manuscripta math. 100, 291 – 304 (1999)

Bruno Deschamps

Clôtures totalement réelles des corps de nombres ordonnables

Received : 5 May 1998 / Revised version : 1 December 1998

Abstract. This article is concerned with arithmetic properties of totally real closures of formally real fields. We generalize previous results of Fried, Völklein and Pop to show that if an algebraic extension $K/\mathbb{Q}$ is formally real and hilbertian then the absolute Galois group of the cyclotomic closure of the totally real closure of K is pro-free. In addition, we give a precise description of the Brauer group of $\widetilde{K}_{\mathrm{tr}}$: it is always an elementary abelian 2-group. Finally, using a result of Glass and Ribenboim, we show that an automorphism of the group $\mathrm{Aut}(\widetilde{K}_{\mathrm{tr}}^{+*}, \leq_1, .)$, where K is a formally real number field, is necessarily the identity.

1. Introduction

Soit $\mathbb{Q}^{\mathrm{tr}}$ le corps des nombres algébriques totalement réels (i.e. l'ensemble des éléments de $\overline{\mathbb{Q}}$ qui n'ont que des conjugués réels). F.Pop a prouvé que $\mathbb{Q}^{\mathrm{tr}}(\sqrt{-1})$ est un corps PAC. Un corps K est dit P(seudo)-A(lgébriquement)-C(los) si et seulement si toute variété lisse irréductible définie sur K possède un point K-rationnel. Un théorème de Weissauer, qui affirme que toute extension finie stricte d'une extension galoisienne d'un corps hilbertien est hilbertienne ([FJ]), prouve que $\mathbb{Q}^{\mathrm{tr}}(\sqrt{-1})$ est hilbertien. Il s'ensuit que le groupe de Galois absolu de $\mathbb{Q}^{\mathrm{tr}}(\sqrt{-1})$ est pro-libre de rang dénombrable. Ce dernier point provient du théorème de Fried–Völklein, qui assure que tout corps PAC, hilbertien, dénombrable et de caractéristique 0 a un groupe de Galois absolu pro-libre de rang dénombrable [FV].

Nous considérons ici plus généralement la clôture totalement réelle d'un corps ordonnable K. Après avoir introduit la notion de clôture totalement réelle d'un corps ordonnable K (notée $\widetilde{K}_{\mathrm{tr}}$) et établi quelques propriétés générales sur ces corps (2.1), nous montrons, en utilisant les résultats de Fried–Völklein-Pop mentionnés ci-dessus, que la conclusion «$\widetilde{K}_{\mathrm{tr}}(\sqrt{-1})$ a un groupe de Galois absolu pro-libre» subsiste si K est un corps de nombres ordonnable. Ceci peut-être vu comme un analogue de la conjecture de Shafarevich (voir 2.3, remarque a/). Nous donnons d'autres cas où ce résultat reste vrai (e.g. $\mathbb{R}((X))$), mais en général ce résultat n'est pas vrai (voir 2.3, remarque a/). Nous complétons cette étude en donnant la structure

B. Deschamps: "Algèbre et théorie des nombres", Université Lille I, UFR de Mathématique, Bât. M2, USTL, F-59655 Villeneuve d'Ascq Cedex, France.
e-mail: brudesch@ccr.jussieu.fr

Mathematics Subject Classification (1991): Primary 12F12, 14H30; Secondary 14G20

du groupe de Brauer de $\widetilde{K}_{\rm tr}$, en particulier nous montrons que $Br(\mathbb{Q}^{tr}) \simeq \bigoplus_n \mathbb{Z}/2$ (Théorème 2) et que $Br(\mathbb{R}((X_1))\cdots((X_n))) = (\mathbb{Z}/2)^{\frac{n(n+1)}{2}+1}$ (Proposition 4).

La deuxième partie de cette article est consacrée à une application d'une idée de Glass et Ribenboim ([GR]). Nous montrons que si $\leq_1$ désigne un ordre compatible sur $\widetilde{K}_{\rm tr}$, alors tout automorphisme σ de $\widetilde{K}_{\rm tr}^{+*}$ qui respecte $\leq_1$ (i.e. $\forall (x, y) \in \widetilde{K}_{\rm tr}^{+*}$, $x \leq_1 y \Rightarrow \sigma(x) \leq_1 \sigma(y)$) est nécessairement l'identité.

Nous tenons à remercier Pierre Dèbes, Jean-Claude Douai, Dan Haran et Moshe Jarden et Florian Pop pour les remarques qu'ils ont faites sur ce texte et nous adressons de même tous nos remerciements au rapporteur de cet article pour les précieux commentaires qu'il nous a prodigués et qui ont contribué à enrichir substentiellement cet article.

2. Clôtures totalement réelles des corps ordonnables

Dans cette partie nous utiliserons les résultats principaux de la théorie d'Artin-Schreier sur les corps ordonnés. Nous renvoyons le lecteur à [R], Ch IX, dont nous utilisons la terminologie. Dans tout ce qui suit, K désignera un corps ordonnable et G_K le groupe de Galois absolu, $\mathrm{Gal}(\overline{K}/K)$, de K.

2.1. Généralités

On considère ici les classes de conjugaison des éléments d'ordre 2 de G_K. Ainsi deux éléments c, c' d'ordre 2 de G_K sont conjugués si et seulement si il existe $\sigma \in G_K$ tel que $c = \sigma c' \sigma^{-1}$. Notons alors que si $K_c = \overline{K}^{<c>}$ et $K_{c'} = \overline{K}^{<c'>}$, on a $\sigma(K_c) = K_{c'}$. Réciproquement, rappellons cet élément de la théorie d'Artin-Schreier : l'ensemble des corps K_0 extensions algébriques de K tels que $[\overline{K} : K_0] < +\infty$ est exactement l'ensemble des extensions ordonnées maximales de K. Dans ce cas, on a toujours $[\overline{K} : K_0] = 2$.

Définition 1. *On appelle pré-clôture totalement réelle de K tout corps obtenu comme intersection des extensions ordonnées maximales de K appartenant à la même classe de conjugaison. En d'autres termes L est une pré-clôture totalement réelle de K si et seulement si il existe $c \in G_K$ d'ordre 2 tel que :*

$$L = \bigcap_{\sigma \in G_K} \overline{K}^{<\sigma c \sigma^{-1}>}$$

On appelle alors clôture totalement réelle de K, le corps $\widetilde{K}_{\rm tr}$ obtenu en prenant l'intersection de toutes les pré-clôtures totalement réelles de K.

Le groupe de Galois absolu de la clôture totalement réelle d'un corps ordonné K est donc l'adhérence du sous-groupe de G_K généré par les éléments de 2-torsion (qui sont exactement les éléments de torsion de G_K d'après la théorie d'Artin-Schreier). Ce groupe étant distingué dans G_K, l'extension $\widetilde{K}_{\rm tr}/K$ est galoisienne.

Si $K = \mathbb{Q}$, comme $\mathbb{Q}$ admet un unique ordre compatible, tous les corps réel clos de $\overline{\mathbb{Q}}$ sont conjugués. Il n'y a donc qu'une seule pré-clôture totalement réelle de $\mathbb{Q}$, on la note traditionnellement $\mathbb{Q}^{tr}$. Etablissons maintenant, quelques propriétés sur ces objets :

Proposition 1. 1. *Les énoncés suivants sont équivalents :*

i) *L est une pré-clôture totalement réelle de K.*

ii) *L est une extension galoisienne ordonnable maximale (pour ces deux conditions) de K.*

iii) *Il existe $c \in G_K$ d'ordre 2 tel que $L \subset K_c = \overline{K}^{<c>}$ et telle que*

$$L = \{x \in K_c / \forall \sigma \in G_K,\ \sigma(x) \in K_c\}.$$

2. *Le corps $\widetilde{K}_{\rm tr}$ est un corps pythagoricien (i.e. $\widetilde{K}_{\rm tr}^2 = \widetilde{K}_{\rm tr}^2 + \widetilde{K}_{\rm tr}^2$), en particulier il n'est pas hilbertien.*

3. *Pour toute extension L/K de corps ordonnables, on a $\widetilde{K}_{\rm tr} \subset \widetilde{L}_{\rm tr}$. En particulier, pour tout corps ordonnable K, on a $\mathbb{Q}^{\rm tr} \subset \widetilde{K}_{\rm tr}$.*

4. *La clôture cyclotomique de $\widetilde{K}_{\rm tr}$ est le corps $\widetilde{K}_{\rm tr}(\sqrt{-1})$.*

Preuve. 1. i) $\Rightarrow$ ii) Par définition, il existe $c \in G_K$ d'ordre 2 tel que L soit le sous-corps de $\overline{K}$ laissé fixe par le sous-groupe G de G_K engendré par les $\sigma c \sigma^{-1}$. Le groupe G est distingué, son adhérence (pour la topologie de Krull) l'est donc aussi. Par conséquent l'extension L/K est galoisienne.

