Calcul de $\cos\left(\frac{2\pi}{17}\right)$**.** Soit $\zeta = \exp\left(\frac{2\pi}{17}\right)$, de sorte que $2\cos\left(\frac{2\pi}{17}\right) = \zeta + \zeta^{-1}$. L'extension $\mathbb{Q}(\zeta)/\mathbb{Q}$ est galoisienne de groupe de Galois $(\mathbb{Z}/17\mathbb{Z})^*$ qui est cyclique, engendré par exemple par 3 [*]. On a la suite de sous-groupes (tous distingués) suivante :

$$\{1\} \subseteq \underbrace{\langle 3^8\rangle}_{=\langle -1\rangle} \subseteq \underbrace{\langle 3^4\rangle}_{=\langle 4\rangle} \subseteq \underbrace{\langle 3^2\rangle}_{=\langle 2\rangle} \subseteq \langle 3\rangle = (\mathbb{Z}/17\mathbb{Z})^*,$$

à laquelle correspond la suite d'extensions quadratiques :

$$\mathbb{Q}(\zeta) \supseteq \underbrace{\mathbb{Q}(\zeta)^{\langle 3^8\rangle}}_{=\mathbb{Q}(\zeta+\zeta^{-1})} \supseteq \underbrace{\mathbb{Q}(\zeta)^{\langle 3^4\rangle}}_{=:\mathbb{Q}(x_2)} \supseteq \underbrace{\mathbb{Q}(\zeta)^{\langle 3^2\rangle}}_{=:\mathbb{Q}(x_1)} \supseteq \mathbb{Q}.$$

Notons σ_1, σ_2 et σ_3, respectivement, les générateurs des groupes de Galois des extensions $\mathbb{Q}(x_1)/\mathbb{Q}$, $\mathbb{Q}(x_2)/\mathbb{Q}(x_1)$ et $\mathbb{Q}\left(\zeta+\zeta^{-1}\right)/\mathbb{Q}(x_2)$. Alors, pour calculer $\cos\left(\frac{2\pi}{17}\right)$, remarquons que :

- le nombre $\zeta+\zeta^{-1}$ est racine de $X^2 - \left((\zeta+\zeta^{-1}) + \sigma_3\left(\zeta+\zeta^{-1}\right)\right)X + \left(\zeta+\zeta^{-1}\right)\sigma_3\left(\zeta+\zeta^{-1}\right)$, qui est à coefficients dans $\mathbb{Q}(x_2)$ grâce à l'invariance par le groupe de Galois ;
- le nombre x_2 est racine de $X^2 - (x_2 + \sigma_2(x_2))X + x_2\sigma_2(x_2) \in \mathbb{Q}(x_1)[X]$;
- le nombre x_1 est racine de $X^2 - (x_1 + \sigma_1(x_1))X + x_1\sigma_1(x_1) \in \mathbb{Q}[X]$.

Alors, on doit choisir x_1 et x_2 sous une forme simple, pour que les quantités $x_i + \sigma_i(x_i)$, $x_i\sigma_i(x_i)$ soient faciles à calculer [†], et que les coefficients du polynôme minimal de $2\cos\left(\frac{2\pi}{17}\right)$ s'expriment simplement à l'aide de x_2. Ceci donnera une expression de $\cos\left(\frac{2\pi}{17}\right)$ à l'aide de radicaux, sommes et produits d'éléments de $\mathbb{Q}(x_2)$, puis $\mathbb{Q}(x_1)$, puis $\mathbb{Q}$.

Il est naturel de prendre pour x_1 et x_2 une moyenne de ζ par les éléments du groupe de Galois de $\mathbb{Q}(\zeta)/\mathbb{Q}(\zeta)^{\langle 3^2\rangle}$ et $\mathbb{Q}(\zeta)/\mathbb{Q}(\zeta)^{\langle 3^4\rangle}$ respectivement, puisque ces moyennes seront par construction invariantes sous l'action des groupes de Galois voulus. Or ces groupes de Galois sont $\langle 3^2\rangle$ et $\langle 3^4\rangle$ respectivement ; choisissons donc :

$$x_1 = \sum_{k=0}^{7} \zeta^{3^{2k}} = \left(\zeta+\zeta^{-1}\right) + \left(\zeta^2+\zeta^{-2}\right) + \left(\zeta^4+\zeta^{-4}\right) + \left(\zeta^8+\zeta^{-8}\right),$$

$$x_2 = \sum_{k=0}^{3} \zeta^{3^{4k}} = \left(\zeta+\zeta^{-1}\right) + \left(\zeta^4+\zeta^{-4}\right)$$

(écrire les groupes de Galois comme engendrés par des puissances de 3 permettra de mieux apprécier l'action de $\langle 3\rangle$ sur x_1 et x_2, même s'il semble plus agréable pour le calcul d'utiliser $\langle 2\rangle$ et $\langle 4\rangle$).

