JOURNAL de Théorie des Nombres de BORDEAUX

*anciennement Séminaire de Théorie des Nombres de Bordeaux*

Bruno DESCHAMPS

**Sur le groupe unitaire relatif à une involution d'un corps algébriquement clos**

Tome 23, n° 3 (2011), p. 629-644.

<http://jtnb.cedram.org/item?id=JTNB_2011__23_3_629_0>

*Journal de Théorie des Nombres*
*de Bordeaux* **23** (2011), 629-644

# Sur le groupe unitaire relatif à une involution d'un corps algébriquement clos

par Bruno DESCHAMPS

Résumé. Dans cet article, nous tentons de généraliser à d'autres situations l'isomorphisme de groupes topologiques qui existe entre le groupe $\mathbb{R}/\mathbb{Z}$ et le groupe unitaire $\mathbb{U} = \{z \in \mathbb{C}/\ |z| = 1\}$.

Nous montrons que cet isomorphisme existe algébriquement en toute généralité : pour tout corps algébriquement clos $C$ et toute involution $c$ de $C$ les groupes $\mathbb{U}(C,c) = \{z \in C/\ zc(z) = 1\}$ et $C^{<c>}/\mathbb{Z}$ sont isomorphes. Nous donnons ensuite un exemple d'involution $c_0$ de $\mathbb{C}$ qui n'est pas conjuguée, dans le groupe $\mathrm{Aut}(\mathbb{C})$, à la conjugaison complexe et telle que $\mathbb{U}(\mathbb{C}, c_0)$ soit topologiquement isomorphe à $\mathbb{C}^{<c_0>}/\mathbb{Z}$.

Abstract. *On the unitary group associated to an involution of an algebraically closed field.*

In this article, we try to see if the topological isomorphism that exists between the group $\mathbb{R}/\mathbb{Z}$ and the unitary group $\mathbb{U} = \{z \in \mathbb{C}/\ |z| = 1\}$ can be generalized to some other situations.

We show that this isomorphism exists algebraically in all situations : for a given algebraically closed field $C$ and a given involution $c$ of $C$, the groups $\mathbb{U}(C,c) = \{z \in C/\ zc(z) = 1\}$ and $C^{<c>}/\mathbb{Z}$ are isomorphic. We then give an example of an involution $c_0$ of $\mathbb{C}$ which is not conjugated, in the group $\mathrm{Aut}(\mathbb{C})$, to the complex conjugacy and such that $\mathbb{U}(\mathbb{C}, c_0)$ is isomorphic as a topological group to $\mathbb{C}^{<c_0>}/\mathbb{Z}$.

## 1. Introduction

L'application $x \longmapsto e^{ix}$ définit un épimorphisme continu du groupe additif des réels $\mathbb{R}$ sur le groupe unitaire $\mathbb{U} = \{z \in \mathbb{C}/\ |z| = 1\}$. Par passage au quotient, on en déduit l'existence d'un isomorphisme de groupes topologiques entre $\mathbb{U}$ et $\mathbb{R}/\mathbb{Z}$. Dans cet article on s'intéresse à comprendre si ce résultat perdure dans un cadre plus général.

Pour ce faire, on regarde le corps des nombres réels $\mathbb{R}$ comme corps des invariants du corps des nombres complexes $\mathbb{C}$ sous l'action de la conjugaison complexe $c$. Le groupe $\mathbb{U}$ représente alors le groupe des éléments de norme

Manuscrit reçu le 31 mai 2010.
*Classification math.* 12E30, 12F10, 12J15.

1 de l'extension $\mathbb{C}/\mathbb{R}$. Etant donné une extension finie $L/K$, déterminer la nature algébrique du groupe des éléments de $L$ de norme 1 est une question très délicate en toute généralité. Notre généralisation portera sur le cas où le corps $L$ est algébriquement clos. A ce sujet, faisons un bref rappel sur les corps réel clos.

Un corps réel clos est un corps ordonné qui ne possède pas d'extension algébrique ordonnée stricte. La théorie d'Artin-Schreier assure alors qu'un corps $R$ est réel clos si et seulement si $R \neq \overline{R}$ et $\overline{R} = R(\sqrt{-1})$. Réciproquement, un corps $R$ tel que $1 < [\overline{R} : R] < +\infty$ est un corps réel clos et on a donc forcément $\mathrm{car}(R) = 0$ et $[\overline{R} : R] = 2$. Une conséquence de ces résultats est qu'un automorphisme d'un corps algébriquement clos qui est d'ordre fini est nécéssairement une involution. (Pour les propriétés arithmétiques relatives aux corps réels clos que nous utiliserons dans ce texte, nous renvoyons le lecteur à [1] et [7].)

On se fixe donc un corps algébriquement clos $C$ (de caractéristique 0), une involution $c$ de ce corps et l'on pose $\mathfrak{R}(C, c) = C^{<c>}$ le sous-corps réel clos de $C$ associé à $c$. On considère alors le *groupe unitaire de $C$ relativement à $c$*

$$\mathbb{U}(C, c) = \{z \in C/\ zc(z) = 1\}$$

qui est donc le groupe des éléments de norme 1 de l'extension $C/R$ où $R = \mathfrak{R}(C, c)$. La question est de comprendre le lien éventuel qui existe entre le groupe multiplicatif $(\mathbb{U}(C, c), .)$ et le groupe additif $(R, +)$. On peut se demander, dans le cas général, si l'on dispose d'un isomorphisme de groupes abstraits

$$\mathbb{U}(C, c) \underset{\text{alg}}{\simeq} R/\mathbb{Z}$$

La présence du facteur $\mathbb{Z}$ est bien sûr inspirée par le cas particulier $R = \mathbb{R}$, mais il convient de remarquer qu'en toute généralité, il ne peut exister d'isomorphisme entre $R$ et $\mathbb{U}(C, c)$. En effet, si l'on considère une racine $n$-ième de l'unité, $\xi \in C$, alors on a

$$1 = 1.c(1) = \xi^n c(\xi^n) = (\xi c(\xi))^n$$

et donc $\xi' = \xi c(\xi)$ est aussi une racine $n$-ième de l'unité dans $R$. C'est un élément positif de $R$, car en tant que norme elle est la somme de deux carrés d'éléments de $R$. Si $\xi' < 1$ (ou $\xi' > 1$) alors $1 = \xi'^n < 1$ (ou $1 = \xi'^n > 1$), ce qui est absurde, donc $\xi' = 1$ et $\xi \in \mathbb{U}(C, c)$. On en déduit que $\mathbb{U}(C, c)$ est un groupe qui contient l'ensemble $\mu_\infty$ des racines de l'unité (qui forme un sous-groupe isomorphe à $\mathbb{Q}/\mathbb{Z}$) et donc possède de la torsion au contraire du groupe additif $R$. Ainsi, se poser la question de l'existence d'un isomorphisme $\mathbb{U}(C, c) \underset{\text{alg}}{\simeq} R/\mathbb{Z}$ revient, de ce point de vue, à se poser la question de l'existence d'un épimorphisme $R \longrightarrow \mathbb{U}(C, c)$ à noyau minimal (i.e. de rang 1).

La question de la nature de ce noyau n'a pas d'influence sur la structure algébrique du quotient $R/\mathbb{Z}$. En effet, $R$ étant un corps, si $A =< \alpha >$ et $B =< \beta >$ désignent deux sous-groupes monogènes non triviaux de $R$, alors l'automorphisme de groupe additif de $R$, $x \longmapsto \frac{\beta}{\alpha}x$, induit un isomorphisme entre $A$ et $B$ qui assure, par passage au quotient, que les groupes $R/A$ et $R/B$ sont isomorphes.