Soit maintenant L'/K une extension galoisienne ordonnable telle que $L \subset L'$. Soit K_0 un corps ordonné maximal contenant L' de groupe de Galois absolu $\{1, c\}$. Comme $L' \subset K_0 = \overline{K}^{<c>}$ et que L'/K est extension galoisienne, on en déduit que pour tout $\sigma \in G_K$, $L' \subset \overline{K}^{<\sigma c \sigma^{-1}>}$. Donc $L' \subset L$.

ii) $\Rightarrow$ iii) Soit L/K une extension galoisienne ordonnable maximale. Il existe une extension K_c ordonnée maximale contenant L. Soit

$$L' = \{x \in K_c / \forall \sigma \in G_K,\ \sigma(x) \in K_c\}.$$

Soit $x \in L$ et $\sigma \in G_K$, on a $\sigma(x) \in L \subset K_c$, donc $L \subset L'$.

Maintenant, il est clair que L'/K est une extension ordonnable et galoisienne. Donc $L = L'$ iii) $\Rightarrow$ i) Evident.

2. Le fait que $\widetilde{K}_{\rm tr}$ soit un corps pythagoricien provient du fait que les corps réel clos sont toujours des corps pythagoriciens et que toute intersection de corps pythagoriciens est un corps pythagoricien.

Le polynôme $X^2 - T_1^2 - T_2^2 \in \widetilde{K}_{\rm tr}(T_1, T_2)[X]$ est irréductible (nous sommes en caractéristique nulle). Or, pour toute spécialisation $(T_1, T_2) = (t_1, t_2)$, le polynôme $X^2 - t_1^2 - t_2^2$ est réductible sur $\widetilde{K}_{\rm tr}$. Donc $\widetilde{K}_{\rm tr}$ n'est pas hilbertien.

3. Soient $x \in \widetilde{K}_{\rm tr}$ et c une L-involution de $\overline{L}$. L'automorphisme c laissant fixe K, il laisse fixe $\overline{K}$ si bien que c définit par restriction une K-involution de $\overline{K}$, on a alors $c(x) = x$ et par suite $x \in \widetilde{L}_{\rm tr}$.

4. Si K_0 un corps réel clos dans $\overline{\mathbb{Q}}$ et $c \in G_{K_0}$ d'ordre 2, alors $c(\zeta_n) = \zeta_n^{-1}$ pour tout ζ_n racine n-ième de l'unité. En effet, $\zeta_n c(\zeta_n) \in K_0$, mais comme $\zeta_n c(\zeta_n)$ est aussi une racine de l'unité, on en déduit que $\zeta_n c(\zeta_n) = 1$ (il est classique qu'un corps ordonnable ne possède pas d'autres racines de l'unité que ± 1, le cas -1 s'élimine de lui-même).

Prenons ζ_n une racine primitive n-ième de l'unité et notons $\alpha_n = \zeta_n + \zeta_n^{-1}$ et $\beta_n = \sqrt{-1}(\zeta_n - \zeta_n^{-1})$. D'après ce qui précède, tous corps réel clos contient α_n et β_n, par conséquent α_n et β_n sont dans $\mathbb{Q}^{tr}$. Or $\zeta_n = \frac{1}{2}(\alpha_n - \sqrt{-1}\beta_n) \in \mathbb{Q}^{tr}(\sqrt{-1})$.

Soit maintenant K un corps ordonnable quelconque, puisque $\mathbb{Q}^{tr} \subset \widetilde{K}_{tr}$ et que $\mathbb{Q}^{tr}(\sqrt{-1})$ contient les racines de l'unité, on en déduit immédiatement que $\widetilde{K}_{tr}^{cycl} = \widetilde{K}_{tr}(\sqrt{-1})$ (il est évident que puisque $\widetilde{K}_{tr}$ est ordonnable, $\sqrt{-1} \notin \widetilde{K}_{tr}$). □

2.2. *Exemples*

Exemple 1. Considérons un corps de nombres ordonnable K. Si $K \subset \mathbb{Q}^{tr}$ (en particulier si K est une extension galoisienne ordonnable de $\mathbb{Q}$), alors $\widetilde{K}_{tr} = \mathbb{Q}^{tr}$. En effet, comme $K \subset \mathbb{Q}^{tr}$, on a donc $\widetilde{K}_{tr} \subset \widetilde{\mathbb{Q}^{tr}}_{tr} = \mathbb{Q}^{tr}$ (on a toujours $\widetilde{(\widetilde{K}_{tr})}_{tr} = \widetilde{K}_{tr}$). De plus, $\mathbb{Q} \subset K$, donc $\mathbb{Q}^{tr} \subset \widetilde{K}_{tr}$.

Lorsque $K = \mathbb{Q}(\alpha)$ est un corps de nombres ordonnable non inclus dans $\mathbb{Q}^{tr}$ (par exemple $K = \mathbb{Q}(\sqrt[3]{2})$) le problème est plus délicat. On sait que $\mathbb{Q}^{tr}(\alpha) \subset \widetilde{K}_{tr}$. On peut affirmer que cette inclusion est toujours stricte et même que $[\widetilde{K}_{tr} : \mathbb{Q}^{tr}(\alpha)]$ est infini. En effet, d'après le théorème de Weissauer (voir introduction), toute extension finie de $\mathbb{Q}^{tr}(\alpha)$ est hilbertienne. Mais $\widetilde{K}_{tr}$ n'est pas hilbertien (proposition 1).

Exemple 2. Regardons maintenant le cas d'une extension transcendante de $\mathbb{Q}$. On pose $\mathbb{Q}^r = \overline{\mathbb{Q}} \cap \mathbb{R}$. Soit alors $K = \mathbb{Q}^r((X))$ le corps des séries de Laurent à coefficients dans $\mathbb{Q}^r$ (c'est un corps ordonnable, par exemple par l'ordre lexicographique).

Proposition 2. *On a* $\widetilde{\mathbb{Q}^r((X))}_{tr} = \mathbb{Q}^r((X))$. *De manière plus précise,* $\mathbb{Q}^r((X))$ *ne possède que deux pré-clôtures totalement réelles qui sont les corps* $\mathbb{Q}^r((\sqrt{X}))$ *et* $\mathbb{Q}^r((\sqrt{-X}))$.

Preuve. Soit $E/\mathbb{Q}^r((X))$ une extension galoisienne ordonnable maximale. Il est clair que $E \cap \overline{\mathbb{Q}} = \mathbb{Q}^r$: sinon cette intersection vaut $\overline{\mathbb{Q}}$ tout entier et alors E n'est plus ordonnable (car $\sqrt{-1} \in E$). On en déduit alors que E est une extension régulière sur $\mathbb{Q}^r$.

