséquence:

PROPOSITION 5. — *Le groupe additif k^+ de k est un groupe de type $(p, ..., p)$ (f fois).*