Une remarque sur la méthode de Cardan

Si P admet une racine réelle et deux racines complexes conjuguées, la formule de Cardan donne une expression de cette première au moyen d'extraction de radicaux réels uniquement. En revanche, on ne peut éviter d'en passer par des complexes lorsque P a ses trois racines dans $\mathbb{R}$. Plus précisément :

Théorème 1 *Soit* $\mathrm{P(X)} = x^3 + a_2x^2 + a_1x + a_0$ *un polynôme irréductible sur* $\mathbb{K}_0 = \mathbb{Q}[a_0, a_1, a_2]$ *et ayant ses trois racines réelles. Alors il n'existe pas de tour d'extensions* $\mathbb{K}_0 \subset \cdots \subset \mathbb{K}_n \subset \mathbb{R}$ *telle que pour tout* i, $\mathbb{K}_i$ *s'obtienne par adjonction à* $\mathbb{K}_{i-1}$ *d'une racine* p_i*-ième (où* p_i *est un nombre premier), et telle que* $\mathbb{K}_n$ *contienne une racine de* P.

N.B. La restriction p_i premier n'en est pas une. En effet, pour rajouter une racine pq-ième d'un nombre a, il suffit de rajouter la racine p-ième de a, puis à l'étape suivante la racine q-ième du nombre obtenu.

Démonstration : Procédant par l'absurde, supposons donnée une tour d'extensions $\mathbb{K}_0 \subset \cdots \subset \mathbb{K}_n \subset \mathbb{R}$ telle que pour tout i, $\mathbb{K}_i$ s'obtienne par adjonction à $\mathbb{K}_{i-1}$ d'une racine p_i-ième (p_i premier), telle que $\mathbb{K}_n$ contienne une racine de P, et que le nombre n soit minimal parmi toutes les tours vérifiant ces propriétés. Distinguons deux cas, selon que p_n vaut 2 ou vaut au moins 3.

Supposons d'abord $p_n = 2$, de sorte que $\mathbb{K}_n$ est une extension galoisienne (car quadratique) de $\mathbb{K}_{n-1}$. Soit x une racine de P contenue dans $\mathbb{K}_n$. Si l'unique $\mathbb{K}_{n-1}$-automorphisme non-trivial de $\mathbb{K}_n$ envoie la racine x sur elle-même, cela signifie que x est dans $\mathbb{K}_{n-1}$, ce qui contredit la minimalité de n. Sinon, si y est l'image de x par cet automorphisme, alors $\mathbb{K}_n$ contient deux racines de P, x et y, donc contient la troisième racine z. En effet la somme $x + y + z = -a_2$ est dans $\mathbb{K}_0$ donc dans $\mathbb{K}_n$, et donc $z \in \mathbb{K}_n$. Et alors z est nécessairement stable par cet automorphisme, car envoyé sur une racine qui ne peut être ni x ni y. Et l'on retrouve la contradiction précédente en considérant z plutôt que x.

Supposons maintenant $p_n \geq 3$. Nous allons utiliser le :

Lemme 2 *Si* $p \geq 3$ *est un nombre premier, si* $\mathbb{K}$ *est un sous-corps de* $\mathbb{R}$*, si* a *est un élément de* $\mathbb{K}$ *qui n'est pas une puissance* p*-ième dans* $\mathbb{K}$*, alors le polynôme* $\mathrm{X}^p - a$ *est irréductible sur* $\mathbb{K}$*. Si* $\mathbb{L} = \mathbb{K}[\sqrt[p]{a}]$ *est le sous-corps de* $\mathbb{R}$ *obtenu en adjoignant à* $\mathbb{K}$ *l'unique racine* p*-ième réelle de* a*, et si* σ *est un* $\mathbb{K}$*-plongement non trivial de* $\mathbb{L}$ *dans* $\mathbb{C}$*, alors l'intersection de* $\sigma(\mathbb{L})$ *et de* $\mathbb{R}$ *se réduit à* $\mathbb{K}$*.*

Appliquons le lemme avec $\mathbb{K} = \mathbb{K}_{n-1}$ et $\mathbb{L} = \mathbb{K}_n$. Soit x une racine de P contenue dans $\mathbb{L}$. Tout $\mathbb{K}$-plongement de $\mathbb{L}$ dans $\mathbb{C}$ va permuter les racines de P, donc envoyer x dans $\mathbb{R}$ et donc, par la dernière assertion du lemme, va stabiliser x. Cela signifie que x est dans $\mathbb{K}$, et contredit à nouveau la minimalité de n.

□

Démonstration du lemme : Tout d'abord, le polynôme $X^p - a$ est irréductible sur $\mathbb{K}$. En effet, si au contraire $X^p - a$ s'écrit sous la forme $Q(X)R(X)$, avec Q et R deux polynômes de $\mathbb{K}[X]$ de degrés respectivement q et $p-q$ ($1 \leq q \leq p-1$), alors les termes constants de Q et R sont respectivement (au signe près) $(\sqrt[p]{a})^q$ et $(\sqrt[p]{a})^{p-q}$. Pour voir cela, il suffit de décomposer sur $\mathbb{C}$ notre polynôme :

$$X^p - a = \prod_{k=0}^{p} \left(X - e^{\frac{2ik\pi}{p}} \sqrt[p]{a} \right)$$

Les polynômes Q et R sont donc les produits de q (resp. $p-q$) termes de la forme $X - e^{\frac{2ik\pi}{p}} \sqrt[p]{a}$, donc leurs termes constants sont eux des produits de q (resp. $p-q$) termes de la forme $-e^{\frac{2ik\pi}{p}} \sqrt[p]{a}$. En particulier, ils sont donc de module respectivement $(\sqrt[p]{a})^q$ et $(\sqrt[p]{a})^{p-q}$. Comme par hypothèse ce sont des éléments de $\mathbb{K}$ donc de $\mathbb{R}$, on obtient la forme annoncée.