Considérons une extension galoisienne $F/\mathbb{Q}^r((X))$ de degré fini $n > 1$, avec $F \subset E$ et posons $F' = \overline{\mathbb{Q}}.F$. Comme $F/\mathbb{Q}^r((X))$ est régulière, il s'ensuit que $F'/\overline{\mathbb{Q}}((X))$ est galoisienne de degré n. D'après le théorème de Puiseux, $F' = \overline{\mathbb{Q}}((X^{1/n}))$ et $\mathrm{Gal}(F'/\overline{\mathbb{Q}}((X)))$ est le groupe cyclique $\mathbb{Z}/n$ engendré par l'automorphisme σ_0 qui laisse invariant $\overline{\mathbb{Q}}$ et qui envoie $X^{1/n}$ sur $\zeta_n X^{1/n}$ (ζ_n désigne une racine primitive n-ième de l'unité fixée une fois pour toutes).

Il est clair que $F \subset F'$. On a les extensions :

$$\begin{array}{ccc} \mathbb{Q}^r((X)) & \xrightarrow{\mathbb{Z}/2} & \overline{\mathbb{Q}}((X)) \\ {\scriptstyle \mathbb{Z}/n}\big\downarrow & & {\scriptstyle \mathbb{Z}/n}\big\downarrow \\ F & \xrightarrow{\mathbb{Z}/2} & F' \end{array} .$$

L'extension $F'/\mathbb{Q}^r((X))$ est galoisienne et son groupe de Galois est isomorphe au groupe diédral D_n. En effet, la conjugaison complexe c est un automorphisme du corps des séries de Puiseux, $Puis(\overline{\mathbb{Q}})$, qui relève l'élément non trivial de $\mathrm{Gal}(\overline{\mathbb{Q}}((X))/\mathbb{Q}^r((X)))$ dans $\mathrm{Gal}(F'/\mathbb{Q}^r((X)))$. On vérifie sans mal que l'action de c sur σ_0 est $\sigma_0{}^c = \sigma_0^{-1}$.

Le groupe $\mathrm{Gal}(\overline{\mathbb{Q}}((X^{1/n}))/F)$ est un sous-groupe distingué d'ordre 2 de D_n. Par conséquent n est pair et si $n > 2$ alors ce groupe est le centre $Z(D_n)$ de D_n. Mais $Z(D_n)$ ($\subset \mathbb{Z}/n$) laisse fixe $\overline{\mathbb{Q}}$, ce qui contredit $F \cap \overline{\mathbb{Q}} = \mathbb{Q}^r$, donc $n = 2$.

Ainsi, il existe $S(X) \in \mathbb{Q}^r((X))$ qui n'est pas un carré et tel que

$$F = \mathbb{Q}^r((X))(\sqrt{S(X)}).$$

Deux cas se présentent alors,

- $S(X) = X^\alpha(1 + \sum_{n>0} a_n X^n)$ ($\alpha \notin 2\mathbb{Z}$) et dans ce cas $F = \mathbb{Q}^r((\sqrt{X}))$.
- $S(X) = -X^\alpha(1 + \sum_{n>0} a_n X^n)$ ($\alpha \notin 2\mathbb{Z}$) et dans ce cas $F = \mathbb{Q}^r((\sqrt{-X}))$.

Ces deux corps sont bien ordonnables puisqu'ils sont tout deux isomorphes à $\mathbb{Q}^r((X))$. Maintenant, E ne peut pas contenir simultanément $\mathbb{Q}^r((\sqrt{X}))$ et $\mathbb{Q}^r((\sqrt{-X}))$, sinon E contiendrait $\sqrt{-1}$, ce qui est impossible puisque E est ordonnable. Comme E est limite inductive de ses sous-extensions galoisiennes finies, E est soit $\mathbb{Q}^r((\sqrt{X}))$, soit $\mathbb{Q}^r((\sqrt{-X}))$. L'intersection de ces deux corps est bien réduite à $\mathbb{Q}^r((X))$. □

L'exemple précédent se généralise à $K((X))$ quand K désigne une extension ordonnée maximale d'un corps ordonnable quelconque (par exemple $\mathbb{R}((X))$). Dans le cas de $K((X))$, avec K un corps ordonnable, le problème est plus délicat car nous possédons moins de renseignements sur la nature des extensions finies de ce corps, on peut toutefois décrire assez clairement $\widetilde{K((X))}_{tr}$ de la manière suivante :

Théorème 1. *Soit K un corps ordonnable, le corps $\widetilde{K((X))}_{tr}$ est égal à la clôture algébrique de $K((X))$ dans $\widetilde{K}_{tr}((X))$.*

Preuve. Pour établir ce résultat, rappelons tout d'abord le lemme suivant : si L est un corps, on note $Puis(L)$ le corps des séries de Puiseux à coefficients dans L, on a alors :

Lemme. *Soit K un corps de caractéristique* 0. *La clôture algébrique de $K((X))$ dans le corps $Puis(\overline{K})$ des séries de Puiseux à coefficients dans $\overline{K}$ est égale* $\bigcup_{L/K \text{ finie}}$ *$Puis(L)$ (cette réunion étant en fait une limite inductive).*

Preuve du lemme. Soit L/K une extension finie de degré d et $T(X) = \sum_{k \geq k_0} a_k X^{\frac{k}{n}}$ ($n \in \mathbb{N}$) un élément de $Puis(L)$. Comme $X^{\frac{1}{n}}$ est de degré n sur $K((X))$, on en déduit que T est de degré au plus nd sur $K((X))$ et par suite que $\mathrm{Puis}(L)$ est une extension algébrique de $K((X))$. Donc

$$\bigcup_{L/K \text{ finie}} \mathrm{Puis}(L) \subset \overline{K((X))}.$$

Réciproquement, soit $T(X) = \sum_{k \geq k_0} a_k X^{\frac{k}{n}} \in \overline{K((X))}$. Notons L le corps engendré sur K par les coefficients a_k et montrons que L/K est finie. Prenons σ_1 et σ_2, deux K-isomorphismes distincts de L. Il est clair que σ_1 et σ_2 peuvent être vus comme $K((X))$-isomorphismes de $K((X))(T)$ (l'action de σ_1 et σ_2 sur T étant définie par l'action sur les coefficients des séries). Mais alors, $\sigma_1(T) \neq \sigma_2(T)$ car sinon $\sigma_1(a_k) = \sigma_2(a_k)$ pour tout k et par suite, comme L est engendré par les a_k, l'action de σ_1 et σ_2 coinciderait sur L. Comme pour tout K-isomorphisme σ de L, $\sigma(T)$ est un conjugué de T sur $K((X))$ dans $\overline{K((X))}$, on en déduit qu'il y a au maximum $[K((X))(T) : K((X))]$ K-isomorphismes de L, c'est à dire (puisque nous sommes en caractéristique 0) que L/K est finie. $\square$

Revenons à la preuve de notre théorème, et prenons K un corps ordonnable, notons Ω la clôture algébrique de $K((X))$ dans $\widetilde{K}_{\mathrm{tr}}((X))$. Etablissons quelques résultats intermédiaires :

a) On a $\Omega \subset \widetilde{K((X))}_{\mathrm{tr}}$. Par le lemme, on obtient immédiatement que $\Omega = \bigcup_L L((X))$ avec $L \subset \widetilde{K}_{\mathrm{tr}}$ et L/K finie. Alors, si c est une $K((X))$-involution de $\overline{K((X))}$, c définit par restriction une K-involution de $\overline{K}$. Soit L/K finie et α un élément primitif de L/K, α est aussi un élément primitif de $L((X))/K((X))$. Toute série $S(X) \in L((X))$ pouvant s'écrire $S(X) = \sum_{k=0}^{d} \alpha^k S_k(X)$ (avec $S_d(X) \in K((X))$), on en déduit alors que l'action de c sur les séries de $L((X))$ est l'action de c sur les coefficients de ces séries. Par suite, si $L \subset \widetilde{K}_{\mathrm{tr}}$, $L((X))$ est laissé fixe par c.