La connaissance du groupe abstrait $\mathbb{U}(C,c)$ permet de déduire celle de $(C^*,.)$ puisque l'on a l'isomorphisme

$$C^* \simeq \mathbb{U}(C,c) \times R^{+*}$$

où $R^{+*}$ désigne le groupe multiplicatif des éléments strictement positifs du corps $R$. En effet, pour tout $z \in C^*$, on a $zc(z) \in R^{+*}$ et alors l'application

$$z \longmapsto \left( \frac{z}{\sqrt{zc(z)}}, \sqrt{zc(z)} \right)$$

fournit un isomorphisme entre $C^*$ et $\mathbb{U}(C,c) \times R^{+*}$.

A corps algébriquement clos fixé $C$, il existe une correspondance biunivoque entre les classes de conjugaison d'involutions de $C$ dans le groupe $\mathrm{Aut}(C)$ et les classes d'isomorphisme de sous-corps réels clos de $C$. Si $c, c^{'}$ désignent deux involutions de $C$ et $\sigma \in \mathrm{Aut}(C)$, on a

$$c^{'} = \sigma \circ c \circ \sigma^{-1} \Longleftrightarrow \sigma(\mathfrak{R}(C,c)) = \mathfrak{R}(C,c^{'})$$

Ainsi, l'existence d'un isomorphisme $\mathbb{U}(C,c) \underset{\text{alg}}{\simeq} \mathfrak{R}(C,c)/\mathbb{Z}$ est une question qui ne dépend pas du représentant de la classe de conjugaison de $c$ dans $\mathrm{Aut}(C)$.

Dans ce texte, nous montrons qu'en toute généralité, il existe un isomorphisme $\mathbb{U}(C,c) \underset{\text{alg}}{\simeq} \mathfrak{R}(C,c)/\mathbb{Z}$ pour tout corps algébriquement clos $C$ de caractéristique 0 et toute involution $c$. Ce résultat est l'objet du théorème 2.1 auquel le paragraphe 2 de ce texte est consacré.

Les éléments positifs d'un corps réel clos $R$ étant les carrés, il s'ensuit qu'un tel corps possède un unique ordre compatible $\leq$. Cet ordre permet de définir une topologie sur $R$ en prenant comme base d'ouverts les intervalles ouverts

$$]x,y[= \{z \in R/\ x < z < y\}$$

Si $C$ désigne la cloture algébrique de $R$ et $c$ l'involution de $\mathrm{Gal}(C/R)$, on peut alors définir sur $C$ une *pseudo-distance*

$$d : C \times C \longrightarrow R^+$$

de la manière suivante : les normes d'éléments de $C$ étant des éléments positifs de $R$, ils possèdent chacun une unique racine carrée positive. Si $\lambda, \mu \in C$, on pose alors

$$d(\lambda,\mu) = \sqrt{(\lambda-\mu)c(\lambda-\mu)}$$

Cette pseudo-distance vérifie les axiomes définissant une distance à la différence près qu'il s'agit là d'une application qui n'est pas à valeurs réelles. Si $\lambda \in C$ et $\varepsilon \in R^{+*}$, on définit la pseudo-boule de centre $\lambda$ et de rayon $\varepsilon$ comme étant l'ensemble

$$B(\lambda, \varepsilon) = \{\mu \in C/\ d(\lambda, \mu) < \varepsilon\}$$

La topologie que l'on considère sur $C$ est la topologie engendrée par les pseudo-boules. Exactement comme dans le cas de $\mathbb{R}$ et $\mathbb{C}$ munis des distances usuelles, on voit que $C$ muni de la topologie des pseudo-boules est un espace homéomorphe à l'espace topologique produit $R \times R$ où $R$ est muni de la topologie de l'ordre.

S'il existe des isomorphismes algébriques $\mathbb{U}(C,c) \underset{\text{alg}}{\simeq} R/\mathbb{Z}$ on peut se demander si, parmi eux, il en existe un qui soit aussi topologique (une fois que l'on munit les groupes $\mathbb{U}(C,c)$ et $R$ des topologies précédemment décrites). Si c'est le cas on notera alors

$$\mathbb{U}(C,c) \underset{\text{top}}{\simeq} R/\mathbb{Z}$$

On remarquera que l'existence d'un tel isomorphisme de groupes topologiques est plus forte que la simple existence d'un épimorphisme continu $R \longrightarrow \mathbb{U}(C,c)$ de noyau $\mathbb{Z}$. Dans le cas où $C = \mathbb{C}$ et $c$ est la conjugaison complexe, la continuité de $x \longmapsto e^{ix}$ induit bien par passage au quotient un isomorphisme $\mathbb{U} \underset{\text{top}}{\simeq} \mathbb{R}/\mathbb{Z}$, mais ceci vient du fait que $\mathbb{R}/\mathbb{Z}$ et $\mathbb{U}$ sont des groupes compacts et cette dernière propriété n'est pas vraie dans le cas général.

Dans le paragraphe 3, nous donnons un exemple d'involution, $c_0$ de $\mathbb{C}$, qui n'est pas conjuguée à la conjugaison complexe et pour laquelle on a $\mathbb{U}(\mathbb{C}, c_0) \underset{\text{top}}{\simeq} \mathfrak{R}(\mathbb{C}, c_0)/\mathbb{Z}$ (théorème 3.1). Pour ce faire, on établit un résultat assez général sur les corps de séries de Puiseux (théorème 3.2), qui assure que

$$\mathbb{U}(C,c) \underset{\text{alg}}{\simeq} R/\mathbb{Z} \Longrightarrow \mathbb{U}(\text{Puis}(C), \tilde{c}) \underset{\text{top}}{\simeq} \text{Puis}(R)/\mathbb{Z}$$

Nous adressons nos remerciements à Nour Ghazi et Ivan Suarez Atias pour les commentaires et remarques qu'ils nous ont fait lors de la lecture de la version préliminaire de ce texte.

## 2. Le cas algébrique

Ce paragraphe est consacré à la démonstration du théorème suivant :

**Théorème 2.1.** *Si $\overline{K}$ est un corps algébriquement clos de caractéristique 0 et $c \in \text{Aut}(\overline{K})$ est une involution alors*

$$\mathbb{U}(\overline{K}, c) \underset{alg}{\simeq} \mathfrak{R}(\overline{K}, c)/\mathbb{Z}$$

*Démonstration.* La preuve de ce théorème va reposer sur le fait que les groupes que l'on étudie sont abéliens et divisibles. A ce sujet rappelons le très puissant théorème de classification de ces groupes (voir [5], [6]) :

**Théorème 2.2.** *Si $G$ désigne un groupe abélien et divisible alors*

$$G \simeq \bigoplus_{\alpha} \mathbb{Q} \oplus \bigoplus_{p} \bigoplus_{m(p)} C_{p^\infty}$$

*où $\alpha$ et $m(p)$ sont des cardinaux ($p$ parcourant l'ensemble des nombres premiers) et où $C_{p^\infty} = \varinjlim \mathbb{Z}/p^n\mathbb{Z}$ désigne le $p$-groupe de Prüfer. En particulier, si $\mathrm{Tors}(G)$ désigne le sous-groupe de torsion de $G$, alors*

$$G = G/\mathrm{Tors}(G) \oplus \mathrm{Tors}(G)$$

*et $G/\mathrm{Tors}(G)$ est un $\mathbb{Q}$-espace vectoriel.*

Fixons maintenant un corps $\overline{K}$ algébriquement clos de caractéristique 0 et une involution $c$ de $\overline{K}$.

**Lemme 2.1.** *a)* $\mathrm{Tors}(\mathfrak{R}(\overline{K},c)/\mathbb{Z}) = \mathbb{Q}/\mathbb{Z} \simeq \mu_\infty = \mathrm{Tors}(\mathbb{U}(\overline{K},c))$.

