Le corps de décomposition de $\Phi_{15}(X)$

D'après la formule d'inversion de Möbius :

$$\Phi_1 5(X) = \frac{(X^{15}-1)(X-1)}{(X^5-1)(X^3-1)}$$

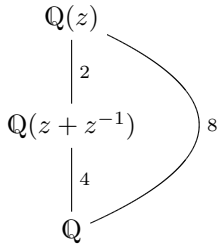
$$= \frac{X^{10}+X^5+1}{X^2+X+1}$$

$$= X^8 - X^7 + X^5 - X^4 + X^3 - X + 1 \ .$$

Soit $z := e^{2i\pi/15}$.

Soit $P(X)$ le polynôme minimal de $2\cos(2\pi/15) = z + z^{-1}$ sur $\mathbb{Q}$.

On sait que $z + z^{-1}$ est de degré $8/2 = 4$ sur $\mathbb{Q}$ car :



Donc $P(X)$ est de degré 4. Mais alors, le polynôme unitaire $X^4P(X+X^{-1}) \in \mathbb{Q}[X]$ est de degré 8 et annule z. Comme $\Phi_{15}(X)$ est le polynôme minimal de z sur $\mathbb{Q}$, on a :

$$\Phi_{15}(X) = X^4 P(X + X^{-1})$$

pour des raisons de degrés.

D'où :

$$P(X + X^{-1}) = \frac{\Phi_{15}(X)}{X^4}$$

$$= X^4 + X^{-4} - X^3 - X^{-3} + X + X^{-1} - 1 \ .$$

Or, si $n \geq 1$, $X^n + X^{-n}$ est un polynôme en $X + X^{-1}$. On vérifie en effet facilement que :

$$X^n + X^{-n} = \widetilde{T}_n(X + X^{-1})$$

où $\widetilde{T}_n(X) := 2T_n(X/2)$ avec T_n le $n-$ème polynôme de Tchebychev (rappelons que T_n est défini par la formule : $(T_n(\cos x) = \cos nx)$.

Donc :

$$P(X) = \widetilde{T}_4 - \widetilde{T}_3 + X - 1 \ .$$

Or : $T_3 = 4X^3 - 3X$ et $T_4 = 8X^4 - 8X^2 + 1$.

Donc :

$$P = X^4 - X^3 - 4X^2 + 4X + 1 \ .$$

b) Soit G le groupe de Galois de $\mathbb{Q}(z)$ sur $\mathbb{Q}$. Rappelons que l'on a un isomorphisme de groupes :

$$(\mathbb{Z}/15\mathbb{Z})^\times \xrightarrow{\simeq} G$$

$$a \longmapsto \sigma_a : z \mapsto z^a \ .$$

Comme $T_3(\cos 2\pi/15) = \cos 2\pi/5$, $\mathbb{Q}(\cos 2\pi/5) \subseteq \mathbb{Q}(\cos 2\pi/15)$.

Soit $Q(X) \in \mathbb{Q}(\cos 2\pi/5)[X]$ le polynôme minimal de $\cos 2\pi/15$ sur $\mathbb{Q}(\cos(2\pi/5))$.

Soit y une racine de Q dans $\mathbb{C}$. Il existe un $\mathbb{Q}(\cos(2\pi/5)-$plongement de $\mathbb{Q}(\cos 2\pi/15)$ dans $\mathbb{C}$: σ tel que $\sigma(x) = y$. Ce plongement se prolonge an un automorphisme $\sigma_a \in G$. Réciproquement si $\sigma_a \in G$ est un $\mathbb{Q}(\cos(2\pi/5)-$automorphisme, alors :

$$0 = Q(\cos 2\pi/15)$$

$$\Rightarrow 0 = \sigma_a(Q(\cos 2\pi/15))$$

$$\Rightarrow Q(\sigma_a(\cos 2\pi/15)) = 0 \ .$$

Donc $\sigma_a(\cos 2\pi/15)$ est une racine de Q.

Ainsi les racines de Q sont les $\sigma_a(\cos 2\pi/15)$ tels que $\sigma_a \in \mathrm{Gal}(\mathbb{Q}(z)/QQ(\cos 2\pi/5))$.