b) On a $\widetilde{K((X))}_{\mathrm{tr}} \subset \mathrm{Puis}(\widetilde{K}_{\mathrm{tr}})$. Soit $c \in G_K$ une involution, il est clair que c se relève en une involution de $\mathrm{Puis}(\overline{K})$ par action sur les coefficients des séries. La restriction $\tilde{c}$ de ce relevé à $\overline{K((X))}$ est une $K((X))$-involution de $\overline{K((X))}$. Soit $T(X) = \sum_{k \geq k_0} a_k X^{\frac{k}{n}} \in \widetilde{K((X))}_{\mathrm{tr}}$, pour tout $c \in G_K$, on a $\tilde{c}(T) = T$, c'est à dire que pour tout k, $c(a_k) = a_k$. On en déduit donc que $a_k \in \widetilde{K}_{\mathrm{tr}}$.

c) On a en fait $\widetilde{K((X))}_{\mathrm{tr}} \subset \widetilde{K}_{\mathrm{tr}}((\sqrt{X}))$. Soit $T(X) = \sum_{k \geq k_0} a_k X^{\frac{k}{n}} \in \widetilde{K((X))}_{\mathrm{tr}}$ et soit ξ_n une racine primitive n-ième de l'unité. Le groupe de Galois de $\overline{K}((X^{\frac{1}{n}}))/\overline{K}((X))$ est engendré par l'automorphisme σ qui a $X^{\frac{1}{n}}$ associe $\xi_n X^{\frac{1}{n}}$. Cet automorphisme

σ se relève au corps $\mathrm{Puis}(\overline{K})$, σ laisse invariant $K((X))$ et globalement invariant $\overline{K((X))}$. Comme $T \in \overline{K}((X^{\frac{1}{n}}))$, on a alors $\sigma(T) = \sum_{k \geq k_0} a_k \xi_n^k X^{\frac{k}{n}} \in \widetilde{K((X))}_{\mathrm{tr}}$ puisque $\widetilde{K((X))}_{\mathrm{tr}}/K((X))$ est galoisienne. Mais alors pour tout k, en vertu du b), $a_k \xi_n^k \in \widetilde{K}_{\mathrm{tr}}$, ceci n'est donc possible que si $\xi_n = \pm 1$, c'est à dire si $n = 1$ ou 2.

d) On a pour finir, $\widetilde{K((X))}_{\mathrm{tr}} \subset \widetilde{K}_{\mathrm{tr}}((X))$. D'après le c), si $T \in \widetilde{K((X))}_{\mathrm{tr}}$, alors T s'écrit dans $\mathrm{Puis}(\overline{K})$, $T(X) = \sum_{k \geq k_0} a_k \sqrt{X}^k$.

Considérons un corps réel clos R de $\overline{K}$ qui contient $\widetilde{K}_{\mathrm{tr}}$. Le corps $R((\sqrt{-X}))$ est ordonnable, soit alors $\widetilde{R}$ une extension algébrique ordonnée maximale de $R((\sqrt{-X}))$ dans $\mathrm{Puis}(\overline{K})$. Notons c l'involution de $\mathrm{Puis}(\overline{K})$ correspondant à $\widetilde{R}$, c est donc une $R((\sqrt{-X}))$-involution. Si $c(\sqrt{X}) = \sqrt{X}$, alors $\sqrt{X} \in \widetilde{R}$, mais comme $\sqrt{-X} \in \widetilde{R}$ on en déduit alors que $\widetilde{R}$ n'est pas ordonnable (car $(\sqrt{X})^2 + (\sqrt{-X})^2 = 0$), ce qui est absurde. Donc $c(\sqrt{X}) = -\sqrt{X}$ et par suite, il existe une $R((\sqrt{-X}))$-involution c de $\mathrm{Puis}(\overline{K})$ qui envoie $\sqrt{X}$ sur $-\sqrt{X}$. L'involution c est aussi une $\widetilde{K}_{\mathrm{tr}}((X))$-involution et définit par restriction une $\widetilde{K}_{\mathrm{tr}}((X))$-involution de $\widetilde{K}_{\mathrm{tr}}((X))$. Il existe $S_1(X)$ et $S_2(X)$ dans $\widetilde{K}_{\mathrm{tr}}((X))$ telles que

$$(T(X) - S_1(X)) = \sqrt{X} S_2(X)$$

mais alors en faisant opérer c, on a

$$(c(T) - c(S_1)) = -\sqrt{X} c(S_2)$$

et comme $c(S_1) = S_1$, $c(S_2) = S_2$ et $c(T) = T$ (T est un élément totalement réel), on en déduit que $S_2 = 0$, c'est à dire $T \in \widetilde{K}_{\mathrm{tr}}((X))$. On a alors $\widetilde{K((X))}_{\mathrm{tr}} \subset \widetilde{K}_{\mathrm{tr}}((X)) \cap \overline{K((X))} = \Omega$. $\square$

Dans le cas où K est un corps réel clos, on retrouve la proposition 2. Le théorème a alors pour corollaire immédiat :

Corollaire 1. *Soit K un corps ordonnable tel que $\widetilde{K}_{\mathrm{tr}} = K$, et n un entier non nul. On a :*

$$\widetilde{K((X_1))\cdots((X_n))}_{\mathrm{tr}} = K((X_1))\cdots((X_n)).$$

Nous allons nous intéresser dans la partie suivante à certaines propriétés arithmétiques des clôtures totalement réelles, notamment dans le cas des corps de nombres ordonnable.

2.3. *Propriétés arithmétiques*

Théorème 2. *Soit K une extension algébrique ordonnable de $\mathbb{Q}$.*

1. *Le corps $\widetilde{K}_{\mathrm{tr}}$ est un corps ample*[1] *et le corps $\widetilde{K}_{\mathrm{tr}}(\sqrt{-1})$ est un corps PAC. En conséquence, si K est hilbertien (en particulier si K est un corps de nombres), alors $G_{\widetilde{K}_{\mathrm{tr}}(\sqrt{-1})}$ est pro-libre.*

[1] Un corps K est dit ample, si toutecourbe lisse et géométriquement irréductible définie sur K possède une infinité de points K-rationnels pour peu qu'elle en possède au moins un. Cette notion à été introduite par Florian Pop (cf [DD]).

2. *Il existe un ensemble D au plus dénombrable tel que $Br(\widetilde{K}_{\rm tr}) = \bigoplus_D \mathbb{Z}/2$, plus exactement, on a*

$$Br(\widetilde{K}_{\rm tr}) \simeq (\widetilde{K}_{\rm tr}^{*})/(\widetilde{K}_{\rm tr}^{*})^{2}$$

en particulier $Br(\mathbb{Q}^{tr}) = \bigoplus_{\mathbb{N}} \mathbb{Z}/2$.

Preuve. 1. La première partie du 1/ est une conséquence du théorème de Pop qui affirme que $\mathbb{Q}^{\rm tr}$ est ample et que $\mathbb{Q}^{\rm tr}(\sqrt{-1})$ est PAC. Les corps $\widetilde{K}_{\rm tr}$ et $\widetilde{K}_{\rm tr}(\sqrt{-1})$ sont respectivement des extensions algébriques de ces deux corps. Or, toute extension algébrique d'un corps ample (resp. PAC) est ample (resp. PAC) (voir [P]). Maintenant si K est hilbertien, le théorème de Weissauer assure que $\widetilde{K}_{\rm tr}(\sqrt{-1})$ est hilbertien, par application du théorème de Fried–Völklein, il s'ensuit que $G_{\widetilde{K}_{\rm tr}(\sqrt{-1})}$ est pro-libre.

