File:BabyKummerTheory.tex compil. le 29 mars 2017,20:21

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

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

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

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 quadratiquement indépendante est quadratiquement indépendante.

Exemple 1. Soient $a_1, \dots, a_r$ des entiers ≥ 2, sans facteur carré, premiers entre deux à deux. Alors la famille $(a_1, \dots, a_r)$ est quadratiquement indépendante dans $\mathbb{Q}$. Il doit en être de même pour $(\varepsilon_1 a_1, \dots, \varepsilon_r a_r)$ avec des $\varepsilon_i = \pm 1$.

Exemple 2. Dans $\mathbb{Q}$, -3 et 3 sont quadratiquement indépendants (bien que non premiers entre eux). En effet, pour $p, q \in \mathbb{N}$:

$$(-3)^p 3^q \text{ carré dans } \mathbb{Q} \quad \Rightarrow \qquad p \text{ pair (puisque } (-3)^p \text{ doit être strictement positif)}$$

puis

$$3^{p+q} \text{ carré dans } \mathbb{Q} \quad \Rightarrow \qquad 3^{q+q} \text{ carré dans } \mathbb{N} \quad \Rightarrow \qquad p+q \text{ pair}$$

Bilan : p, q sont pairs.
Il en est de même pour tout entier $d \geq 2$ sans facteur carré : $(-d, d)$ sont quadratiquement indépendants sur $\mathbb{Q}$.

Exemple 3. 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 $a_1, \dots, a_r$ 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) La famille $\left(\prod_{i \in I} \sqrt{a_i}\right)_{I \subseteq \{1..r\}}$ est une $\mathbf{K}$-base de $\mathbf{K}(\sqrt{a_1}, \sqrt{a_2}, \cdots, \sqrt{a_r})$, de cardinal 2^r. On a donc :

$$\big[\mathbf{K}(\sqrt{a_1}, \sqrt{a_2}, \cdots, \sqrt{a_r}) : \mathbf{K}\big] = 2^r$$

Il est clair que les points **(1)** et **(2)** sont équivalents.
(3) ? ? ?

Eléments de preuve

On pose $\alpha_i = \sqrt{a_i}$.
• On commence par démontrer par récurrence sur r le résultat auxiliaire suivant :

$(\mathcal{P}_r)$ $\qquad [x \in \mathbf{K}(\alpha_1, \ldots, \alpha_r) \text{ et } x^2 \in \mathbf{K}] \quad \Rightarrow \quad$ il existe $I \subset \{1..r\}$ tel que $x \in \mathbf{K}\prod_{i\in I}\alpha_i$

Supposons $\mathcal{P}_{r-1}$ vérifié et posons :

$$\mathbf{K}' = \mathbf{K}(\alpha_1, \ldots, \alpha_{r-1})$$

Montrons alors que $\alpha_r \notin \mathbf{K}'$. En effet, si l'on avait $\alpha_r \in \mathbf{K}'$, puisque $\alpha_r^2 = a_r \in \mathbf{K}$, on pourrait écrire, d'après $\mathcal{P}_{r-1}$:

$$\alpha_r = \lambda \prod_{j\in J} \alpha_j, \quad \text{avec } \lambda \in \mathbf{K}^* \text{ et } J \subseteq \{1..r-1\}$$

En élevant au carré :

$$a_r = \lambda^2 \prod_{j\in J} a_j$$

contredisant ainsi l'indépendance quadratique sur $\mathbf{K}$ de la famille $(a_1, \ldots, a_r)$.
• Sous le couvert de $\mathcal{P}_{r-1}$, une fois obtenu le fait que $\alpha_r \notin \mathbf{K}'$, on a que $(1, \alpha_r)$ est une base de $\mathbf{K}(\alpha_1, \ldots, \alpha_r)$ sur $\mathbf{K}' \overset{\text{def}}{=} \mathbf{K}(\alpha_1, \ldots, \alpha_{r-1})$
• Démontrons alors $\mathcal{P}_r$ (en continuant à supposer $\mathcal{P}_{r-1}$). Soit donc $x \in \mathbf{K}'(\alpha_r)$ vérifiant $x^2 \in \mathbf{K}$ que l'on écrit sur la base $(1, \alpha_r)$ de $\mathbf{K}(\alpha_1, \ldots, \alpha_r)/\mathbf{K}'$:

$$x = u + v\alpha_r, \qquad u, v \in \mathbf{K}'$$

En élevant au carré :

$$x^2 = u^2 + a_r v^2 + 2uv\alpha_r \quad \text{i.e.} \quad \overbrace{(u^2 + a_r v^2 - x^2)}^{\in \mathbf{K}'} + \overbrace{2uv}^{\in \mathbf{K}'}\alpha_r = 0$$

