À propos du corps des nombres constructibles

On dira qu'un corps $K \leq \mathbb{R}$ est *stable par* $\sqrt{\ }$ si

$$^{\forall} x \in K \cap \mathbb{R}_{>0},\ \sqrt{x} \in K\ .$$

Par exemple, l'ensemble des nombres algébriques réels est stable par $\sqrt{\ }$ [†].
On pose $\mathcal{C}$ l'intersection de tous les sous-corps de $\mathbb{R}$ stables par $\sqrt{\ }$.
C'est le plus petit sous-corps de $\mathbb{R}$ stable par $\sqrt{\ }$.
Définition. Les éléments du corps $\mathcal{C}$ sont les nombres réels *constructibles*.
Par exemple $2\cos\frac{2\pi}{17}$ est constructible car :

$$2\cos\left(\frac{2\pi}{17}\right) =$$

$$-\frac{1}{8}+\frac{1}{8}\sqrt{17}+\frac{1}{8}\sqrt{34-2\sqrt{17}}+\frac{1}{4}\sqrt{17+3\sqrt{17}-\sqrt{34-2\sqrt{17}}-2\sqrt{34+2\sqrt{17}}}$$

d'après Gauss.

Théorème. Soit $x \in \mathbb{R}$. Sont équivalentes

(i) Soit π_x le polynôme minimal de x sur $\mathbb{Q}$. Le groupe $\mathrm{Gal}_{\mathbb{Q}}(\pi_x)$ est un $2-$groupe [‡].

(ii) Il existe un sous-corps $K \leq \mathbb{C}$ tel que l'extension $K/\mathbb{Q}$ est **galoisienne** et $x \in K$ et $[K : \mathbb{Q}]$ est une puissance de 2.

(iii) Il existe des corps $\mathbb{Q} = K_0 \leq K_1 \leq ... \leq K_N \leq \mathbb{R}$ tels que $x \in K_N$ et $^{\forall} 1 \leq i \leq N$, $[K_i : K_{i-1}] = 2$.

(iv) Il existe $N \in \mathbb{N}$ et des réels $a_1, ..., a_N > 0$ tels que $x \in \mathbb{Q}(\sqrt{a_1}, ..., \sqrt{a_N})$ et $^{\forall} i, a_i \in \mathbb{Q}(\sqrt{a_1}, ..., \sqrt{a_{i-1}})$.

(v) Le nombre x est constructible.

Démo.

$$i \Rightarrow ii$$

Notons $x = x_1, x_2, ..., x_n$ les racines de π_x dans $\mathbb{C}$. On pose $K = \mathbb{Q}(x_1, ..., x_n)$. Alors l'extension $K/\mathbb{Q}$ est galoisienne, $[K : \mathbb{Q}] = |\mathrm{Gal}(K/\mathbb{Q})| = |\mathrm{Gal}_{\mathbb{Q}}(\pi_x)|$ est une puissance de 2 et $x \in K$.

†. Mais le corps $\mathbb{Q}$ n'est pas stable par $\sqrt{\ }$ car $\sqrt{2} \notin \mathbb{Q}$

‡. *c-à-d* un groupe d'ordre une puissance de 2.

$$ii \Rightarrow iii$$

Soit $K/\mathbb{Q}$ une extension galoisienne de degré $[K:\mathbb{Q}] = 2^\alpha$ telle que $x \in K$.

Soit $G = \mathrm{Gal}(K/\mathbb{Q})$. Comme $|G| = [K:\mathbb{Q}]$, le groupe G estun $2-$groupe. Donc il existe des sous-groupes

$$G = G_0 \geq G_1 \geq ... \geq G_N = 1$$

tels que $^\forall i$, $G_i \triangleleft G$ et $G_i/G_{i+1} \simeq \mathbb{Z}/2\mathbb{Z}$.

On pose alors $K_i = K^{G_i}$.

D'après la correspondance de Galois on obtient une tour d'extensions :

$$K_0 = \mathbb{Q} \leq K_1 \leq ... \leq K_N = K$$

où $^\forall i$, $[K_i : K_{i-1}] = \frac{[K:K_{i-1}]}{[K:K_i]} = \frac{|G_{i-1}|}{|G_i|} = |G_{i-1}/G_i| = 2$.

Si $K_n \leq \mathbb{R}$, c'est terminé. Sinon, vérifions que l'on peut remplacer les K_i par les $K_i \cap \mathbb{R}$.

Pour tout i, $G_i \triangleleft G$ donc l'extension $K_i/\mathbb{Q}$ est galoisienne. Soit $i \geq 1$.

Soit τ la restriction de la conjugaison complexe à K_i. Comme $K_i/\mathbb{Q}$ est galoisienne, $\tau(K_i) = K_i$. On a $K_i^{\langle\tau\rangle} = K_i \cap \mathbb{R}$. Donc $[K_i : K_i \cap \mathbb{R}] = |\langle\tau\rangle| = 1$ si $K_i \leq \mathbb{R}$, 2 sinon.