Or :

$$\sigma(\cos(2k\pi/15)) = \sigma_a(1/2(z^k + z^{-k})$$

$$= 1/2(z^{ak} + z^{-ak})$$

$$= \cos(2ak\pi/15) \ .$$

Donc $\sigma_a \in \mathrm{Gal}\mathbb{Q}(z)/QQ(\cos 2\pi/5) \Leftrightarrow a = \pm 1$ ou $\pm 4 \bmod 15$.

Ainsi $Q = (X - \cos 2\pi/15)(X - \cos 8\pi/15)$ (car Q est à racines simples).

Donc $Q = X^2 - \lambda X + \mu$ où :

$$\lambda = \cos 2\pi/15 + \cos 8\pi/15 = 2\cos \pi/3 \cos \pi/5)$$

$$\mu = \cos 2\pi/15 \cos 8\pi/15 = 1/2(\cos 2\pi/3 + \cos 2\pi/5) \ .$$

Or :

$$\cos \pi/3 = -\cos 2\pi/3 = 1/2$$

et :

$$\cos 2\pi/5 = \frac{-1+\sqrt{5}}{4}$$

$$\cos \pi/5 = -\cos 4\pi/5 = \frac{1+\sqrt{5}}{4}$$

(en particulier, $\mathbb{Q}(\cos 2\pi/5) = \mathbb{Q}(\sqrt{5})$).

Donc $Q = X^2 - \frac{1+\sqrt{5}}{4}X + \frac{-3+\sqrt{5}}{8}$.

On en déduit que :

$$\cos 2\pi/15 = \frac{1+\sqrt{5}}{8} + \frac{\sqrt{15-3\sqrt{5}}}{4} \ .$$

Le corps des nombres constructibles

On dit qu'un sous-corps K de $\mathbb{C}$ est stable par $\sqrt{\ }$ si pour tout $a \in K$, $\sqrt{a} \in K$.

On note $\mathscr{C}$ l'intersection des sous-corps de $\mathbb{C}$ stables par $\sqrt{\ }$. Le corps $\mathscr{C}$ contient $\mathbb{Q}$, mais aussi :

$$\cos 2\pi/15 = \frac{1+\sqrt{5}}{8} + \frac{\sqrt{15-3\sqrt{5}}}{4}$$

et

$$\cos 2\pi/17 =$$

$$-\frac{1}{16}+\frac{1}{16}\sqrt{17}+\frac{1}{16}\sqrt{34-2\sqrt{17}}+\frac{1}{8}\sqrt{17+3\sqrt{17}-\sqrt{34-2\sqrt{17}}-2\sqrt{34+2\sqrt{17}}}.$$

Le corps $\mathscr{C}$ est le corps des nombres complexes qui « peuvent s'expriment avec des racines carrées ». Soit $z \in \mathbb{C}$. On note $P_z \in \mathbb{Q}[X]$ son polynôme minimal (unitaire) sur $\mathbb{Q}$.

Sont équivalentes :
i) $z \in \mathscr{C}$;
ii) l'ordre du groupe de Galois de P_z sur Q est une puissance de 2 ;
iii) il existe une tour d'extensions :

$$\mathbb{Q} = K_0 \subseteq ... \subseteq K_n$$

telle que $[K_i : K_{i-1}] = 2$ pour tout $1 \leq i \leq n$ et $z \in K_n$.

*

En effet :

$$ii \Rightarrow iii :$$

soit K le corps de décomposition de P_z sur $\mathbb{Q}$. Soit G le groupe de galois de K sur $\mathbb{Q}$ *i.e.* le groupe de Galois de P_z sur $\mathbb{Q}$. Soit n tel que $|G| = 2^n$. Le groupe G possède un sous-groupe d'indice 2. Cela se montre par récurrence sur n :

c'est facile si $n = 0$ et plus généralement si G est abélien. En effet, dans ce cas, d'après la description des groupes abéliens finis, on a :

$$G \simeq \mathbb{Z}/2^{a_1}\mathbb{Z} \times ... \times \mathbb{Z}/2^{a_k}\mathbb{Z}$$

pour certains entiers $1 \leq a_1 \leq ... \leq a_k$. On voit que le groupe :

$$\mathbb{Z}/2^{a_1-1}\mathbb{Z} \times ... \times \mathbb{Z}/2^{a_k}\mathbb{Z}$$

est d'indice 2 dans $\mathbb{Z}/2^{a_1}\mathbb{Z} \times ... \times \mathbb{Z}/2^{a_k}\mathbb{Z}$.