2. On a $cd(\widetilde{K}_{\rm tr}(\sqrt{-1})) \leq 1$ (ceci provient du fait qu'un corps PAC est projectif, on peut le voir directement en constatant ques les racines de l'unité sont dans $\widetilde{K}_{\rm tr}(\sqrt{-1})$ (voir [S2])). Par conséquent $Br(\widetilde{K}_{\rm tr}(\sqrt{-1})) = 0$. La suite exacte $1 \to H^2(E/L) \to Br(L) \to Br(E)$ où E/L est un extension algébrique, donne alors l'isomorphisme $Br(\widetilde{K}_{\rm tr}) \simeq H^2(\widetilde{K}_{\rm tr}(\sqrt{-1})/\widetilde{K}_{\rm tr})$. Reste à calculer ce dernier groupe de cohomologie :

Soit $x \in \widetilde{K}_{\rm tr}^{*}(\sqrt{-1})$, on note $N(x) = x\overline{x} = |x|^2$ et $T(x) = \overline{x}x^{-1}$. On a alors $H^2(\widetilde{K}_{\rm tr}(\sqrt{-1})/\widetilde{K}_{\rm tr}) \simeq T^{-1}(1)/N(\widetilde{K}_{\rm tr}^{*}(\sqrt{-1}))$ (ceci vient d'un lemme de cohomologie des groupes classique, voir par exemple [S1] ou [B], lemme IV.5, p. 107). On a clairement $T^{-1}(1) = \widetilde{K}_{\rm tr}^{*}$ et puisque $\widetilde{K}_{\rm tr}$ est pythagoricien, on a $N(\widetilde{K}_{\rm tr}(\sqrt{-1})) = \widetilde{K}_{\rm tr}^{*2}$. On obtient bien $Br(\widetilde{K}_{\rm tr}) \simeq (\widetilde{K}_{\rm tr}^{*})/(\widetilde{K}_{\rm tr}^{*})^{2}$.

Vu sous cette forme, il est clair que $Br(\widetilde{K}_{\rm tr})$ est abélien et a tous ces éléments d'ordre 2. La donnée du cardinal d'un tel groupe commutatif définit à isomorphisme près ce groupe : En effet soient G et G' deux tels groupes de même cardinal. G et G' sont tout deux des $\mathbb{F}_2$-espaces vectoriels. Leur dimension est égale à leur cardinal. Ils sont donc isomorphes.

Reste à voir que $Br(\mathbb{Q}^{\rm tr})$ est bien infini. Pour cela il suffit de considérer les éléments $\sqrt{p}$ de $\mathbb{Q}^{\rm tr}$ où p est un nombre premier. Chacun d'eux définit une classe distincte modulo $\left(\mathbb{Q}^{\rm tr}\right)^{*2}$: en effet si p et q sont deux nombres premiers distincts, il n'existe pas d'éléments $x \in \mathbb{Q}^{\rm tr}$ tel que $\sqrt{p/q} = x^2$ car $\sqrt[4]{p/q}$ n'a pas tous ses conjugués dans $\mathbb{R}$. □

Remarques 1. a) La proposition 1/ du théorème constitue un analogue à la conjecture de Shafarevich (qui prévoit que $G_{\mathbb{Q}^{\rm cycl}}$ est pro-libre). Le point essentiel pour cette analogie est de regarder la conjecture de Shafarevich comme un cas particulier de celle de Fried–Völklein qui prévoit qu'un corps dénombrable, hilbertien à groupe de Galois absolu projectif, a un groupe de Galois absolu pro-libre (voir [FJ] et [DD]). En effet, $\mathbb{Q}^{\rm cycl}$ possède toutes ces propriétés (Kyuk ayant prouvé que $\mathbb{Q}^{\rm cycl}$ était hilbertien). Ici le corps $\widetilde{K}_{\rm tr}(\sqrt{-1})$ est non seulement projectif, mais en plus PAC, ce qui correspond au cas particulier démontré de la conjecture de Fried–Völklein.

Remarquons que dans le cas $K = \mathbb{Q}^r((X))$, le groupe $G_{\overline{\mathbb{Q}}((X))} \simeq \widehat{\mathbb{Z}}$ est pro-libre (de rang 1). Dans cette direction, D.Haran et M.Jarden ont donné des exemples de corps K, tels que $G_{\widetilde{K}_{\rm tr}(\sqrt{-1})}$ soient pro-libres de rang e pour tout

entier e. Cependant, $G_{\widetilde{K}_{\rm tr}(\sqrt{-1})}$ n'est pas pro-libre en général (et donc l'analogue de la conjecture de Shafarevich mentionnée plus haut, n'est pas vraie en général). Dans [EH], I.Efrat et D.Haran donne un exemple de corps pythagoricien K tel que $G_K \simeq \mathbb{Z}/2 \times_s (\mathbb{Z}_2 \times \mathbb{Z}_2)$ (l'action de $\mathbb{Z}/2$ sur $\mathbb{Z}_2 \times \mathbb{Z}_2$ étant défini comme suit : si α désigne un générateur de $\mathbb{Z}_2 \times 0$ et β un générateur de $0 \times \mathbb{Z}_2$, alors l'élément non trivial de $c \in \mathbb{Z}/2$ agit sur α et β par $\alpha^c = \alpha^{-1}$ et $\beta^c = \beta^{-1}$). Le groupe $\mathbb{Z}/2 \times_s (\mathbb{Z}_2 \times \mathbb{Z}_2)$ est engendré par des éléments d'ordre 2. Il s'ensuit que $\widetilde{K}_{\rm tr} = K$ (notons qu'alors K est ordonnable). En adjoignant $\sqrt{-1}$ à $\widetilde{K}_{\rm tr}$, on obtient que $G_{\widetilde{K}_{\rm tr}(\sqrt{-1})} \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$ (l'élément non trivial de $\mathbb{Z}/2$ dans $\mathbb{Z}/2 \times_s (\mathbb{Z}_2 \times \mathbb{Z}_2)$ correspond à la conjugaison "complexe" dans n'importe quelle extension ordonnée maximale de K, dans $\overline{K}$). Or $\mathbb{Z}_2 \times \mathbb{Z}_2$ est de dimension cohomologique 2, $G_{\widetilde{K}_{\rm tr}(\sqrt{-1})}$ n'est donc pas projectif, donc pas pro-libre. Le corollaire 1, donne lui aussi un tel exemple : prenons $K = \mathbb{R}((X_1))\cdots((X_n))$, on a alors $\widetilde{K}_{\rm tr}(\sqrt{-1}) = \mathbb{C}((X_1))\cdots((X_n))$ qui a pour dimension cohomologique n.

b) La preuve de la partie 2/ du théorème 2 repose sur le fait que $G_{\widetilde{K}_{\rm tr}(\sqrt{-1})}$ est projectif. Elle est donc valable pour tout corps tel que $G_{\widetilde{K}_{\rm tr}(\sqrt{-1})}$ soit projectif, par exemple pour $K = \mathbb{R}((X))$, $Br(\mathbb{R}((X)))$ est alors isomorphe à $\mathbb{Z}/2 \times \mathbb{Z}/2$, les classes de $Br(\mathbb{R}((X)))$ étant, modulo les carrés, les élément $1, -1, X, -X$. Dans le cas $K \subset \overline{\mathbb{Q}}$, les choses se passent bien. Remarquons à ce propos que l'on peut, grâce au théorème de Whaples, caractériser plus finement les corps $\widetilde{K}_{\rm tr}$, à groupe de Brauer $\mathbb{Z}/2$:

Proposition 3. *Soit K une extension algébrique de $\mathbb{Q}$, alors $Br(\widetilde{K}_{\rm tr}) = \mathbb{Z}/2$ si et seulement si le groupe de Klein $G = \mathbb{Z}/2 \times \mathbb{Z}/2$ n'est pas groupe de Galois sur $\widetilde{K}_{\rm tr}$.*

Preuve. En effet le théorème de Whaples indique qu'il y a équivalence pour un corps K qui ne contient pas $\sqrt{-1}$ entre :

i) K n'a pas d'extension abélienne de degré 4 ;

ii) $K = K^2 \cup (-K^2)$ et K est pythagoricien.