*b) Les groupes $\mathbb{U}(\overline{K},c)$ et $\mathfrak{R}(\overline{K},c)/\mathbb{Z}$ sont abéliens et divisibles.*

*c)* $\sharp\mathbb{U}(\overline{K},c) = \sharp\mathfrak{R}(\overline{K},c) = \sharp\overline{K}$.

*Démonstration.* a) Est immédiat, compte-tenu du fait que l'on a $\mu_\infty \subset \mathbb{U}(\overline{K},c)$ (voir introduction).

b) Le groupe $\mathfrak{R}(\overline{K},c)/\mathbb{Z}$ est visiblement divisible, puisque $\mathfrak{R}(\overline{K},c)$ l'est. Prenons un élément $z \in \mathbb{U}(\overline{K},c)$, un entier $n \geq 2$ et considérons $\sqrt[n]{z}$ une racine $n$-ème de $z$ dans $\overline{K}$. On a

$$\left(\sqrt[n]{z}c(\sqrt[n]{z})\right)^n = zc(z) = 1$$

et donc $\sqrt[n]{z}c(\sqrt[n]{z}) \in \mu_n$. Mais comme $\sqrt[n]{z}c(\sqrt[n]{z})$ est un élément positif de $\mathfrak{R}(\overline{K},c)$ on en déduit, comme dans l'introduction, que $\sqrt[n]{z}c(\sqrt[n]{z}) = 1$, c'est-à-dire que $\sqrt[n]{z} \in \mathbb{U}(\overline{K},c)$. Ceci prouve finalement que $\mathbb{U}(\overline{K},c)$ est un groupe divisible.

c) On note $i = \sqrt{-1} \in \overline{K}$. On rappelle que $\overline{K} = \mathfrak{R}(\overline{K},c) \oplus i\mathfrak{R}(\overline{K},c)$. Soit $z = a + ib \in \overline{K}$ (avec $a, b \in \mathfrak{R}(\overline{K},c)$), alors $z \in \mathbb{U}(\overline{K},c)$ si et seulement si $a^2 + b^2 = 1$. Les éléments positifs de $\mathfrak{R}(\overline{K},c)$ étant les carrés, il existe donc une bijection entre $\mathbb{U}(\overline{K},c)$ et $\{\pm 1\} \times [-1,1]$ donnée par

$$(\varepsilon, a) \in \{\pm 1\} \times [-1,1] \longmapsto a + \varepsilon i\sqrt{1-a^2}$$

Maintenant, l'application $x \mapsto 1/x$ induit une bijection de $[-1,1]/\{0\}$ sur $]-\infty,-1] \cup [1,+\infty[$ et on en déduit que les ensembles infinis $\mathbb{U}(\overline{K},c)$, $\mathfrak{R}(\overline{K},c)$ et $[-1,1]$ ont même cardinal. L'équipotence entre $\mathfrak{R}(\overline{K},c)$ et $\overline{K}$ découle elle du fait que $[\overline{K} : \mathfrak{R}(\overline{K},c)] = 2$. □

Les groupes $\mathbb{U}(\overline{K},c)$ et $\mathfrak{R}(\overline{K},c)/\mathbb{Z}$ ont donc même groupe de torsion. Pour montrer qu'ils sont isomorphes il suffit donc, en vertu du théorème de classification des groupes abéliens divisibles rappelé plus haut, de vérifier que leurs quotients par leurs torsions respectives sont isomorphes. Puisque ces quotients, $\mathbb{U}(\overline{K},c)/\mu_\infty$ et $\mathfrak{R}(\overline{K},c)/\mathbb{Q}$, sont des $\mathbb{Q}$-espaces vectoriels, il suffit de vérifier qu'ils ont même dimension. Le c) du lemme 2.1 assure par un argument immédiat de cardinalité que ces quotients ont le même cardinal, égal à $\sharp\overline{K}$. La suite de la preuve va distinguer deux cas, suivant que $\sharp\overline{K}$ est dénombrable ou non.

**Cas où $\sharp\overline{K} > \aleph_0$ :** On rappelle que *si $E$ est un $\mathbb{Q}$-espace vectoriel de dimension infinie, alors on a $\sharp E = \dim E$.* Les $\mathbb{Q}$-espaces vectoriels $\mathbb{U}(\overline{K},c)/\mu_\infty$ et $\mathfrak{R}(\overline{K},c)/\mathbb{Q}$ étant indénombrables, ils sont de dimension infinie, et ayant le même cardinal, ils sont donc isomorphes.

**Cas où $\sharp\overline{K} = \aleph_0$ :** Dans cette situation $\mathbb{U}(\overline{K},c)/\mu_\infty$ et $\mathfrak{R}(\overline{K},c)/\mathbb{Q}$ sont dénombrables et donc de dimensions finies ou dénombrables. La dimension de $\mathfrak{R}(\overline{K},c)/\mathbb{Q}$ en tant que $\mathbb{Q}$-espace vectoriel est certainement infinie, puisque par exemple la famille $\{\sqrt{2},\sqrt{3},\cdots,\sqrt{p},\cdots\} \subset \mathfrak{R}(\overline{K},c)$ constitue une famille libre infinie (un argument pour montrer que $\sqrt{p} \in \mathfrak{R}(\overline{K},c)$ est donné dans le lemme 2.5 à venir). Pour conclure, il suffit donc de montrer que $\mathbb{U}(\overline{K},c)/\mu_\infty$, en tant que $\mathbb{Q}$-espace vectoriel, n'est pas de dimension finie.

Raisonnons par l'absurde et supposons que $\mathbb{U}(\overline{K},c)/\mu_\infty$ soit de dimension finie $n \geq 1$ sur $\mathbb{Q}$. Soit $z_1,\cdots,z_{n+1}$ des éléments de $\mathbb{U}(\overline{K},c)$ et $\overline{z_1},\cdots,\overline{z_{n+1}}$ leurs images dans $\mathbb{U}(\overline{K},c)/\mu_\infty$. Par hypothèse, la famille $\{\overline{z_1},\cdots,\overline{z_{n+1}}\}$ comptant $n+1$ éléments, est $\mathbb{Q}$-liée et il existe donc une équation de dépendance $\mathbb{Z}$-linéaire pour cette famille, ce qui implique qu'il existe des entiers relatif $a_1,\cdots,a_{n+1}$ non tous nul tels que $z_1^{a_1}.\cdots.z_{n+1}^{a_{n+1}} \in \mu_\infty$. En élevant à une puissance entière adéquate, on en déduit donc que : pour tous $z_1,\cdots,z_{n+1} \in \mathbb{U}(\overline{K},c)$, il existe des entiers relatifs $s_1,\cdots,s_{n+1}$ non tous nuls tels que

$$z_1^{s_1}.\cdots.z_{n+1}^{s_{n+1}} = 1$$

Pour déduire de ce résultat une absurdité, nous allons préalablement établir quelques propriétés arithmétiques relatives aux extensions quadratiques de $\mathbb{Q}$.

**Lemme 2.2.** *Soit $m \geq 1$ et $d_1,\cdots,d_{m+1} \in \mathbb{Z}$ des entiers tels qu'il existe $m+1$ nombres premiers $p_1,\cdots p_{m+1}$ vérifiant que pour tout $i = 1,\cdots,m+1$, $v_{p_i}(d_i) \notin 2\mathbb{Z}$ et pour $j \neq i$, $v_{p_i}(d_j) \in 2\mathbb{Z}$.*

*Les extensions $\mathbb{Q}(\sqrt{d_1},\cdots,\sqrt{d_m})$ et $\mathbb{Q}(\sqrt{d_{m+1}})$ sont linéairement disjointes sur $\mathbb{Q}$. En particulier l'extension galoisienne $\mathbb{Q}(\sqrt{d_1},\cdots,\sqrt{d_{m+1}})/\mathbb{Q}$ est de groupe de Galois $(\mathbb{Z}/2)^{m+1}$.*

*Démonstration.* Commençons par remarquer que, sous les hypothèses du lemme, l'entier $d_i$ n'est pas un carré et donc que l'extension $\mathbb{Q}(\sqrt{d_i})$ est bien quadratique. Nous montrerons le lemme par récurrence sur l'entier $m$.