Si G n'est pas abélien, notons Z le centre de G. En considérant l'action de G sur lui-même par conjugaison, on peut montrer que $1 \subsetneq Z \subseteq G$. On peut donc appliquer l'hypothèse de récurrence à G/Z.

Il existe un sous-groupe H de G/Z d'indice 2. Si $p : G \to G/Z$ est la surjection $g \mapsto gZ$, le sous-groupe $p^{-1}(H)$ est d'indice 2 dans G car :$G/p^{-1}(H) \simeq (G/Z)/H$.

Donc il existe un sous-groupe G_1 d'indice 2 dans G. Par récurrence, on peut construire une suite de sous-groupes :

$$G = G_0 \supseteq G_1 \supseteq ... \supseteq G_{n-1} \supseteq G_n = 1$$

tels que G_i est d'indice 2 dans G_{i-1} pour tout i.

Posons $K_i := K^{G_i}$. On a :

$$\mathbb{Q} = K_0 \subseteq K_1 \subseteq ... \subseteq K_n = K$$

avec $z \in K$ et $[K_i : K_{i-1}] = [K^{G_i} : K^{G_{i-1}}] = [K : K^{G_{i-1}}]/[K : K^{G_i}] = |G_{i-1}|/|G_i| = 2$.

D'où *iii*.

$$iii \Rightarrow i :$$

Soit $\mathbb{Q} = K_0 \subseteq ... \subseteq K_n$ comme dans l'énoncé *iii*.

Soit $x_i \in K_i \setminus K_{i-1}$. On a : $K_i = K_{i-1}(x_i)$. Soit $\Delta_i \in K_{i-1}$ le discriminant du polynôme minimal de x_i sur K_{i-1}. On a :

$$K_i = K_{i-1}(\sqrt{\Delta_i}) \ .$$

Comme $\mathscr{C}$ est stable par $\sqrt{\ }$, on montre facilement par récurrence que $\sqrt{\Delta_i} \in \mathscr{C}$ pour tout i d'où $K_n \subseteq \mathscr{C}$ et $z \in \mathscr{C}$.

$$i \Rightarrow ii :$$

Soit C l'ensemble des nombres complexes z qui vérifient ii. L'ensemble C est un sous-corps de $\mathbb{C}$. En effet, soient $x, y \in C$. Notons $x_1 = x, x_2, ..., x_m$ les conjugués de x et $y_1 = y, ..., y_n$ les conjugués de y. D'après le théorème de l'élément primitif, il existe $u, v \in \mathbb{C}$ tels que :

$$\mathbb{Q}(x_1, ..., x_m) = \mathbb{Q}(u),\ \mathbb{Q}(y_1, ..., y_n) = \mathbb{Q}(v)\ .$$

Comme $\mathbb{Q}(u)/\mathbb{Q}$ et $\mathbb{Q}(v)/\mathbb{Q}$ sont des extensions galoisiennes, l'extension $\mathbb{Q}(u, v)/\mathbb{Q}$ est aussi galoisienne (si $s : \mathbb{Q}(u, v) \to \mathbb{C}$ est un plongement, alors $s(u) \in \mathbb{Q}(u)$ et $s(v) \in \mathbb{Q}(v)$ donc $s(\mathbb{Q}(u, v)) \subseteq \mathbb{Q}(u, v)$). On a de plus $[\mathbb{Q}(u) : \mathbb{Q}] = 2^a$ et $[\mathbb{Q}(v) : \mathbb{Q}] = 2^b$ pour certains a, b entiers.