Passons au calcul des quantités apparaissant dans les polynômes annulateurs ci-dessus ; σ_3 est un générateur de :

$$\mathrm{Gal}(\mathbb{Q}(\zeta+\zeta^{-1})/\mathbb{Q}(x_2)) \simeq \frac{\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}(x_2))}{\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}(\zeta+\zeta^{-1}))} \simeq \langle 3^4\rangle/\langle 3^8\rangle = \langle 1,3^4\rangle,$$

donc $\sigma_3(\zeta) = \zeta^{3^4}$, et de même $\sigma_2(\zeta) = \zeta^{3^2}$, puis $\sigma_1(\zeta) = \zeta^3$. Il reste à calculer les coefficients des polynômes annulateurs ci-dessus. Les coefficients devant X sont très simples à obtenir, car :

$$(\zeta+\zeta^{-1}) + \sigma_3(\zeta+\zeta^{-1}) = x_2, \qquad x_2 + \sigma_2(x_2) = x_1, \text{ et}$$

$$x_1 + \sigma_1(x_1) = \sum_{g\in\langle 3^2\rangle} \zeta^g + \sum_{g\in\langle 3^2\rangle} \zeta^{3g} = \sum_{k\in(\mathbb{Z}/17\mathbb{Z})^*} \zeta^k = \sum_{k\in\mathbb{Z}/17\mathbb{Z}} \zeta^k - 1 = -1,$$

puisqu'en effet, $(\mathbb{Z}/17\mathbb{Z})^* = \langle 3\rangle = \bigsqcup_{h\in\frac{\langle 3\rangle}{\langle 3^2\rangle}} h\langle 3^2\rangle = \langle 3^2\rangle \bigsqcup 3\langle 3^2\rangle$. Enfin, les coefficients constants sont, d'après un calcul lourd mais sans mystère :

$$x_1\sigma_1(x_1) = 4\sum_{k\in(\mathbb{Z}/17\mathbb{Z})^*} \zeta^k = -4, \qquad x_2\sigma_2(x_2) = \sum_{k\in(\mathbb{Z}/17\mathbb{Z})^*} \zeta^k = -1, \text{ et :}$$

$$(\zeta+\zeta^{-1})\sigma_3(\zeta+\zeta^{-1}) = (\zeta+\zeta^{-1})(\zeta^{-4}+\zeta^4) = \frac{1}{2}\left(x_2^2 - \left(\zeta+\zeta^{-1}\right)^2 - \left(\zeta^4+\zeta^{-4}\right)^2\right) = \frac{1}{2}\left(x_2^2 - (x_1 - x_2) - 4\right).$$

Pour résumer,

$$x_1^2 + x_1 - 4 = 0 \Longrightarrow x_1 = \frac{-1\pm\sqrt{17}}{2}, \qquad x_2^2 - x_1x_2 - 1 = 0 \Longrightarrow x_2 = \frac{x_1 \pm \sqrt{x_1^2+4}}{2} = \frac{x_1 \pm \sqrt{8-x_1}}{2},$$

∗. Comme il a $\varphi(16) = 8$ générateurs, et que ± 1, ± 2, $\pm 2^2$ et $\pm 2^3$ sont d'ordres au plus 8, donc sont les $16 - 8 = 8$ éléments qui ne sont pas générateurs, tout autre élément engendre ce groupe.

†. On reconnaît les applications traces et normes.

et :

$$(\zeta+\zeta^{-1})^2 - x_2(\zeta+\zeta^{-1}) + \frac{1}{2}\left(x_2^2 - (x_1-x_2) - 4\right) = 0 \Longrightarrow \zeta+\zeta^{-1} = \frac{x_2 \pm \sqrt{8 - x_2^2 + 2(x_1-x_2)}}{2}$$
$$= \frac{x_2 \pm \sqrt{7 - x_1x_2 + 2(x_1-x_2)}}{2},$$

et il faut lever l'indétermination sur les signes pour obtenir $\cos\left(\frac{2\pi}{17}\right)$ ‡. Une façon de procéder est de remarquer qu'on obtient tous les conjugués de $\zeta+\zeta^{-1}$ en variant les différents signes, or $2\cos\left(\frac{2\pi}{17}\right)$ est celui correspondant à la plus grande partie réelle, donc on choisit les signes de sorte à maximiser la valeur absolue. Bref :

$$4\cos\left(\frac{2\pi}{17}\right) = \frac{\sqrt{17}-1+\sqrt{34-2\sqrt{17}}}{4} + \frac{\sqrt{68+12\sqrt{17}-8\sqrt{34-2\sqrt{17}}-2\sqrt{34-2\sqrt{17}}(\sqrt{17}-1)}}{4}.$$