Si $K_{i-1} \leq \mathbb{R}$, alors

$$K_{i-1} \cap \mathbb{R} = K_{i-1} \leq K_i \cap \mathbb{R} \leq K_i$$

donc $[K_i \cap \mathbb{R} : K_{i-1} \cap \mathbb{R}] = 1$ ou 2.

Si $K_{i-1} \not\leq \mathbb{R}$, alors $[K_i : K_{i-1} \cap \mathbb{R}] = [K_i : K_{i-1}][K_{i-1} : K_{i-1} \cap \mathbb{R}] = 4$. Or : $[K_i : K_{i-1} \cap \mathbb{R}] = [K_i : K_i \cap \mathbb{R}][K_i \cap \mathbb{R} : K_{i-1} \cap \mathbb{R}] = 2[K_i \cap \mathbb{R} : K_{i-1} \cap \mathbb{R}]$ donc $[K_i \cap \mathbb{R} : K_{i-1} \cap \mathbb{R}] = 2$.

On peut donc considérer les corps $K_i \cap \mathbb{R}$ à la place des corps K_i .

$$\mathbb{Q} = K_0 \cap \mathbb{R} \leq K_1 \cap \mathbb{R} \leq ... \leq K_N \cap \mathbb{R} = K \cap \mathbb{R}$$

et $x \in K \cap \mathbb{R}$ et $^\forall i$, $[K_i \cap \mathbb{R} : K_{i-1} \cap \mathbb{R}] = 1$ ou 2.

$$iii \Rightarrow iv$$

Soit $i \geq 1$. Comme K_i/K_{i-1} est une extension de degré 2, pour un $y \in K_i \setminus K_{i-1}$, on a $K_i = K_{i-1}(y)$.

Comme on suppose $K_i \leq \mathbb{R}$, on a $y \in \mathbb{R}$. Soit π_y le polynôme minimal de y sur K_{i-1}. On a $\pi_y \in K_{i-1}[X] \leq \mathbb{R}[X]$ de degré 2. Son discriminant est > 0 car il y a au moins une racine réelle. Notons-le a_i.

On a $a_i \in K_{i-1} \cap \mathbb{R}_{>0}$ et $K_{i-1}(y) = K_{i-1}(\sqrt{a_i})$.

$$iv \Rightarrow v$$

Comme le corps $\mathcal{C}$ est stable par $\sqrt{}$, on a par récurrence, pour tout i, $\sqrt{a_i} \in \mathcal{C}$ donc $x \in \mathbb{Q}(\sqrt{a_1}, ..., \sqrt{a_N}) \leq \mathcal{C}$.

$$v \Rightarrow i$$

Notons

$$\mathcal{C}' = \left\{ z \in \mathbb{R} \ : \ z \text{ est algébrique sur } \mathbb{Q} \text{ et } \mathrm{Gal}_{\mathbb{Q}}(\pi_z) \text{ est un } 2-\text{groupe} \right\} .$$

Vérifions que $\mathcal{C}'$ est un sous-corps de $\mathbb{R}$ stable par $\sqrt{}$.

Soient $y, z \in \mathcal{C}'$. Notons $y = y_1, ..., y_m$, $z = z_1, ..., z_n$ les conjugués de y et de z dans $\mathbb{C}$.

Alors $\mathbb{Q}(y_1, ..., y_m)$ est le corps de décomposition de π_y. Donc l'extension $\mathbb{Q}(y_1, ..., y_m)/\mathbb{Q}$ est galoisienne et le groupe $\mathrm{Gal}(\mathbb{Q}(y_1, ..., y_m)/\mathbb{Q}) = \mathrm{Gal}_{\mathbb{Q}}(\pi_y)$ est un $2-$groupe. L'extension $\mathbb{Q}(y_1, ..., y_m, z_1, ..., z_n)/\mathbb{Q}$ est aussi galoisienne en tant que corps de décomposition du polynôme $\pi_y \pi_z$. Posons

$$G = \mathrm{Gal}(\mathbb{Q}(y_1, ..., y_m, z_1, ..., z_n)/\mathbb{Q}) \ .$$

D'après la correspondance de Galois,

$$\mathrm{Gal}(\mathbb{Q}(y_1, ..., y_m, z_1, ..., z_n)/\mathbb{Q}(y_1, ..., y_m)) \triangleleft G$$

et on a un isomorphisme de groupes :

$$G/\mathrm{Gal}(\mathbb{Q}(y_1, ..., y_m, z_1, ..., z_n)/\mathbb{Q}(y_1, ..., y_m)) \simeq \mathrm{Gal}(\mathbb{Q}(y_1, ..., y_m)/\mathbb{Q}),\ \sigma \mapsto \sigma\Big|_{\mathbb{Q}(y_1,...,y_m)}$$

donc le groupe quotient :

$$G/\mathrm{Gal}(\mathbb{Q}(y_1, ..., y_m, z_1, ..., z_n)/\mathbb{Q}(y_1, ..., y_m))$$

est un $2-$groupe.