• Pour $m = 1$, il faut montrer que $\sqrt{d_2} \notin \mathbb{Q}(\sqrt{d_1})$. Raisonnons par l'absurde et supposons qu'il existe $a, b \in \mathbb{Q}$ tels que $\sqrt{d_2} = a + b\sqrt{d_1}$. On a alors, en élevant au carré,

$$2ab\sqrt{d_1} = d_2 - a - d_1 b^2 \in \mathbb{Q}$$

et donc $ab = 0$. L'hypothèse $b = 0$ est exclue, car sinon on aurait $\sqrt{d_2} \in \mathbb{Q}$. On a donc $a = 0$ et ainsi $\sqrt{\frac{d_1}{d_2}} \in \mathbb{Q}$, c'est-à-dire que $\frac{d_1}{d_2}$ est un carré dans $\mathbb{Q}$, ce qui est impossible puisque $v_{p_1}(\frac{d_1}{d_2})$ est impair.

Les corps $\mathbb{Q}(\sqrt{d_1})$ et $\mathbb{Q}(\sqrt{d_2})$ sont donc des extensions linéairement disjointes de $\mathbb{Q}$ de groupe de Galois respectif $\mathbb{Z}/2\mathbb{Z}$. On en déduit que le groupe de Galois du compositum, $\mathrm{Gal}(\mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})/\mathbb{Q})$, vaut $(\mathbb{Z}/2\mathbb{Z})^2$.

• Supposons la propriété vraie pour un entier $m - 1 \geq 1$ et considérons $d_1, \cdots, d_{m+1}$ des entiers vérifiant les hypothèses du lemme. L'extension galoisienne $\mathbb{Q}(\sqrt{d_1}, \cdots, \sqrt{d_m})/\mathbb{Q}$ est de groupe $(\mathbb{Z}/2)^m$. Si $H$ désigne un sous-groupe de $(\mathbb{Z}/2)^m$ d'indice 2, en tant que $\mathbb{F}_2$-espace vectoriel il s'agit d'un hyperplan et donc du noyau d'une forme linéaire. Comme nous travaillons sur $\mathbb{F}_2$, les questions de proportionalité ne se posent pas et il y a donc une bijection entre les hyperplans et les polynômes linéaires $a_1X_1 + \cdots + a_mX_m$ non triviaux. On en déduit qu'il existe exactement $2^m - 1$ sous-groupes d'indices 2 dans $(\mathbb{Z}/2)^m$.

La théorie de Galois assure alors qu'il existe exactement $2^m - 1$ sous-extensions quadratiques. Ces extensions sont exactement les extensions $\mathbb{Q}(\omega)/\mathbb{Q}$ où $\omega$ désigne le produit des entiers d'une partie non vide de $\{d_1, \cdots, d_m\}$ (on vérifie sans peine, comme dans le cas $m = 1$, que ces extensions sont distinctes deux à deux).

Dire que $\mathbb{Q}(\sqrt{d_1}, \cdots, \sqrt{d_m})$ et $\mathbb{Q}(\sqrt{d_{m+1}})$ sont linéairement disjointes sur $\mathbb{Q}$ équivaut à dire que le corps $\mathbb{Q}(\sqrt{d_{m+1}})$ n'est pas un sous-corps de $\mathbb{Q}(\sqrt{d_1}, \cdots, \sqrt{d_m})$. Si tel était le cas, ce serait une extension quadratique et donc, d'après ce qui précède, il existerait $\omega$ le produit des entiers d'une partie non vide de $\{d_1, \cdots, d_m\}$ tel que $\mathbb{Q}(\sqrt{d_{m+1}}) = \mathbb{Q}(\omega)$. Le même argument que dans le cas $m = 1$ conduit alors à une absurdité. □

Considérons maintenant, pour un entier $k \geq 2$ donné, l'élément

$$\alpha_k = \frac{1 + i\sqrt{k^2 - 1}}{k}$$

Son polynôme minimal sur $\mathbb{Q}$ est $X^2 - \frac{2}{k}X + 1$. On a

**Lemme 2.3.** *Pour tout $k \geq 3$ et tout entier relatif $h$ tel que $|h| \geq 1$, on a*

$$\mathbb{Q}(\alpha_k^h) = \mathbb{Q}(\alpha_k) = \mathbb{Q}(\sqrt{1 - k^2})$$

*Démonstration.* On peut visiblement se limiter, dans cette preuve, au cas $h \geq 1$. On a $\alpha_k^h = a_h + b_h\alpha_k$ avec $a_h, b_h \in \mathbb{Q}$ et il s'ensuit que

$$\begin{aligned}\mathbb{Q}(\alpha_k^h) \neq \mathbb{Q}(\alpha_k) &\iff b_h = 0 \iff \alpha_k^h \in \mathbb{Q} \iff \alpha_k^h = \pm 1 \text{ (car } |\alpha_k| = 1) \\ &\iff \alpha_k^{2h} = 1 \iff \left(X^2 - \tfrac{2}{k}X + 1\right) \text{ divise } (X^{2h} - 1)\end{aligned}$$

Ainsi, le polynôme irréductible $X^2 - 2/kX + 1 \in \mathbb{Q}[X]$ est un facteur premier du polynôme $X^{2h} - 1$ dont la décomposition, $X^{2h} - 1 = \prod_{i|2h} \Phi_i(X)$, ne possède que des facteurs unitaires à coefficients dans $\mathbb{Z}$. Comme, pour $k \geq 3$, $X^2 - \frac{2}{k}X + 1 \notin \mathbb{Z}[X]$, on en déduit bien que $\mathbb{Q}(\alpha_k^h) = \mathbb{Q}(\alpha_k)$. □

**Lemme 2.4.** *Il existe des entiers $k_1, \cdots, k_{n+1} \geq 3$ et $n+1$ nombres premiers $p_1, \cdots p_{n+1}$ tels que pour tout $i = 1, \cdots, n+1$, $v_{p_i}(1 - k_i^2) \notin 2\mathbb{Z}$ et pour $j \neq i$, $v_{p_i}(1 - k_j^2) \in 2\mathbb{Z}$.*

*Démonstration.* On pose $k_1 = 3$ et pour tout $i = 1, \cdots, n$, $k_{i+1} = (k_i^2 - 1)!$. On note $d_i = 1 - k_i^2$ et l'on remarque que si $i < j$ alors les entiers $d_i$ et $d_j$ sont premiers entre eux. En effet, si $p$ divise $d_i$, alors $p \leq |d_i| = k_i^2 - 1 \leq k_{j-1}^2 - 1$ (car la suite $(k_i)_i$ est visiblement croissante) et donc $p$ divise $k_j$ et ne peut donc diviser $d_j$.

