**Zeitschrift:** L'Enseignement Mathématique
**Herausgeber:** Commission Internationale de l'Enseignement Mathématique
**Band:** 20 (1974)
**Heft:** 3-4: L'ENSEIGNEMENT MATHÉMATIQUE

**Artikel:** SOMMES DE CARRÉS D'ENTIERS D'UN CORPS
**Autor:** Moser, Claude
**Kapitel:** 2. Etude du cas p impair
**DOI:** https://doi.org/10.5169/seals-46913

## 2. Etude du cas $p$ impair

Cette étude se résume à l'énoncé et à la démonstration du théorème suivant:

### 2.1. *Théorème*

*Si $p$ est impair, tout entier de $K$ est somme de carrés d'entiers ($A = A_2$); plus précisément :*

1. *Pour qu'un entier de $K$ soit un carré, il faut que sa valuation normalisée soit un nombre pair. Un entier $x = u\pi^{2n}$ de valuation $2n$ est un carré dans $A$ si et seulement si la classe de $u$ dans $\bar{K}$ est un carré.*

2. *Si $p$ est congru à* 1 modulo 4, $-1$ *est un carré et tout entier est somme de deux carrés d'entiers,* ($s(A) = 1$, $t(A) = 2$).

3. *Si $p$ est congru à* $-1$ modulo 4, *on a $s(A) = 1$ et $t(A) = 2$ (resp. $s(A) = 2$ et $t(A) = 3$) si $f$ est pair (resp. impair). Si $f$ est impair, les entiers de valuation paire sont somme de deux carrés d'entiers tandis que les entiers de valuation impaire sont somme de trois carrés d'entiers et pas moins.*

En vue de la démonstration de ce théorème, rappelons quelques propriétés des corps finis:

### 2.2. *Lemme*

*Soit $p$ un nombre premier impair et soit $\mathbf{F}_p$ le corps à $p$ éléments.*

1. *Si $p$ est congru à* 1 modulo 4, *alors* $-1$ *est un carré dans $\mathbf{F}_p$ ; si $p$ est congru à* $-1$ modulo 4, $-1$ *n'est pas un carré dans $\mathbf{F}_p$, mais est somme de deux carrés dans $\mathbf{F}_p$.*

2. *Soit $k$ une extension finie de $\mathbf{F}_p$. Si $p$ est congru à* $-1$ modulo 4 *alors* $-1$ *est un carré dans $k$ si et seulement si $k/\mathbf{F}_p$ est de degré pair.*

Le groupe multiplicatif $\dot{\mathbf{F}}_p$ du corps $\mathbf{F}_p$ est cyclique d'ordre $p-1$. Il admet un seul sous-groupe d'ordre $\dfrac{p-1}{2}$. Or l'endomorphisme ($x \mapsto x^2$, $\dot{\mathbf{F}}_p \to \dot{\mathbf{F}}_p$) a pour noyau $\{-1, +1\}$. Il en résulte que le groupe des carrés de $\dot{\mathbf{F}}_p$ est l'unique sous-groupe d'ordre $\dfrac{p-1}{2}$ de $\dot{\mathbf{F}}_p$. Un élément est un carré si et seulement si son ordre divise $\dfrac{p-1}{2}$. Puisque l'ordre de $-1$ est 2, $-1$ est

un carré si et seulement si $\frac{p-1}{2}$ est pair. Il suffit de montrer que si $a \in \mathbf{F}_p$ n'est pas un carré il est somme de deux carrés. Pour cela considérons $A = \{ x \mid \exists y, x = y^2 \}$ et $B(a) = \{ x \mid \exists y, x = a - y^2 \}$. Ces deux sous-ensembles de $\mathbf{F}_p$ ont pour cardinal $\frac{p+1}{2}$. Puisque Card $\mathbf{F}_p = p$ on a $A \cap B(a) \neq \varnothing$, ce qui prouve que $a$ est somme de deux carrés dans $\mathbf{F}_p$.

La deuxième assertion résulte de ce que pour tout $n \geqslant 1$, $\mathbf{F}_p$ admet une extension de degré $n$ unique (à isomorphisme près) (cf. par exemple [2] ou [8]). Ceci étant, si $p$ est congru à $-1$ modulo 4 l'unique extension de degré 2 de $\mathbf{F}_p$ est $\mathbf{F}_p(\sqrt{-1})$.

Démontrons maintenant le théorème 2.1:

1. La première assertion est évidente. Soit $u$ une unité de $A$. Si la classe de $u$ modulo $\mathfrak{P}$ n'est pas un carré, a fortiori $u$ n'est pas un carré dans $A$. Si au contraire la classe de $u$ est un carré dans $\overline{K}$, il existe une unité $b$ de $A$ telle que l'on ait $u - b^2 \in \mathfrak{P}$. On peut alors appliquer au polynôme $X^2 - u$ le lemme de Hensel (1.1.1) et conclure que $u$ est un carré dans $A$.

2 et 3. Remarquons que 2 est une unité de $A$ et que pour tout élément $a$ de $A$ on a l'égalité:

$$(*) \quad a = \left(\frac{a+1}{2}\right)^2 - \left(\frac{a-1}{2}\right)^2 .$$

Si $p$ est congru à 1 modulo 4 ou si le degré résiduel $f = [\overline{K} : \mathbf{F}_p]$ de $K$ est pair, alors $-1$ est un carré dans $\overline{K}$ (cf. lemme 2.2) et la première partie du théorème permet d'affirmer que $-1$ est un carré dans $A$. On conclut facilement en utilisant (*) que tout élément de $A$ est somme de deux carrés dans $A$.

Enfin, si $p$ est congru à $-1$ modulo 4 et si le degré résiduel de $K$ est impair, $-1$ est somme de deux carrés dans $\overline{K}$. Il existe donc deux unités $u$ et $z$ de $A$ telles que $-1 - u^2 - z^2 \in \mathfrak{P}$. On applique alors le lemme de Hensel au polynôme $X^2 + 1 + u^2$ pour conclure qu'il existe une unité de de $A$ telle que $1 + u^2 + w^2 = 0$. Alors toute unité de $A$ est somme de deux carrés d'éléments de $A$ puisque toute unité est soit un carré soit l'opposé d'un carré. Pour terminer remarquons que les éléments de $K$ qui sont somme de deux carrés dans $K$ sont les normes des éléments de $K(\sqrt{-1})$. L'égalité $[\dot{K} : N(K(\sqrt{-1}))\cdot] = 2$ implique qu'aucun élément de valuation impaire n'est somme de deux carrés dans $K$. Enfin tout élément de valuation impaire de $A$ est somme de trois carrés dans $A$ en vertu de l'égalité (*).