Or le morphisme de groupes

$$\mathrm{Gal}(\mathbb{Q}(y_1, ..., y_m, z_1, ..., z_n)/\mathbb{Q}(y_1, ..., y_m)) \to \mathrm{Gal}(\mathbb{Q}(z_1, ..., z_n)/\mathbb{Q}),\ \sigma \mapsto \sigma\Big|_{\mathbb{Q}(z_1,...,z_n)}$$

est injectif. Donc le groupe

$$\mathrm{Gal}(\mathbb{Q}(y_1, ..., y_m, z_1, ..., z_n)/\mathbb{Q}(y_1, ..., y_m))$$

est aussi un 2−groupe.

On en déduit que G est un 2−groupe.

Puisque $\mathbb{Q}(y,z) \leq \mathbb{Q}(y_1,...,y_m,z_1,...,z_n)$, on en déduit que si

$$w \in \{z+y, z-y, zy, z/y\}$$

(si $y \neq 0$) alors le corps engendré par w et ses consugués est un sous-corps de $\mathbb{Q}(y_1,...,y_m,z_1,...,z_n)$ donc $\mathrm{Gal}_{\mathbb{Q}}(\pi_w)$ est un 2−groupe. †

Donc $w \in \mathcal{C}'$.

Ainsi $\mathcal{C}'$ est bien un sous-corps de $\mathbb{R}$. Montrons que $\mathcal{C}'$ est stable par $\sqrt{}$.

Soit $y \in \mathcal{C}' \cap \mathbb{R}_{>0}$. Notons $y = y_1,...,y_m$ les conjugués de y dans $\mathbb{C}$. Notons $\delta_1 = \sqrt{y}$ et $\delta_2, ...\delta_m$ des racines carrés des y_i :

$$^{\forall} i,\ \delta_i^2 = y_i \ .$$

Le corps $\mathbb{Q}(\delta_1,...,\delta_m)$ est une extension galoisienne de $\mathbb{Q}$ (comme corps de décomposition du polynôme $(X^2-y_1)...(X^2-y_m)$ †).

Posons $G = \mathrm{Gal}(\mathbb{Q}(\delta_1,...,\delta_m)/\mathbb{Q})$, $H = \mathrm{Gal}_{\mathbb{Q}}(\pi_y) = \mathrm{Gal}(\mathbb{Q}(y_1,...,y_m)/\mathbb{Q})$ et $K = \mathrm{Gal}(\mathbb{Q}(\delta_1,...,\delta_m)/\mathbb{Q}(y_1,...,y_m))$.

Puisque $\sqrt{y} = \delta_1$, le corps de décomposition de $\sqrt{y}$ est contenu dans $\mathbb{Q}(\delta_1,...,\delta_m)$ et donc

$$\mathrm{Gal}_{\mathbb{Q}}(\pi_{\sqrt{y}})$$

est un quotient de G.

Nous allons voir que G est un 2−groupe. En effet, $G/K \simeq H$ est un 2−groupe. Donc il suffit de montrer que K est un 2−groupe. Or Pour tout $\sigma \in K$, on a

$$^{\forall} i,\ \sigma(\delta_i)^2 = \sigma(y_i) = y_i = \delta_i^2$$
$$\Rightarrow {}^{\forall} i,\ \sigma(\delta_i) = \pm\delta_i = (-1)^{\epsilon_i(\sigma)}\delta_i$$

pour certains $\epsilon_i(\sigma) \in \mathbb{Z}/2\mathbb{Z}$.

On vérifie facilement que l'application :

$$K \to (\mathbb{Z}/2\mathbb{Z})^m,\ \sigma \mapsto (\epsilon_i(\sigma))_{i=1}^m$$

est un morphisme injectif de groupes. Donc K est bien un 2−groupe !

Donc $\sqrt{y} \in \mathcal{C}'$ et $\mathcal{C}'$ est stable par $\sqrt{}$.

On a donc $\mathcal{C} \leq \mathcal{C}'$ et

$$x \in \mathcal{C} \Rightarrow \mathrm{Gal}_{\mathbb{Q}}(\pi_x) \text{ est un 2−groupe.}$$

Q.e.d.

†. comme quotient du groupe $\mathrm{Gal}(\mathbb{Q}(y_1,...,y_m,z_1,...,z_n)/\mathbb{Q})$.

†. $\in \mathbb{Q}[X]$ car les coefficients sont symétriques en les y_i et $\pi_y = (X-y_1)..(X-y_m)$.