File:BabyKummerTheory.tex compil. le 8 juillet 2016,22:07

Objectif : énoncer et prouver un trés cas particulier de la théorie de Kummer

Soit $\mathbf{K}$ un corps commutatif et $a_1, \ldots, a_r$ des éléments de $\mathbf{K}^*$; convenons de dire que $a_1, \ldots, a_r$ sont *quadratiquement indépendants* si pour $e_1, \ldots, e_r \in \mathbb{Z}$ on a l'implication :

$$a_1^{e_1} \cdots a_r^{e_r} \text{ est un carré dans } \mathbf{K}^* \quad \Longrightarrow \quad \text{chaque } e_1, \ldots, e_r \text{ est pair}$$

C'est une notion purement multiplicative. Il faut la voir dans le 2-groupe K^*/K^{*2} (quotient du groupe multiplicatif K^* par son sous-groupe des carrés) : en pensant dans sa tête ce 2-groupe de manière additive donc comme un $\mathbb{F}_2$-espace vectoriel, elle dit que les classes $\overline{a_1}, \cdots, \overline{a_r}$ y sont $\mathbb{F}_2$-linéairement indépendantes. Il est clair qu'elle ne dépend que de la classe de a_i modulo les carrés. On peut d'ailleurs dans la définition ci-dessus supposer que e_i est dans $\mathbb{N}$ (quitte à remplacer e_i par $e_i + 2h$ avec h assez grand).
Il est clair qu'une sous-famille d'une famille

Exemple 1. Soient $a_1, \ldots, a_r$ des entiers ≥ 2, sans facteur carré, premiers entre deux à deux. Alors la famille $(a_1, \ldots, a_r)$ est quadratiquement indépendante dans $\mathbb{Q}$.

Exemple 2. Dans le corps des fractions rationnelles $\mathbb{Q}(x)$, les 3 homographies suivantes :

$$x_1 = x, \qquad x_2 = \frac{x+1}{-x+1}, \qquad x_3 = \frac{-1}{x}$$

sont quadratiquement indépendantes. En effet, on peut remplacer cette famille par la famille de polynômes $\big(x, (x+1)(1-x), -x\big)$. Supposons que le produit

$$x^p \left((x+1)(1-x)\right)^q (-x)^r \quad \text{soit un carré dans } \mathbb{Q}[x]$$

La considération des irréductibles $x+1$ et $1-x$ entraîne que q est pair. On a donc que $x^p \times (-x)^r$ est un carré dans $\mathbb{Q}[x]$ i.e. $(-1)^r x^{p+r}$ est un carré dans $\mathbb{Q}[x]$ donc r et $p+r$ sont pairs. Bilan : p, q, r sont pairs.

• Bien que la notion d'indépendance quadratique soit purement multiplicative, elle interagit avec « toute la structure de corps » de $\mathbf{K}$, du moins en caractéristique $\neq 2$. C'est l'objet des points suivants dans lesquels on suppose désormais que $\mathbf{K}$ est de $\boxed{\text{caractéristique} \neq 2}$ et que $a_1, \ldots, a_r$ sont quadratiquement indépendants. Ci-dessous, quelques résultats (ils sont liés).

(1) On a une suite d'extensions quadratiques les unes sur les autres :

$$\mathbf{K} \overset{2}{\subset} \mathbf{K}(\sqrt{a_1}) \overset{2}{\subset} \mathbf{K}(\sqrt{a_1}, \sqrt{a_2}) \overset{2}{\subset} \cdots\cdots \overset{2}{\subset} \mathbf{K}(\sqrt{a_1}, \sqrt{a_2}, \cdots, \sqrt{a_{r-1}}) \overset{2}{\subset} \mathbf{K}(\sqrt{a_1}, \sqrt{a_2}, \cdots, \sqrt{a_r})$$

(2)