Comme il a été établi que $(1, \alpha_r)$ est $\mathbf{K}'$-libre, on a (caractéristique distincte de 2) soit $u = 0$ soit $v = 0$.
▶ cas $u = 0$; alors $x = v\alpha_r$ et l'hypothèse $x^2 \in \mathbf{K}$ fait que $v^2 \in \mathbf{K}$ et comme $v \in \mathbf{K}'$, on peut conclure par récurrence sur r.
▶ cas $v = 0$; alors $x = u \in \mathbf{K}'$ et on peut conclure par récurrence sur r.

Bilan : on a d'une part prouvé $(\mathcal{P}_r)$ par récurrence sur r et d'autre part montré que $(1, \alpha_r)$ est une base de $\mathbf{K}(\alpha_1, \ldots, \alpha_r)$ sur $\mathbf{K}(\alpha_1, \ldots, \alpha_{r-1})$. Et comme $\mathcal{P}_1, \mathcal{P}_2, \ldots, \mathcal{P}_r$ sont vérifiés, on obtient le point **(1)** du bas de la page précédente (et donc le point **(2)**).

L'aspect galoisien

On garde le même contexte i.e. $\mathbf{K}$ est un corps de caractéristique $\neq 2$ et $a_1, \ldots a_r \in \mathbf{K}^*$ sont quadratiquement indépendants dans $\mathbf{K}$. On pose :

$$\mathbf{L} = \mathbf{K}(\alpha_1, \ldots, \alpha_r) \qquad \text{avec } \alpha_i^2 = a_i$$

Il est clair que $\mathbf{L}/\mathbf{K}$ est galoisienne car c'est le corps de décomposition sur $\mathbf{K}$ du polynôme :

$$(X^2 - a_1)(X^2 - a_2)\cdots(X^2 - a_r)$$

Pour $\sigma \in \mathrm{Gal}(\mathbf{L}/\mathbf{K})$, on a $\sigma(\alpha_i) = \pm\alpha_i$ et on peut définir :

$$\Phi : \mathrm{Gal}(\mathbf{L}/\mathbf{K}) \ni \sigma \longmapsto \left(\frac{\sigma(\alpha_1)}{\alpha_1}, \cdots, \frac{\sigma(\alpha_r)}{\alpha_r}\right) \in \{\pm 1\}^r$$

qui est un morphisme de groupes, visiblement injectif.
Pour conclure que Φ est un isomorphisme, on peut utiliser le fait que $\#\mathrm{Gal}(\mathbf{L}/\mathbf{K}) = [\mathbf{L} : \mathbf{K}] = 2^r$.
Mais on peut s'en passer en considérant la $\mathbf{K}$-base $(\pi_I)_{I\subseteq\{1..r\}}$:

$$\pi_I = \prod_{i\in I} \alpha_i \quad \text{qui vérifie} \quad \pi_I\pi_J = \frac{\pi_{I\cup J}}{\pi_{I\cap J}}$$

Soit $\varepsilon = (\varepsilon_1, \cdots, \varepsilon_r) \in \{\pm 1\}^r$. Il y a une seule application $\mathbf{K}$-linéaire σ_ε définie sur la $\mathbf{K}$-base :

$$\sigma_\varepsilon(\pi_I) = \prod_{i\in I} \varepsilon_i \times \pi_I$$

C'est une bijection $\mathbf{K}$-linéaire. Et on vérifie facilement que σ_ε est un morphisme de $\mathbf{K}$-algèbres de $\mathbf{L}$ sur lui-même donc un $\mathbf{K}$-automorphisme de $\mathbf{L}$. Et l'on a $\Phi(\sigma_\varepsilon) = \varepsilon$.