Le dernier point à voir pour conclure est que $|d_i|$ n'est certainement pas un carré. Ceci est assuré par le fait que s'il existait $u \in \mathbb{Z}$ tel que $k_i^2 - u^2 = 1$ on aurait $(k_i - u)(k_i + u) = 1$ et donc $k_i = 0, 1$. □

**Lemme 2.5.** *Pour tout $k \geq 2$, on a $\alpha_k \in \mathbb{U}(\overline{K}, c)$.*

*Démonstration.* Pour tout $k \geq 2$, $k^2 - 1$ est un élément positif de $\mathbb{Q}$, donc de $\mathfrak{R}(\overline{K}, c)$, mais comme dans $\mathfrak{R}(\overline{K}, c)$ les éléments positifs sont les carrés, on en déduit que $\sqrt{k^2 - 1} \in \mathfrak{R}(\overline{K}, c)$. Un calcul immédiat montre alors que $\alpha_k c(\alpha_k) = 1$. □

On considère donc l'équation

$$z_1^{s_1} . \cdots . z_{n+1}^{s_{n+1}} = 1$$

où l'on a pris $z_j = \alpha_{k_j}$ pour $j = 1, \cdots, n+1$, où les $k_j$ sont les entiers trouvés dans le 2.4.

Un des $s_i$ est non nul, disons $s_{n+1}$. On a donc $\alpha_{k_{n+1}}^{-s_{n+1}} = \alpha_{k_1}^{s_1} . \cdots . \alpha_{k_n}^{s_n}$ et donc, d'après le lemme 2.3, on a $\mathbb{Q}(\alpha_{k_{n+1}}) = \mathbb{Q}(\alpha_{k_{n+1}}^{-s_{n+1}}) \subset \mathbb{Q}(\alpha_{k_1}, \cdots, \alpha_{k_n})$ ce qui constitue une absurdité aux vues des lemmes 2.2 et 2.4. □

## 3. Un cas topologique où l'involution n'est pas conjuguée à la conjugaison complexe

L'objet de cette partie est de montrer le théorème suivant

**Théorème 3.1.** *Il existe une involution $c_0$ de $\mathbb{C}$ qui n'est pas conjuguée, dans* $\mathrm{Aut}(\mathbb{C})$*, à la conjugaison complexe et telle que* $\mathbb{U}(\mathbb{C}, c_0) \underset{top}{\simeq} \mathfrak{R}(\mathbb{C}, c_0)/\mathbb{Z}$.

Pour ce faire, nous allons commencer par étudier quelques propriétés arithmétiques et topologiques des corps de séries de Puiseux.

Etant donné un corps $K$ quelconque, on note $K((X))$ le corps des séries de Laurent et l'on considère la valuation usuelle sur ce corps que l'on notera $v$. On note $K[[X]]$ l'anneau des séries entières (qui est l'anneau de la valuation $v$),

$$I_v(K) = XK[[X]]$$

l'idéal de la valuation $v$, et

$$1 + I_v(K) = \{S \in K[[X]] / \ S(0) = 1\}$$

le groupe des unités principales. Pour deux entiers $n|m$, on définit le morphisme $\varphi_{nm} : K((X_n)) \longrightarrow K((X_m))$ obtenu en posant $\varphi_{nm}(X_n) = X_m^k$ où $k = m/n$. Le système considéré pour tous les couples d'entiers $n|m$ est inductif et, par définition, le corps des séries de Puiseux à coefficients dans $K$ est le corps obtenu en prenant la limite inductive de ce système : $\mathrm{Puis}(K) = \varinjlim_n K((X_n))$.

Il s'agit d'une extension algébrique de $K((X_1))$ et l'on constate que, *via* le plongement considéré, la variable $X_n$ est une racine $n$-ième de $X_1$. C'est pourquoi on notera dans la suite $X = X_1$ et $X_n = X^{1/n}$. Le corps $\mathrm{Puis}(K)$ peut alors être moralement vu comme la réunion des corps $K((X^{1/n}))$.

Pour $n \geq 1$, on pose $v_n$ (resp. $I_{v_n}(K)$, resp. $1 + I_{v_n}(K)$) la valuation (resp. l'idéal de la valuation, le groupe des unités principales) de $K((X^{1/n}))$ ($v_n(X^{1/n}) = 1/n$). Toutes ces données étant compatibles au système inductif considéré, on en déduit qu'il existe une valuation $v$ sur $\mathrm{Puis}(K)$ obtenu en posant $v(S) = v_n(S)$ si $S \in K((X^{1/n}))$. On constate alors que, si l'on note $\mathrm{Puis}[K]$ l'anneau de la valuation, $\mathfrak{I}_v(K)$ l'idéal de la valuation et $1 + \mathfrak{I}_v(K) = \{S \in \mathrm{Puis}[K] / \ S(0) = 1\}$ le groupe des unités principales, alors on a

$$\mathrm{Puis}[K] = \varinjlim K[[X^{1/n}]], \ \mathfrak{I}_v(K) = \varinjlim I_{v_n}(K), \ 1 + \mathfrak{I}_v(K) = \varinjlim 1 + I_{v_n}(K)$$

Lorsque $K = C$ est un corps algébriquement clos de caractéristique 0, le corps $\mathrm{Puis}(C)$ est lui-même algébriquement clos (voir [8]). Si $R$ désigne un sous-corps réel clos de $C$ et si $c$ désigne l'involution telle que $C^{<c>} = R$, on peut faire agir $c$ sur les coefficients d'une série de Puiseux :

$$c\left(\sum_{k \geq k_0} a_k X^{k/n}\right) = \sum_{k \geq k_0} c(a_k) X^{k/n}$$

On obtient alors un automorphisme involutif $\tilde{c}$ de $\mathrm{Puis}(C)$ dont le corps des invariants est $\mathrm{Puis}(R)$. Ce dernier corps est donc un corps réel clos. L'unique ordre compatible sur $\mathrm{Puis}(R)$ est défini par les carrés et, compte

tenu du fait que dans Puis($R$) une série est un carré si et seulement si son premier coefficient non nul est lui-même un carré, on en déduit que si $S = \sum_{k \geq k_0} a_k X^{k/n}$ avec $a_{k_0} \neq 0$, on a

$$S > 0 \text{ dans } \mathrm{Puis}(R) \Longleftrightarrow a_{k_0} > 0 \text{ dans } R$$

**Proposition 3.1.** *Soit $R$ un corps réel clos et $C$ sa cloture algébrique.*

*1/ Les topologies sur* Puis($R$)*, définies respectivement par l'ordre $\leq$ et par la valuation $v$, coincident.*

*2/ Les topologies sur* Puis($C$)*, définies respectivement par la pseudo-distance et par la valuation $v$, coincident.*

*Démonstration.* 1/ La topologie de l'ordre sur Puis($R$) est celle engendrée par les intervalles ouverts

$$]S_1, S_2[ = \{S \in \mathrm{Puis}(R)/\ S_1 < S < S_2\}$$

Comme pour les deux topologies considérées, Puis($R$) est un groupe topologique, il suffit de montrer qu'il existe deux systèmes fondamentaux de voisinages de 0, $(U_n)_n$ et $(V_n)_n$, un pour chacune des topologies, tels que pour tout $n \geq 0$, $U_{n+1} \subset V_n \subset U_n$. On obtient de tels systèmes en considérant, pour $n$ fixé, les ensembles

$$U_n = ]-X^n, X^n[ \text{ et } V_n = \{S/\ v(S) > n\}$$

2/ L'argument est le même en considérant les ensembles

$$U_n = ]-X^n, X^n[ \times ]-X^n, X^n[ \text{ et } V_n = \{S/\ v(S) > n\}$$

Les $U_n$ forment bien un système fondamental de voisinages de 0 pour la topologie définie par la pseudo-distance puisque celle-ci correspond à la topologie produit (voir l'introduction). □

**Remarques :** 1/ La topologie induite par Puis($R$) sur $R$ est donc discrète.

2/ Les corps topologiques Puis($R$) et Puis($C$) sont des corps topologiques totalement discontinus.

3/ Le corps ordonné Puis($R$) n'est pas archimédien.