Le corps $\widetilde{K}_{\rm tr}$ étant toujours pythagoricien, d'après le théorème de Diller et Dress ([Rib]), $\widetilde{K}_{\rm tr}$ n'a aucune extension cyclique de degré 4. Donc les seules extensions abéliennes à éviter pour $\widetilde{K}_{\rm tr}$ sont celles de groupe $G = \mathbb{Z}/2 \times \mathbb{Z}/2$. □

De manière générale, on peut affirmer :

Théorème 3. *Soit K un corps ordonnable, $Br(\widetilde{K}_{\rm tr})$ est un 2-groupe abélien élémentaire (i.e. tous les éléments de $Br(\widetilde{K}_{\rm tr})$ sont d'ordre 2).*

Preuve. De [Sc], p. 237 (36), on déduit que pour tout corps K ordonnable de groupe de Galois Γ et tout entier n, on a la suite exacte :

$$1 \longrightarrow H^1(\Gamma/T, PGL_n(\overline{K})) \longrightarrow H^1(\Gamma, PGL_n(\overline{K})) \longrightarrow \prod_{\xi} H^1(K_\xi, PGL_n(\overline{K})),$$

où T désigne le sous-groupe de Γ engendré par les éléments de torsion, ξ parcourt les ordres compatibles sur K et K_ξ correspond au corps réels clos associés à ξ. Si l'on prend $K = \widetilde{K}_{\rm tr}$, alors $T = \Gamma$, il y a donc une injection de $H^1(\Gamma, PGL_n(\overline{K}))$ dans $\prod_\xi H^1(K_\xi, PGL_n(\overline{K}))$. Maintenant si $n \neq 2$, $H^1(K_\xi, PGL_n(\overline{K})) = 0$ et donc $H^1(\Gamma, PGL_n(\overline{K})) = 0$. Si $n = 2$ alors $H^1(\Gamma, PGL_2(\overline{K})) = 0$ s'injecte dans $\prod_\xi \mathbb{Z}/2$. $H^1(\Gamma, PGL_n(\overline{K}))$ représentant la partie de n-torsion de $Br(K)$, la preuve est ainsi établie. Notons que vu sous cette forme, les éléments de $Br(K)$ proviennent en quelques sortes des ordres compatibles sur K. □

Dans le cas de $K = \mathbb{R}((X_1))\cdots((X_n))$, on trouve plus précisement :

Proposition 4. *Pour tout entier $n \in \mathbb{N}$, on a*

$$Br(\mathbb{R}((X_1))\cdots((X_n))) = (\mathbb{Z}/2)^{\alpha_n}$$

avec $\alpha_n = \dfrac{n(n+1)}{2} + 1$ (cette propriété restant valable si l'on remplace $\mathbb{R}$ par n'importe quel corps réel clos).

Preuve. Etablissons pour commencer le lemme suivant :

Lemme. *Soit $n \in \mathbb{N}^*$. Le groupe de Galois absolu de $\mathbb{C}((X_1))\cdots((X_n))$ est égal à $\widehat{\mathbb{Z}} \times \cdots \times \widehat{\mathbb{Z}}$ (n fois). En conséquence de quoi le groupe de Galois absolu de $\mathbb{R}((X_1))\cdots((X_n))$ est égal à $\mathbb{Z}/2 \times_s (\widehat{\mathbb{Z}} \times \cdots \times \widehat{\mathbb{Z}})$ (l'action de $\mathbb{Z}/2$ sur $(\widehat{\mathbb{Z}} \times \cdots \times \widehat{\mathbb{Z}})$ étant le passage à l'inverse). En particulier, ce dernier groupe est librement engendré par $n+1$ involutions.*

Preuve du lemme. Pour ne pas alourdir de notations la preuve, nous traitons juste le cas $n = 2$, le cas général s'obtenant de manière similaire.

Le lemme de la preuve du théorème 1, permet d'affirmer que $\overline{\mathbb{C}((X))((Y))}$ est égal à $\bigcup_{(n,m)} \mathbb{C}((X^{\frac{1}{n}}))((Y^{\frac{1}{m}}))$. L'extension $\mathbb{C}((X^{\frac{1}{n}}))((Y^{\frac{1}{m}}))/\mathbb{C}((X))((Y))$ a pour groupe de Galois $\mathbb{Z}/n \times \mathbb{Z}/m$. Les flêches du système projectif $(\mathbb{Z}/n \times \mathbb{Z}/m)_{n,m}$ associé se considérent coordonnées par coordonnées. On a donc en passant à la limite inverse :

$$\mathrm{Gal}(\overline{\mathbb{C}((X))((Y))}/\mathbb{C}((X))((Y))) = \widehat{\mathbb{Z}} \times \widehat{\mathbb{Z}}$$

l'action d'un couple $(\sigma, \mu) \in \widehat{\mathbb{Z}} \times \widehat{\mathbb{Z}}$ sur un élément $S = \sum_{q \geq q_0, p \geq n_q} a_{p,q} X^{\frac{p}{n}} Y^{\frac{q}{m}}$ de $\overline{\mathbb{C}((X))((Y))}$ étant visiblement égal à :

$$(\sigma, \mu)(S) = \sum_{q \geq q_0, p \geq n_q} a_{p,q} \sigma(X^{\frac{p}{n}}) \mu(Y^{\frac{q}{m}})$$

($\widehat{\mathbb{Z}}$ étant alors vu comme groupe de Galois absolu de $\mathbb{C}((X))$ resp. $\mathbb{C}((Y))$).

La conjugaison complexe définit par action sur les coordonnées des séries l'élément non trivial de $\mathrm{Gal}(\mathbb{C}((X))((Y))/\mathbb{R}((X))((Y)))$. Elle se relève en une involution c de $\overline{\mathbb{C}((X))((Y))}$ par action sur les coefficients des séries de Puiseux. On a alors la suite exacte scindée suivante :

$$1 \longrightarrow \mathbb{Z}/2 \longrightarrow G_{\mathbb{R}((X))((Y))} \longrightarrow \widehat{\mathbb{Z}} \times \widehat{\mathbb{Z}} \longrightarrow 1.$$

On vérifie sans mal que l'action de c sur $\widehat{\mathbb{Z}} \times \widehat{\mathbb{Z}}$ est bien le passage à l'inverse, ce qui permet d'écrire

$$G_{\mathbb{R}((X))((Y))} \simeq \mathbb{Z}/2 \times_s (\widehat{\mathbb{Z}} \times \widehat{\mathbb{Z}}).$$

Dans ce dernier groupe, il est clair que les involutions $(c, (0,0))$, $(c, (\alpha, 0))$, $(c, (0, \beta))$ (α et β étant des générateurs topologique de $\widehat{\mathbb{Z}}$) engendrent librement ce groupe.

Dans le cas général, on a :

$$G_{\mathbb{R}((X_1))\cdots((X_n))} \simeq \mathbb{Z}/2 \times_s (\widehat{\mathbb{Z}} \times \cdots \times \widehat{\mathbb{Z}})$$

les $n+1$ involutions à considérer étant

$$(c, (0, \cdots, 0)), (c, (a_1, \cdots, 0)), \cdots, (c, (0, \cdots, a_n))$$

où chaque a_i est un générateur topologique de $\widehat{\mathbb{Z}}$. □

Revenons à la preuve de notre proposition. Elle est visiblement vraie au rang $n = 0$, supposons la vraie au rang n et posons $k = \mathbb{R}((X_1))\cdots((X_n))$ et $K = \mathbb{R}((X_1))\cdots((X_{n+1})) = k((X))$. Comme K est complet, on a alors (voir [S1]) la suite exacte suivante :

$$1 \longrightarrow Br(k) \longrightarrow Br(K) \longrightarrow \mathrm{Hom}(G_k, \mathbb{Q}/\mathbb{Z}) \longrightarrow 1.$$

Comme G_k est librement engendré par $n+1$ involutions, on en déduit que $\mathrm{Hom}(G_k, \mathbb{Q}/\mathbb{Z}) = (\mathbb{Z}/2)^{n+1}$. D'après le théorème 3, $Br(K)$ est un 2-groupe abélien élémentaire, on a donc $Br(K) = (\mathbb{Z}/2)^{\alpha_{n+1}}$, avec $\alpha_{n+1} = \alpha_n + (n+1) = \dfrac{(n+1)(n+2)}{2} + 1$. □

Mentionnons pour finir ce paragraphe, la conjecture la plus «raisonnable» sur la pro-liberté de $G_{\widetilde{K}_{\mathrm{tr}}(\sqrt{-1})}$ dans le cas général :

Conjecture. *Soit K un corps dénombrable, ordonnable et hilbertien. Si $G_{\widetilde{K}_{\mathrm{tr}}(\sqrt{-1})}$ est projectif, alors $G_{\widetilde{K}_{\mathrm{tr}}(\sqrt{-1})}$ est pro-libre.*

(Cette conjecture est en fait un cas particulier de la conjecture de Fried–Völklein, puisqu'alors, par le théorème de Weissauer, $\widetilde{K}_{\mathrm{tr}}(\sqrt{-1})$ est un corps hilbertien.)