Le morphisme $\mathrm{Gal}(\mathbb{Q}(u, v)/\mathbb{Q}(v) \to \mathrm{Gal}(\mathbb{Q}(u)/\mathbb{Q})$, $s \mapsto s\big|_{\mathbb{Q}(u)}$ est clairement injectif. Donc $|\mathrm{Gal}(\mathbb{Q}(u, v) : \mathbb{Q}(v)| = [\mathbb{Q}(u, v) : \mathbb{Q}(v)]$ est une puissance de 2. On en déduit que $[\mathbb{Q}(u, v) : \mathbb{Q}] = [\mathbb{Q}(u, v) : \mathbb{Q}(v)][\mathbb{Q}(v) : \mathbb{Q}]$ est aussi une puissance de 2. En particulier, tous les éléments de $\mathbb{Q}(u, v)$ vérifient ii. Donc $\mathbb{Q}(u, v) \subseteq C$ et $\mathbb{Q}(x, y) \subseteq \mathbb{Q}(u, v) \subseteq C$.

Il est facile de voir que le corps C est stable par tout plongement de C dans $\mathbb{C}$ (*i.e.* $C/\mathbb{Q}$ est une extension normale). Le corps C est stable par la racine carrée. En effet, soit $x \in \mathbb{C}$ tel que $x^2 \in C$. Alors tous les conjugués $x_1, ..., x_n$ de x vérifient $x_i^2 \in C$. D'après le théorème de l'élément primitif, il existe $z \in C$ tel que $\mathbb{Q}(z) = \mathbb{Q}(x_1^2, ..., x_n^2)$. L'extension $\mathbb{Q}(x_1, ..., x_n)/\mathbb{Q}$ est galoisienne de degré une puissance de 2 car $\mathbb{Q}(x_1, ..., x_n)/\mathbb{Q}(z)$ est de degré une puissance de 2 tout comme $\mathbb{Q}(z)/\mathbb{Q}$. Donc $x \in \mathbb{Q}(x_1, ..., x_n) \subseteq C$.

On en conclut que $\mathscr{C} \subseteq C$ *i.e.* $i \Rightarrow ii$.

Application :

Si $z = \sqrt[3]{2}$, z est de degré 3 sur $\mathbb{Q}$. Donc son polynôme minimal a un corps de décomposition sur $\mathbb{Q}$ de degré un multiple de 3. Donc z n'est pas constructible.

Si $z = e^{2i\pi/n}$, le polynôme minimal de z sur $\mathbb{Q}$ est $\Phi_n(X)$. Son corps de décomposition est $\mathbb{Q}(z)$. Le groupe de Galois correspondant est isomorphe à $(\mathbb{Z}/n\mathbb{Z})^\times$, d'ordre $\varphi(n)$.

Or si $n = 2^a p_1^{a_1} ... p_r^{a_r}$ pour certains nombres premiers impairs distincts $p_1, ..., p_r$ et certains entiers $a \geq 0$, $a_i \geq 1$.

On a $\varphi(n) = 2^{a-1} p_1^{a_1-1}(p_1 - 1)...p_r^{a_r-1}(p_r - 1)$. C'est une puissance de 2 si et seulement si $a_i = 0$ et $p_i - 1 \in 2^{\mathbb{Z}_{>0}}$ pour tout i.

Les nombres $2^l + 1$ sont premiers seulement si l est lui-même une puissance de 2.

En effet, écrivons $l = 2^q l'$ avec $q \geq 0$ et l' impair. On a alors :

$$2^l + 1 = (2^q + 1)(1 \pm ... \pm 2^{q(l'-1)})\ .$$

Les nombres premiers de la forme :

$$F_\alpha := 2^{2^\alpha} + 1$$

sont appelés *nombres premiers de Fermat.*

Donc $z = e^{2i\pi/n}$ est constructible si et seulement si

$$n = 2^a F_1 ... F_t$$

pour un $a \geq 0$ et certains nombres premiers F_i de Fermat distincts.

Par exemple, $3, 5, 17, 257, 65537$ sont des nombres premiers de Fermat mais on ne sait pas s'il en existe d'autres.

Par exemple : F_5 n'est pas premier.