**3.1. Une exponentielle sur le corps des séries de Laurent.** On se fixe un corps $K$ quelconque. Si $S \in I_v(K)$ alors la suite $(S^n/n!)_n$ converge vers 0 pour $v$. On en déduit, puisque $K[[X]]$ est un anneau ultramétrique complet, que la série $\sum \dfrac{S^n}{n!}$ converge. Ceci permet d'introduire une fonction exponentielle :

$$\begin{array}{rccc} \mathbf{exp}: & I_v(K) & \longrightarrow & K[[X]] \\ & S & \longmapsto & \mathbf{exp}(S) = \displaystyle\sum_{n \geq 0} \frac{S^n}{n!} \end{array}$$

**Proposition 3.2.** *L'application* **exp** *est un isomorphisme de groupes topologiques entre les groupes* $(I_v(K),+)$ *et* $(1+I_v(K),.)$.

*Démonstration.* L'application **exp** est visiblement à valeurs dans $1+I_v(K)$. Pour $S,S' \in I_v$, on a

$$\mathbf{exp}(S+S') = \sum_{n\geq 0} \frac{(S+S')^n}{n!} = \sum_{n\geq 0}\sum_{k=0}^{n} \frac{C_n^k}{n!} S^k S'^{n-k} = \sum_{n\geq 0}\sum_{k=0}^{n} \frac{S^k}{k!}\frac{S'^{n-k}}{(n-k)!}$$

Maintenant, puisque nous sommes dans un espace ultramétrique complet, le produit de Cauchy de deux séries converge vers le produit des séries et donc

$$\mathbf{exp}(S).\mathbf{exp}(S') = \left(\sum_{n\geq 0}\frac{S^n}{n!}\right).\left(\sum_{n\geq 0}\frac{S'^n}{n!}\right) = \sum_{n\geq 0}\sum_{k=0}^{n}\frac{S^k}{k!}\frac{S'^{n-k}}{(n-k)!}$$

ce qui prouve le caractère morphique de **exp**.

Venons-en maintenant au caractère bijectif. Considérons deux séries quelconques $S = \sum_{n\geq 1} a_n T^n \in I_v(K)$ et $\Omega = 1 + \sum_{n\geq 1}\lambda_n T^n \in 1+I_v(K)$. En convenant que $a_0 = 0$, on a alors

$$\Omega = \mathbf{exp}(S) \Longleftrightarrow \forall n \geq 1,\ \lambda_n = \sum_{h=1}^{n}\frac{1}{h!}\sum_{i_1+\cdots+i_h=n} a_{i_1}\cdots a_{i_h}$$

Cette dernière condition équivaut à $a_1 = \lambda_1$ et, pour tout $n \geq 2$,

$$a_n = \lambda_n - \sum_{h=2}^{n}\frac{1}{h!}\sum_{i_1+\cdots+i_h=n} a_{i_1}\cdots a_{i_h}$$

et, dans la somme incriminée de cette égalité, le terme $a_n$ n'apparait jamais (puisque $a_0 = 0$).

On en déduit, par récurrence immédiate, que pour $(\lambda_n)_n$ donnée il existe une unique suite $(a_n)_n$ vérifiant cette dernière relation. Ceci assure alors la bijectivité de la fonction **exp**.

Puisque la fonction **exp** est un isomorphisme et que $\mathbf{exp}(0) = 1$, sa bicontinuité équivaut à sa continuité en 0 et à la continuité de $\mathbf{exp}^{-1}$ en 1. Il suffit alors de remarquer que pour tout $S \in I_v(K)$, $v(\mathbf{exp}(S)-1) = v(S)$ pour conclure. □

On va maintenant considérer le cas où $K = \overline{K} = C$ est un corps algébriquement clos et on va se donner une involution $c$ de $C$. On étend $c$ à $C((X))$, en une involution $\tilde{c}$, en la faisant agir sur les coefficients des séries. Le corps des invariants, par l'action de $\tilde{c}$, est $R((X))$ où $R = C^{<c>}$. On note $U = \{S \in C((X))/\ S.\tilde{c}(S) = 1\}$ et $U_0 = \{S \in 1+I_v(C)/\ S.\tilde{c}(S) = 1\} = (1+I_v(C)) \cap U$.

**Proposition 3.3.** *Les groupes $U$ et $\mathbb{U}(C,c)\times U_0$ sont isomorphes. L'application $S\longmapsto \mathbf{exp}(iS)$ définit un isomorphisme entre les groupes topologiques $I_v(R)$ et $U_0$, en conséquence de quoi $U$ est isomorphe à $\mathbb{U}(\overline{K},c)\times I_v(R)$.*

*Démonstration.* Soit $S=\sum_{n\geq n_0}a_nX^n\in U$ avec $a_{n_0}\neq 0$. On a

$$1=S.\tilde{c}(S)=a_0c(a_0)X^{2n_0}+\sum_{n\geq 2n_0+1}\cdots$$

et donc on a $n_0=0$ et $a_0\in\mathbb{U}(C,c)$. L'application

$$\begin{array}{ccc}\mathbb{U}(C,c)\times U_0 & \longrightarrow & U\\ (\alpha,S) & \longmapsto & \alpha.S\end{array}$$

est alors visiblement un isomorphisme de groupes.

Soit $\Omega\in 1+I_v(C)$ et $S\in I_v$ (unique) tel que $\Omega=\mathbf{exp}(S)$. On a

$$\begin{array}{rcl}\Omega.\tilde{c}(\Omega)=1 & \Longleftrightarrow & \mathbf{exp}(S).\tilde{c}(\mathbf{exp}(S))=1\Longleftrightarrow \mathbf{exp}(S).\mathbf{exp}(\tilde{c}(S))=1\\ & & \text{(puisque } \tilde{c} \text{ est visiblement un automorphisme}\\ & & \text{continu du corps des séries de Laurent)}\\ & \Longleftrightarrow & \mathbf{exp}(S+\tilde{c}(S))=1=\mathbf{exp}(0)\Longleftrightarrow S+\tilde{c}(S)=0\\ & \Longleftrightarrow & S\in iI_v(R)\end{array}$$

On déduit de ce qui précède que l'application $S_0\longmapsto \mathbf{exp}(iS_0)$ est un isomorphisme de $I_v(R)$ sur $U_0$. □

**3.2. Corps des séries de Puiseux.** L'objectif de ce paragraphe est de montrer le théorème général suivant :

**Théorème 3.2.** *Soient $C$ un corps algébriquement clos, $c$ une involution de $C$ et $R=\mathfrak{R}(C,c)$. Si $\mathbb{U}(C,c)\underset{alg}{\simeq}\mathfrak{R}(C,c)/\mathbb{Z}=R/\mathbb{Z}$ alors*

$$\mathbb{U}(\mathrm{Puis}(C),\tilde{c})\underset{top}{\simeq}\mathfrak{R}(\mathrm{Puis}(C),\tilde{c})/\mathbb{Z}=\mathrm{Puis}(R)/\mathbb{Z}$$

On garde les notations du théorème et on pose

$$\mathbb{U}_0(\mathrm{Puis}(C),\tilde{c})=\{S\in 1+\mathfrak{I}_v(C)/\ S\tilde{c}(S)=1\}$$

Si on considère pour $n\geq 1$, $U_0(C)_n=\{S\in 1+I_{v_n}(C)/\ S.\tilde{c}(S)=1\}$, on a alors

$$\mathbb{U}_0(\mathrm{Puis}(C),\tilde{c})=\varinjlim U_0(C)_n$$

**Lemme 3.1.** *L'application*

$$\mathbf{E}:\mathfrak{I}_v(R)\longrightarrow\mathbb{U}_0(\mathrm{Puis}(C),\tilde{c})$$

*définie, pour $S\in I_{v_n}(R)$, par $\mathbf{E}(S)=\mathbf{exp}(iS)$ est bien définie et constitue un isomorphisme de groupes topologiques.*