Remarque. Si on remarque que x_1 est une somme indexée par les carrés non nuls de $\mathbb{Z}/17\mathbb{Z}$, alors son calcul devient aisé §. En effet,

$$\left|\sum_{n\in\mathbb{Z}/17\mathbb{Z}} \zeta^{n^2}\right|^2 = \sum_{m\in\mathbb{Z}/17\mathbb{Z}}\sum_{n\in\mathbb{Z}/17\mathbb{Z}} \zeta^{n^2-m^2} = \sum_{m\in\mathbb{Z}/17\mathbb{Z}}\sum_{n\in\mathbb{Z}/17\mathbb{Z}} \zeta^{(n-m)(m+n)} = \sum_{m\in\mathbb{Z}/17\mathbb{Z}}\sum_{n\in\mathbb{Z}/17\mathbb{Z}} \zeta^{-2mn},$$

car $n \mapsto m+n$ est une permutation de $\mathbb{Z}/17\mathbb{Z}$ pour tout m fixé, et

$$\sum_{n\in\mathbb{Z}/17\mathbb{Z}} \zeta^{-2mn} = \begin{cases} 17 & \text{si } -2m \equiv 0 \bmod 17 \\ 0 & \text{sinon} \end{cases} = \begin{cases} 17 & \text{si } m \equiv 0 \bmod 17 \\ 0 & \text{sinon,} \end{cases}$$

donc : $\left|\sum_{n\in\mathbb{Z}/17\mathbb{Z}} \zeta^{n^2}\right|^2 = 17$. Or $\sum_{n\in\mathbb{Z}/17\mathbb{Z}} \zeta^{n^2}$ est un réel, car $n \mapsto -n$ permute les carrés de $\mathbb{Z}/17\mathbb{Z}$ (cela tient au fait que $-1 = (3^4)^2$ est un carré de $\mathbb{Z}/17\mathbb{Z}$) et alors cette somme est invariante par $\zeta \mapsto \zeta^{-1} = \bar{\zeta}$. Donc : $\sum_{n\in\mathbb{Z}/17\mathbb{Z}} \zeta^{n^2} = \pm\sqrt{17}$, et on en déduit que $x_1 = \frac{\pm\sqrt{17}-1}{2}$ (l'analyse de Fourier permet aussi de calculer cette somme directement et lève l'indétermination sur le signe).

‡. Cela ne peut pas se faire par la théorie de Galois, puisque dans son principe même elle ne permet pas de distinguer une racine carrée de son opposé : toute relation algébrique vérifiée par une racine carrée $\sqrt{a}$ l'est aussi par $\sigma(\sqrt{a}) = -\sqrt{a}$ (c'est précisément le but de la théorie de Galois de formaliser l'étude de ce genre de symétrie entre racines d'un polynôme !). Par ailleurs, Galois appelait cette théorie (bientôt éponyme) la *théorie de l'ambiguïté*, pour cette raison.

§. Remarquer cela n'a rien d'exceptionnel : on sait d'une part que $(\mathbb{Z}/17\mathbb{Z})^*$ est cyclique, donc admet un unique sous-groupe de tout ordre possible, et d'autre part que l'ensemble des carrés de $(\mathbb{Z}/p\mathbb{Z})^*$ est un sous-groupe d'indice 2 pour tout p premier impair (parce que $x \mapsto x^2$ est un morphisme de groupes dont le noyau $\{\pm 1\}$ contient deux éléments). Alors, $\langle 3^2\rangle$ étant d'indice 2, il est le sous-groupe des carrés de $(\mathbb{Z}/17\mathbb{Z})^*$. Ou, plus concrètement : une puissance paire de 3 est évidemment un carré, et une puissance impaire de 3 n'en est pas un (sinon 3 serait un carré, et serait d'ordre au plus 8). Comme 3 engendre le groupe, on en déduit que $\langle 3^2\rangle$ contient tous les carrés de $(\mathbb{Z}/17\mathbb{Z})^*$.