3. Automorphismes préservant l'ordre

Dans [GR], Glass et Ribenboim prouvent le résultat suivant :

Théorème. *Soit G un sous-groupe multiplicatif de $\overline{\mathbb{Q}} \cap \mathbb{R}^{+*}$ ordonné par l'ordre induit par $\mathbb{R}$. Le groupe des automorphismes de G préservant l'ordre, $\mathrm{Aut}(G, \leq, .)$ est isomorphe à un sous-groupe de $(\mathbb{Q}^{+*}, .)$.*

De manière plus précise, si σ désigne un automorphisme de G qui respecte l'ordre (i.e. $x < y \Rightarrow \sigma(x) < \sigma(y)$), alors il existe $r \in (\mathbb{Q}^{+*}, .)$ tel que pour tout $x \in G$,

$$\sigma(x) = x^r.$$

En particulier, le groupe $\mathrm{Aut}(G, \leq, .)$ est un sous-groupe du centre de $\mathrm{Aut}(G, .)$. L'objectif de cette partie est d'appliquer le résultat de Glass et Ribenboim dans le cas des clôtures totalement réelles des corps de nombres ordonnables. Dans le paragraphe 3.1 on établit quelques propriétés de $\mathrm{Aut}(G, \leq, .)$ dans le cas où G est un groupe multiplicatif de $\overline{\mathbb{Q}}$ et $\leq$ représente l'ordre réel. Dans le paragraphe 3.2, on applique ces propriétés au cas de $G = \widetilde{K}_{\mathrm{tr}}^{+*}$ muni d'un ordre $\leq_1$ quelconque.

3.1. L'ordre réel

Proposition 5. *Soit K un sous-corps réel de $\overline{\mathbb{Q}}$ ordonné par l'ordre réel. Il existe une partie $\mathcal{P}_0 \subset \mathcal{P}$ ($\mathcal{P}$ désigne l'ensemble des nombres premiers) tel que*

$$\mathrm{Aut}(K^{+*}, \leq, .) = \langle \mathcal{P}_0 \rangle.$$

Réciproquement, pour tout $\mathcal{P}_0 \subset \mathcal{P}$, il existe un sous-corps réel de $\overline{\mathbb{Q}}$, K, tel que

$$\mathrm{Aut}(K^{+*}, \leq, .) = \langle \mathcal{P}_0 \rangle$$

Preuve. Pour la première partie de la proposition, il suffit de remarquer que si $p_1, \cdots, p_n$ sont n nombres pemiers distincts deux à deux et si $\alpha_1, \cdots, \alpha_n$ sont n entiers relatifs non nuls tels que $r = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$, alors

$$x \mapsto x^r \in \mathrm{Aut}(K^{+*}, \leq, .) \Longleftrightarrow x \mapsto x^{p_i} \in \mathrm{Aut}(K^{+*}, \leq, .) \text{ pour tout i.}$$

En effet si $r = \dfrac{s}{t}$ avec s et t deux nombres entiers premiers entre eux, alors d'après Bezout, il existe u et v tels que $us + vt = 1$ et donc $\dfrac{1}{t} = v + ur$. Soit $x \in G = K^{+*}$, comme x^v et x^u sont dans G, on a $x^{\frac{1}{t}} = x^v(x^u)^r \in G$, donc $x \mapsto x^t$ est un automorphisme de G et par suite, il en est de même de $x \mapsto x^s$. On peut donc supposer que tous les α_i sont négatifs. Pour tout $x \in G$, on a

$$x^{\frac{1}{p_i}} = x^{r(p_1^{-\alpha_1} \cdots p_i^{-\alpha_1 - 1} \cdots p_n^{-\alpha_n})} \in G$$

donc $x \mapsto x^{p_i}$ est un automorphisme de G.

Pour la deuxième partie de la proposition, prenons une partie non vide $\mathcal{P}_0 \subset \mathcal{P}$ et considérons la suite de corps $(K_n)_n$ définie par : $K_0 = \mathbb{Q}$ et si pour $n \geq 0$ on suppose avoir construit K_n, alors on définit K_{n+1} en prenant le corps engendré sur K_n par toute les racines p_i-ièmes réelles de tous les éléments positifs de K_n pour tous les $p_i \in \mathcal{P}_0$.

On pose $K = \bigcup\limits_n K_n$. Il est clair que pour tout $x \in K^{+*}$ et pour tout $p_i \in \mathcal{P}_0$, $\sqrt[p_i]{x} \in K^{+*}$. On a donc $< \mathcal{P}_0 > \subset \mathrm{Aut}(K^{+*}, \leq, .)$. Si l'inclusion était stricte, il existerait un nombre premier $p \notin \mathcal{P}_0$ tel que $x \mapsto x^p$ soit un automorphisme de K^{+*}. Donc $\sqrt[p]{2} \in K$, mais alors il existe une suite de premiers distincts deux à deux appartenant tous à $\mathcal{P}_0$ et une suite de réels $\omega_1, \cdots, \omega_n$ tels que $\omega_1 \in \mathbb{Q}$ et pour tout $i = i, \cdots, n-1$, $\omega_{i+1} \in \mathbb{Q}(\sqrt[p_1]{\omega_1}, \cdots, \sqrt[p_i]{\omega_i})$ et tel que $\sqrt[p]{2} \in \mathbb{Q}(\sqrt[p_1]{\omega_1}, \cdots, \sqrt[p_n]{\omega_n})$. Remarquons à présent que

$$\mathbb{Q}(\sqrt[p_1]{\omega_1}, \cdots, \sqrt[p_i]{\omega_i})/\mathbb{Q}(\sqrt[p_1]{\omega_1}, \cdots, \sqrt[p_{i-1}]{\omega_{i-1}})$$

est soit de degré 1 (alors $\sqrt[p_i]{\omega_i} \in \mathbb{Q}(\sqrt[p_1]{\omega_1}, \cdots, \sqrt[p_{i-1}]{\omega_{i-1}})$) soit de degré p_i (alors $\sqrt[p_i]{\omega_i} \notin \mathbb{Q}(\sqrt[p_1]{\omega_1}, \cdots, \sqrt[p_{i-1}]{\omega_{i-1}})$). Cette propriété provient du fait que le polynôme $X^p - a$ ($a \in K$) est irreductible sur K si et seulement si K ne contient aucune racine de $X^p - a$ (voir [L], VIII.9). Comme les corps considérés ici sont réels, si $\mathbb{Q}(\sqrt[p_1]{\omega_1}, \cdots, \sqrt[p_{i-1}]{\omega_{i-1}})$ contient une racine de $X^{p_i} - \omega_i$ alors celle-ci est obligatoirement $\sqrt[p_i]{\omega_i}$.

Donc $\mathbb{Q}(\sqrt[p_1]{\omega_1}, \cdots, \sqrt[p_n]{\omega_n})/\mathbb{Q}$ a pour degré d un produit des p_i. Mais le degré de $\sqrt[p]{2}$ sur $\mathbb{Q}$ est p, qui ne peut pas diviser d par hypothèse. Ceci contredit le fait que $\sqrt[p]{2} \in \mathbb{Q}(\sqrt[p_1]{\omega_1}, \cdots, \sqrt[p_n]{\omega_n})$. □

3.2. Le groupe $\mathrm{Aut}(\widetilde{K}_{\mathrm{tr}}^{+*}, \leq_1, .)$

Si K désigne un corps ordonnable et $\leq_1$ un ordre compatible sur K, on notera K^{+*} l'ensemble des éléments strictement positifs de K pour $\leq_1$ et $\mathrm{Aut}(K^{+*}, \leq_1, .)$ le groupe des automorphismes de K^{+*} préservant l'ordre $\leq_1$.