*Démonstration.* Le fait que $\mathbf{E}$ soit un isomorphisme découle du fait que, d'après la proposition 3.3, l'application $S \longmapsto \mathbf{exp}(iS)$ est un isomorphisme de $I_{v_n}(R)$ sur $U_0(C)_n$ pour tout $n \geq 1$ et que l'on a $\mathfrak{I}_v(R) = \varinjlim I_{v_n}(R)$ et $\mathbb{U}_0(\mathrm{Puis}(C), \tilde{c}) = \varinjlim U_0(C)_n$. La bicontinuité de $\mathbf{E}$ découle du fait que pour tout $S \in \mathfrak{I}_v(R)$, on a $v(\mathbf{E}(S) - 1) = v(S)$. □

**Lemme 3.2.** *On note $R^d$ (resp. $\mathbb{U}^d(C, c)$) le groupe additif $R$ (resp. multiplicatif $\mathbb{U}(C, c)$) muni de la topologie discrète. On note aussi* $\mathrm{Puis}^\circ(R)$ *le sous-groupe additif de* $\mathrm{Puis}(R)$ *constitué des séries de Puiseux dont le coefficient constant est nul. On a*

$$\mathbb{U}^d(C, c) \times \mathbb{U}_0(\mathrm{Puis}(C), \tilde{c}) \underset{top}{\simeq} \mathbb{U}(\mathrm{Puis}(C), \tilde{c}) \text{ et } \mathrm{Puis}(R) \underset{top}{\simeq} R^d \times \mathrm{Puis}^\circ(R)$$

*Démonstration.* Considérons l'application

$$\begin{array}{rccc} D: & \mathrm{Puis}(R) & \longrightarrow & R^d \times \mathrm{Puis}^\circ(R) \\ & S = \displaystyle\sum_{k \geq k_0} a_k X^{k/n} & \longmapsto & (a_0, S^\circ) \qquad (\text{où } S^\circ = S - a_0) \end{array}$$

Il s'agit visiblement d'un isomorphisme de groupes. Ces groupes étant des groupes topologiques, pour montrer la continuité de $D$, il suffit de la montrer en 0. Ceci est assuré par le fait que l'ouvert fondamental $\{0\} \times ]-X^n, X^n[$ a pour image réciproque par $D$ l'ouvert $]-X^n, X^n[$. L'image directe de $]-X^n, X^n[$ (qui est un ouvert fondamental) par $D$ étant alors $\{0\} \times ]-X^n, X^n[$, ceci prouve que $D^{-1}$ est continue en 0.

On considère maintenant l'application

$$\begin{array}{rccc} P: & \mathbb{U}^d(C, c) \times \mathbb{U}_0(\mathrm{Puis}(C), \tilde{c}) & \longrightarrow & \mathbb{U}(\mathrm{Puis}(C), \tilde{c}) \\ & (a_0, S) & \longmapsto & a_0.S \end{array}$$

qui est visiblement un isomorphisme de groupes.

Si l'on note $B_v(0, n) = \{S \in \mathrm{Puis}(C) / \ v(S) > n\}$, alors l'ouvert fondamental

$$(1 + B_v(0, n)) \cap \mathbb{U}(\mathrm{Puis}(C), \tilde{c})$$

a pour image réciproque par $P$ l'ouvert

$$\{1\} \times ((1 + B_v(0, n)) \cap \mathbb{U}_0(\mathrm{Puis}(C), \tilde{c})$$

ce qui prouve la bicontinuité de $P$. □

**Lemme 3.3.** *Les groupes topologiques $\mathfrak{I}_v(R)$ et* $\mathrm{Puis}^\circ(R)$ *sont isomorphes.*

*Démonstration.* Soit $f : \mathbb{Q}^* \longrightarrow \mathbb{Q}^{+*}$ une bijection croissante telle que

$$(*)\ \exists \alpha, \alpha',\ \forall n \geq 1,\ f\left(\frac{1}{n}\mathbb{Z} \cap [\alpha, +\infty[\right) = \frac{1}{n}\mathbb{Z} \cap [\alpha', +\infty[$$

Considérons l'application

$$\begin{array}{rccc} \Theta: & \mathrm{Puis}^\circ(R) & \longrightarrow & \mathfrak{I}_v(R) \\ & \displaystyle\sum_{k \geq k_0} a_k X^{k/n} & \longmapsto & \displaystyle\sum_{k \geq k_0} a_k X^{f(k/n)} \end{array}$$

qui est bien définie à cause de l'hypothèse $(*)$. Il est clair que $\Theta$ est un morphisme de groupes additifs, son caractère bijectif s'obtient en exprimant sa réciproque

$$\begin{array}{rccc} \Theta^{-1}: & \mathfrak{I}_v(R) & \longrightarrow & \mathrm{Puis}^\circ(R) \\ & \displaystyle\sum_{k\geq 0} a_k X^{k/n} & \longmapsto & \displaystyle\sum_{k\geq 0} a_k X^{f^{-1}(k/n)} \end{array}$$

La continuité de $\Theta$ en 0 est assurée par le fait que $f$ est une bijection croissante. En effet, soit $r \in \mathbb{Q}$, posons $r' = f^{-1}(r)$ et considérons les boules

$$B_r = \{S \in \mathfrak{I}_v(R)/\ v(S) > r\} \text{ et } B_{r'} = \{S \in \mathrm{Puis}^\circ(R)/\ v(S) > r'\}$$

On a alors $\Theta(B_{r'}) = B_r$, ce qui prouve bien la continuité de $\Theta$ en 0. La continuité de $\Theta^{-1}$ en 0 découle, de même, du fait que $f^{-1}$ est une bijection croissante.

Reste à exhiber une application $f$ ayant les propriétés sus-mentionnées. On définit $f$ de la manière suivante :

Sur $]-\infty, -1]$, on pose $f(r) = -1/r$.

Sur $[1, +\infty[$, on pose $f(r) = r + 3$.

Sur $]0, 1]$ on définit $f$ comme fonction affine rationnelle par morceaux : on pose $\alpha_1 = \beta_1 = 2$ et pour tout $n \geq 2$,

$$\alpha_n = 2 - \sum_{k=1}^{n-1} \frac{1}{k!} \text{ et } \beta_n = \sum_{k=0}^{n} \frac{1}{k!}$$

et sur l'intervalle $\left]\dfrac{1}{n+1}, \dfrac{1}{n}\right]$ on pose $f(r) = f_n(r) = \alpha_n r + \beta_n$.

La suite $(\alpha_n)_n$ est une suite décroissante de rationnels strictement positifs, la suite $(\beta_n)_n$ converge vers la base de l'exponentielle réelle $e$. Par ailleurs, on a pour tout $n \geq 2$

$$(\alpha_{n-1} - \alpha_n) = \frac{1}{(n-1)!} = n\frac{1}{n!} = n(\beta_n - \beta_{n-1})$$

on en déduit que

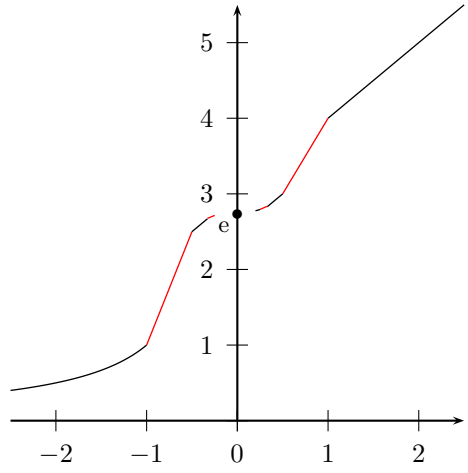
$$f_{n-1}\left(\frac{1}{n}\right) = \frac{\alpha_{n-1}}{n} + \beta_{n-1} = \frac{\alpha_n}{n} + \beta_n = f_n\left(\frac{1}{n}\right)$$

Ainsi, sur $]0, 1]$, la fonction de la variable réelle $f$ est continue, affine rationnelle par morceaux et strictement croissante. Par ailleurs, on a

$$\lim_{r\to 0^+} f(r) = \lim_n f\left(\frac{1}{n}\right) = \lim_n f_n\left(\frac{1}{n}\right) = \lim_n \left(\frac{\alpha_n}{n} + \beta_n\right) = \lim_n \beta_n = e$$

Ainsi $f$ définie une bijection de $]0, 1] \cap \mathbb{Q}$ sur $]e, 4] \cap \mathbb{Q}$.