En particulier, le corps $\mathbb{K}$ contient les nombres $(\sqrt[p]{a})^q$ et $(\sqrt[p]{a})^{p-q}$, avec q un entier compris entre 1 et $p-1$. Il contient donc toutes leurs puissances (entières). Nous allons voir qu'il contient alors le nombre $\sqrt[p]{a}$, ce qui contredit l'hypothèse que a n'est pas une puissance p-ième dans $\mathbb{K}$, et établit donc l'irréductibilité du polynôme $X^p - a$ dans $\mathbb{K}[X]$.

Comme $1 \leq q \leq p-1$, on nécessairement q premier à p, donc par le théorème de Bezout on peut trouver deux entiers n et m tels que $qn + pm = 1$, et donc $q(n+m) + (p-q)m = 1$ (*i.e.* q est premier à $p-q$). On a donc :

$$\sqrt[p]{a} = (\sqrt[p]{a})^{q(n+m)+(p-r)m} = \left((\sqrt[p]{a})^q\right)^{n+m} \cdot \left((\sqrt[p]{a})^{p-q}\right)^m$$

Et donc $\sqrt[p]{a} \in \mathbb{K}$, ce qui on l'a vu est absurde.

Soit σ un $\mathbb{K}$-plongement non trivial de $\mathbb{L} = \mathbb{K}[\sqrt[p]{a}]$ dans $\mathbb{C}$, c'est-à-dire un morphisme (injectif) de corps qui fixe les éléments de $\mathbb{K}$. Alors l'image $\sigma(\mathbb{L})$ de σ est un sous-corps de $\mathbb{C}$. Comme $\mathbb{R}$ est bien sûr lui-aussi un sous-corps de $\mathbb{C}$, $\sigma(\mathbb{L}) \cap \mathbb{R}$ un sous-corps de $\sigma(\mathbb{L})$.

Notons ensuite que tout élément de $\mathbb{L}$ est de la forme $Q(\sqrt[p]{a})$, avec Q un polynôme de $\mathbb{K}[X]$ de degré au plus $p-1$ (les polynômes constants correspondant aux éléments de $\mathbb{K}$)

L'application σ est un morphisme de corps qui fixe les éléments de $\mathbb{K}$, donc pour tout élément t de $\mathbb{L}$ et pour tout polynôme Q à coefficients dans $\mathbb{K}$, on a $\sigma(Q(t)) = Q(\sigma(t))$. En particulier, σ envoie donc $\sqrt[p]{a}$ sur une racine de $X^p - a$, donc $\sigma(\sqrt[p]{a})$ est de la forme $e^{\frac{2ik\pi}{p}} \sqrt[p]{a}$, avec $1 \leq k \leq p-1$. (Si l'on avait $k = 0$, on aurait $\sigma(\sqrt[p]{a}) = \sqrt[p]{a}$, et alors σ fixerait tous les polynômes en $\sqrt[p]{a}$ à coefficients dans $\mathbb{K}$, c'est-à-dire $\mathbb{L}$ tout entier, or on a supposé σ non trivial.)

Un élément x de $\mathbb{L}$, de la forme $Q(\sqrt[p]{a})$ (avec $Q \in \mathbb{K}[X]$ de degré au plus $p-1$) est alors envoyé par σ sur $Q(e^{\frac{2ik\pi}{p}} \sqrt[p]{a})$. Et donc $\sigma(\mathbb{L})$ est en fait le corps $\mathbb{K}[e^{\frac{2ik\pi}{p}} \sqrt[p]{a}]$, en particulier c'est une extension de $\mathbb{K}$ de degré p premier. Les seuls sous-corps de $\sigma(\mathbb{L})$ contenant $\mathbb{K}$ sont donc $\mathbb{K}$ et $\sigma(\mathbb{L})$ tout entier. (Le degré d'une extension de $\mathbb{K}$ sous-corps de $\sigma(\mathbb{L})$ doit être un diviseur de p). Comme $\sigma(\mathbb{L}) \cap \mathbb{R}$ un sous-corps de $\sigma(\mathbb{L})$, on a soit $\sigma(\mathbb{L}) \cap \mathbb{R} = \sigma(\mathbb{L})$ soit $\sigma(\mathbb{L}) \cap \mathbb{R} = \mathbb{K}$.

Comme $\sigma(\mathbb{L})$ contient l'élément $e^{\frac{2ik\pi}{p}} \sqrt[p]{a}$ qui n'est pas réel, on conclut :

$$\sigma(\mathbb{L}) \cap \mathbb{R} = \mathbb{K} \qquad \square$$