Proposition 6. *Soit K un corps de nombres ordonnable et $\leq_1$ un ordre sur $\widetilde{K}_{\mathrm{tr}}$. On a*

$$\mathrm{Aut}(\widetilde{K}_{\mathrm{tr}}^{+*}, \leq_1, .) = 1.$$

Preuve. Commencons par montrer que $\mathrm{Aut}(K^{+*}, \leq_1, .) = 1$ où $\leq_1$ désigne un ordre quelconque sur K.

Puisque $\mathbb{Q}$ ne possède qu'un seul ordre compatible, si R_1 et R_2 sont deux corps réel clos dans $\overline{\mathbb{Q}}$, alors il sont isomorphes. Prenons alors R une extension ordonnée algébrique maximale de K (l'ordre de R prolonge $\leq_1$). Comme R est réel clos, il existe donc un isomorphisme σ entre R et $\overline{\mathbb{Q}} \cap \mathbb{R}$. Maintenant un isomorphisme de corps ordonné, transfert l'ordre du corps de départ sur un ordre du corps d'arrivée. Comme $\mathbb{R}$ est uniquement ordonnable, on en déduit que l'ordre transféré à $\sigma(K)$ par $\leq_1$ est l'ordre induit par $\mathbb{R}$ sur $\sigma(K)$. Si on prouve que $\mathrm{Aut}(\sigma(K)^{+*}, \leq, .) = 1$ (ici $\leq$ désigne l'ordre induit par $\mathbb{R}$), alors si $\tau \in \mathrm{Aut}(K^{+*}, \leq_1, .)$, on a $\sigma \circ \tau \circ \sigma^{-1} \in \mathrm{Aut}(\sigma(K)^{+*}, \leq, .) = 1$ et par conséquent, $\tau = 1$. En conséquence de quoi, pour montrer notre proposition, on peut supposer que $K \subset \mathbb{R}$ et que $\leq_1$ est l'ordre $\leq$ induit par $\mathbb{R}$ sur K.

Dans ces conditions, supposons qu'il existe un nombre premier p tel que $x \mapsto x^p$ soit un automorphisme de K^{+*}. Considérons la famille infinie de polynômes $(X^p - q)_{q \text{ premier}}$. Comme K est un corps de nombres, il n'y a qu'un nombre fini de ces polynômes qui ne soient pas irréductibles sur K. Prenons alors un nombre premier q_0 tel que $(X^p - q_0)$ soit irréductible sur K. On a donc $\sqrt[p]{q_0} \notin K$ ce qui est en contradiction avec le fait que $x \mapsto x^p$ soit un automorphisme de K^{+*}.

Soit maintenant $\leq_1$ un ordre sur $\widetilde{K}_{\mathrm{tr}}$ et R une extension algébrique ordonnée maximale de $\widetilde{K}_{\mathrm{tr}}$ dont l'ordre prolonge $\leq_1$. Soit σ un isomorphisme entre R et $\overline{\mathbb{Q}} \cap \mathbb{R}$. Posons $K_1 = \sigma(K)$ et $L = \sigma(\widetilde{K}_{\mathrm{tr}})$. Notons que comme précédement, l'ordre transféré par σ est l'ordre induit par $\mathbb{R}$ sur K_1 et L. Maintenant, si T désigne un corps réel clos (inclus dans $\overline{\mathbb{Q}}$) contenant K, alors $\sigma(T)$ est un corps réel clos contenant K_1. Réciproquement, tout corps réel clos T' contenant K_1 a pour image par σ^{-1} un corps réel clos contenant K. L'isomorphisme σ définit donc une bijection entre les corps réels clos contenant K et ceux contenant K_1. Maintenant, comme σ est bijectif, on a

$$\sigma(\widetilde{K}_{\mathrm{tr}}) = \sigma\Big(\bigcap_{K \subset R} R\Big) = \bigcap_{K \subset R} \sigma(R) = \bigcap_{K_1 \subset R} R = \widetilde{K}_{1\mathrm{tr}}.$$

(R parcourt l'ensemble des corps réel clos de $\overline{\mathbb{Q}}$.)

Comme précédement, σ transfert l'ordre $\leq_1$ de $\widetilde{K}_{\mathrm{tr}}$ sur l'ordre induit par $\mathbb{R}$ sur $\widetilde{K}_{1\,\mathrm{tr}}$. On peut donc supposer sans perte de généralité que $\widetilde{K}_{\mathrm{tr}} \subset \mathbb{R}$ et $\leq_1 = \leq$. $\square$

Pour montrer notre proposition, il suffit alors de prouver le résultat suivant :

Lemme. *Soit L/K une extension galoisienne telle que $L \subset \overline{\mathbb{Q}} \cap \mathbb{R}$, si* $\mathrm{Aut}(K^{+*}, \leq, .) = 1$ *alors* $\mathrm{Aut}(L^{+*}, \leq, .) = 1$.

Preuve. Supposons $\mathrm{Aut}(K^{+*}, \leq, .) = 1$ et qu'il existe un premier p tel que $x \mapsto x^p \in \mathrm{Aut}(L^{+*}, \leq, .)$. Par hypothèse, il existe $\alpha \in K^{+*}$ tel que $\sqrt[p]{\alpha} \notin K$. Le polynôme $X^p - \alpha$ est donc irréductible sur K et comme L/K est galoisienne, $X^p - \alpha$ est totalement décomposé sur L puisque $\sqrt[p]{\alpha} \in L$. Par suite, les racines p-ième de l'unité sont dans L. Mais comme L est réel, on a nécessairement $p = 2$.

Maintenant, $X^4 - \alpha$ est irréductible sur K (car $\sqrt{\alpha} \notin K$ et comme $\alpha > 0$, $\alpha \notin -4K^4$, voir alors [L], VIII.9). Comme $\sqrt{\sqrt{\alpha}} \in L$, $X^4 - \alpha$ est totalement décomposé sur L, donc $\sqrt{-1} \in L$ ce qui est absurde. $\square$

Bibliographie

[B] Blanchard, A.: *Les corps non commutatifs*. Collection Sup, PUF, (1972)

[DD] Dèbes, P. and Deschamps, B.: The Inverse Galois Problem over Large Fields. In: *Geometric Galois action II*. London Math. Soc. Lecture Note Series, Cambridge: Cambridge Univ. Press, P. Lochak and L. Schneps (eds.), **243**, 1997, pp. 119-138

[EH] Efrat, I. and Haran, D.: On Galois groups over pythagorean and semi-real closed fields. Israel J. Math. **85**, 57–78 (1994)

[FJ] Fried, M. and Jarden, M.: *Field Arithmetic*. Berlin–Heidelberg–New York: Springer-Verlag, 1985

[FV] Fried, M and Völklein, H.: The embedding problem over a Hilbertian PAC-field. Annals Math. **135**, 469–481 (1992)

[GR] Glass, A.M.W. and Ribenboim, Paulo.: Automorphisms of the ordered multiplicative group of positive rational numbers. Proceedings of the A.M.S, **122**, 15–18 (1994)

[L] Lang, S.: *Algebra*. Reading, MA: Addison Wesley, **4177**, 1967

[P] Pop, F.: Embedding problems over large field. Annals Math. **144**, 1–35 (1996)

[R] Ribenboim, P.: *Arithmétique des corps*. Paris: Hermann, 1973

[Sc] Scheiderer, K.: *Real and etale cohomology*. Lecture notes in Mathematics, Berlin–Heidelberg–New York: Springer-Verlag, **1588**

[S1] Serre, J.-P.: *Corps locaux*. Paris: Hermann, 1968

[S2] Serre, J.-P.: Cohomologie galoisienne. Lecture notes in Mathematics, Berlin–Heidelberg–New York: Springer-Verlag, 1962