Sur $[-1, 0[$, comme précédemment, on définit $f$ comme fonction affine rationnelle par morceaux qui opère une bijection croissante de $[-1, 0[\cap\mathbb{Q}$




sur $[1, e[\cap\mathbb{Q}$. Le graphe de la fonction obtenue ressemble à peu près à ce qui précède.

Il est clair que $f$ opère une bijection croissante de $\mathbb{Q}^*$ sur $\mathbb{Q}^{+*}$ et que l'on a par ailleurs, pour tout $n \geq 1$, $f\left(\frac{1}{n}\mathbb{Z} \cap [1, +\infty[\right) = \frac{1}{n}\mathbb{Z} \cap [4, +\infty[$. □

*Preuve du théorème 3.2.* Grace aux lemmes 3.1, 3.2 et 3.3, on dispose d'un épimorphisme continu de groupes topologiques

$$\mathrm{EXP} : \mathrm{Puis}(R) \longrightarrow \mathbb{U}(\mathrm{Puis}(C), \tilde{c})$$

défini par les composées successives

$$\mathrm{Puis}(R) \longrightarrow R^d \times \mathrm{Puis}^\circ(R) \longrightarrow R^d \times \mathfrak{I}_v(R) \longrightarrow$$
$$\longrightarrow \mathbb{U}^d(C, c) \times \mathbb{U}_0(\mathrm{Puis}(C), \tilde{c}) \longrightarrow \mathbb{U}(\mathrm{Puis}(C), \tilde{c})$$

$$S \longmapsto (a_0, S^\circ) \longmapsto (a_0, \Theta(S^\circ)) \longmapsto (\varepsilon^{a_0}, E(\Theta(S^\circ))) \longmapsto \varepsilon^{a_0} E(\Theta(S^\circ))$$

Le noyau du morphisme $R^d \times \mathfrak{I}_v(R) \longrightarrow \mathbb{U}^d(C, c) \times \mathbb{U}_0(\mathrm{Puis}(C), \tilde{c})$ correspond au noyau du morphisme algébrique $R^d \longmapsto \mathbb{U}^d(C, c)$ qui est $\mathbb{Z}$ par hypothèse. Puisque $R^d$ est un espace discret, il en est de même de $R^d/\mathbb{Z}$ et donc le passage au quotient définit un isomorphisme de groupes topologiques $R^d/\mathbb{Z} \underset{\text{top}}{\simeq} \mathbb{U}^d(C, c)$ qui fournit, par produit, un isomorphisme de groupes topologiques

$$(R^d \times \mathfrak{I}_v(R))/(\mathbb{Z} \times \{0\}) \underset{\text{top}}{\simeq} \mathbb{U}^d(C, c) \times \mathbb{U}_0(\mathrm{Puis}(C), \tilde{c})$$

On en déduit que l'application EXP définit, par passage au quotient, un isomorphisme de groupes topologiques entre $\mathrm{Puis}(R)/\mathbb{Z}$ et $\mathbb{U}(\mathrm{Puis}(C), \tilde{c})$. □

*Preuve du théorème 3.1.* Les corps $\mathbb{C}$ et Puis($\mathbb{C}$) sont deux corps qui, étant algébriquement clos de caractéristique 0 et possédant un même cardinal indénombrable, sont isomorphes (argument classique utilisant le théorème de Steinitz sur des sous-extensions transcendantes pures maximales de ces corps). On se fixe donc $\varphi : \mathrm{Puis}(\mathbb{C}) \longrightarrow \mathbb{C}$ un isomorphisme abstrait et on considère l'involution de $\mathbb{C}$, $c_0 = \varphi \circ \tilde{c} \circ \varphi^{-1}$.

Le théorème 3.2 assure que l'on a $\mathbb{U}(\mathrm{Puis}(\mathbb{C}), \tilde{c}) \underset{\mathrm{top}}{\simeq} \mathrm{Puis}(\mathbb{R})/\mathbb{Z}$. Maintenant $\varphi$ définit, par restriction, un isomorphisme entre $\mathrm{Puis}(\mathbb{R}) = \mathfrak{R}(\mathrm{Puis}(\mathbb{C}), \tilde{c})$ et $\mathfrak{R}(\mathbb{C}, c_0)$, et comme $\varphi$ envoie les carrés sur les carrés, sa restriction représente donc un isomorphisme de corps tolopologiques. On en déduit que $\varphi$ est un isomorphisme de corps topologiques entre le corps Puis($\mathbb{C}$) muni de la topologie induite par $\tilde{c}$ et le corps $\mathbb{C}$ muni de la topologie induite par $c_0$ et, par suite, que

$$\mathbb{U}(\mathbb{C}, c_0) \underset{\mathrm{top}}{\simeq} \mathfrak{R}(\mathbb{C}, c_0)/\mathbb{Z}$$

Le point à vérifier maintenant est que $c_0$ n'est pas conjuguée à la conjugaison complexe. Si tel était le cas, disons que $c_0 = \sigma c \sigma^{-1}$, alors *via* $\varphi$, les corps réels clos $\mathfrak{R}(\mathbb{C}, \sigma c \sigma^{-1}) \simeq \mathfrak{R}(\mathbb{C}, c) = \mathbb{R}$ et $\mathfrak{R}(\mathrm{Puis}(\mathbb{C}), \tilde{c}) = \mathrm{Puis}(\mathbb{R})$ seraient isomorphes. Or Puis($\mathbb{R}$) n'est pas un corps archimédien (d'après la remarque du début du §3), au contraire de $\mathbb{R}$. Ainsi, l'involution $c_0$ n'est pas conjuguée à la conjugaison complexe. □

## Bibliographie


[1] B. Deschamps, *Problèmes d'arithmétique et de théorie de Galois*. Hermann, Paris, 1998.

[2] B. Deschamps, *Clôture totalement réelle des corps de nombres ordonnables*. Manuscripta Mathematica **100** (1999), 291–304.

[3] B. Deschamps, *Le corps des séries de Puiseux généralisées*. Acta Arithmetica **XCVI.4** (2001), 351–360.

[4] B. Deschamps, *Des automorphismes continus d'un corps de séries de Puiseux*. Acta Arithmetica **CXVIII.3** (2005), 205-229.

[5] L. Fuchs, *Infinite Abelian Groups*. Vol. I, Academic Press, New-York, 1970.

[6] E. Hewitt and K. A. Ross, *Abstract Harmonic Analysis I*. Springer, Berlin, 1963.

[7] P. Ribenboim, *L'arithmétique des corps*. Hermann, Paris, 1972.

[8] J.-P. Serre, *Corps locaux (4ème édition)*. Hermann, Paris, 1997.



Bruno Deschamps
Département de Mathématiques de l'Université du Maine
Avenue Olivier Messiaen 72085 Le Mans cedex 9.
*E-mail*: Bruno.Deschamps@univ-lemans.fr
*URL*: http://perso.univ-lemans.fr/~bdesch/