THE SEVENTEENTH ROOT OF UNITY VIA QUADRATICS

1. The Environment

Let $p = 17$, and let

$$\zeta = \zeta_{17} = e^{2\pi i/17}.$$

The field $\mathbb{Z}/17\mathbb{Z}$ has multiplicative group

$$G = (\mathbb{Z}/17\mathbb{Z})^\times = \langle 3 \rangle = \{1, 3, 9, 10, 13, 5, 15, 11, 16, 14, 8, 7, 4, 12, 2, 6\}.$$

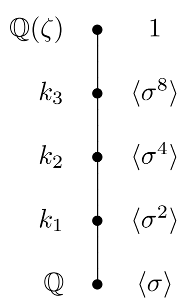
Consequently the automorphism

$$\sigma : \mathbb{Q}(\zeta_{17}) \longrightarrow \mathbb{Q}(\zeta_{17}), \quad \zeta \longmapsto \zeta^3$$

has order 16. The subgroups of the cyclic group $\langle\sigma\rangle$ are

$$\begin{aligned}
&\langle \sigma : \zeta \longmapsto \zeta^3 \rangle, && \text{of order } 16,\\
&\langle \sigma^2 : \zeta \longmapsto \zeta^9 \rangle, && \text{of order } 8,\\
&\langle \sigma^4 : \zeta \longmapsto \zeta^{13} \rangle, && \text{of order } 4,\\
&\langle \sigma^8 : \zeta \longmapsto \zeta^{16} \rangle, && \text{of order } 2,\\
&\langle \sigma^{16} = 1 \rangle, && \text{of order } 1.
\end{aligned}$$

Corresponding to the chain of subgroups there is a tower of fields



Following Gauss, this writeup shows how to compute ζ by a succession of square roots, by successively constructing the fields on the left side of the diagram.

2. Constructing the First Extension Field

Let

$$r_1 = \zeta + \zeta^{\sigma^2} + \zeta^{\sigma^4} + \zeta^{\sigma^6} + \zeta^{\sigma^8} + \zeta^{\sigma^{10}} + \zeta^{\sigma^{12}} + \zeta^{\sigma^{14}}.$$

Then r_1 is σ^2-invariant but not σ-invariant, so that the quadratic polynomial

$$f_1(X) = (X - r_1)(X - r_1^\sigma)$$

is σ-invariant. That is,

$$f_1(X) = X^2 + b_1 X + c_1 \in \mathbb{Q}[X],$$

where

$$b_1 = -r_1 - r_1^\sigma = -\sum_{j=1}^{16} \zeta^{\sigma^j} = -\sum_{j=1}^{16} \zeta^j = 1,$$

and

$$c_1 = r_1 r_1^\sigma.$$

Although c_1 can be computed directly by hand, proceed instead by defining a quadratic character of G, a homomorphism of G whose square is the trivial homomorphism,

$$\chi : G \longrightarrow \{\pm 1\}, \quad \chi(3^e) = (-1)^e.$$

The *Gauss sum* associated to ζ and χ is

$$\tau = \sum_{j \in G} \chi(j)\zeta^j,$$

or,

$$\begin{aligned}\tau = \zeta + \zeta^{\sigma^2} + \zeta^{\sigma^4} + \zeta^{\sigma^6} + \zeta^{\sigma^8} + \zeta^{\sigma^{10}} + \zeta^{\sigma^{12}} + \zeta^{\sigma^{14}} \\ - \zeta^{\sigma} - \zeta^{\sigma^3} - \zeta^{\sigma^5} - \zeta^{\sigma^7} - \zeta^{\sigma^9} - \zeta^{\sigma^{11}} - \zeta^{\sigma^{13}} - \zeta^{\sigma^{15}}.\end{aligned}$$

Thus

$$r_1 - r_1^\sigma = \tau, \qquad r_1 + r_1^\sigma = -1,$$

so that

$$r_1 = \frac{\tau - 1}{2}, \qquad r_1^\sigma = -\frac{\tau + 1}{2},$$

and consequently

$$r_1 r_1^\sigma = -\frac{\tau^2 - 1}{4}.$$

The Gauss sum is symmetrized so that its square is easy to compute,

$$\begin{aligned}\tau_1^2 &= \sum_{j \in G} \sum_{k \in G} \chi(jk)\zeta^{j+k} \\ &= \sum_{j \in G} \sum_{k \in G} \chi(j^2 k)\zeta^{j(1+k)} && \text{replacing } k \text{ by } jk \\ &= \sum_{k \in G} \chi(k) \sum_{j \in G} \zeta^{(1+k)j} && \text{by the properties of } \chi \\ &= 16\chi(-1) - \sum_{k \neq -1} \chi(k) && \text{evaluating the geometric inner sum} \\ &= 17 && \text{since } \chi(-1) = 1 \text{ and } \sum_{k \in G} \chi(k) = 0.\end{aligned}$$

It follows that

$$r_1 r_1^\sigma = -\frac{17 - 1}{4} = -4.$$

In sum, the polynomial

$$f_1(X) = X^2 + X - 4 \in \mathbb{Q}[X]$$

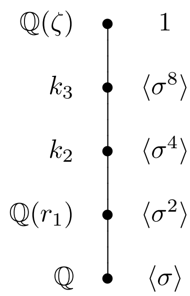
has roots

$$r_1 = \frac{-1 + \sqrt{17}}{2}, \qquad r_1^\sigma = \frac{-1 - \sqrt{17}}{2}.$$

(Since

$$\begin{aligned} r_1 &= \zeta + \zeta^9 + \zeta^{13} + \zeta^{15} + \zeta^{16} + \zeta^8 + \zeta^4 + \zeta^2 \\ r_1^\sigma &= \zeta^3 + \zeta^{10} + \zeta^5 + \zeta^{11} + \zeta^{14} + \zeta^7 + \zeta^{12} + \zeta^6, \end{aligned}$$

comparing which powers of ζ occur in r and in r^σ shows that r lies farther to the right.) Thus we have climbed the first step up the tower of fields corresponding to the subgroup of the Galois group,



Since $r_1 + r_1^\sigma = -1$, the field $\mathbb{Q}(r_1)$ is in fact $\mathbb{Q}(r_1, r_1^\sigma)$.

3. Constructing the Second Extension Field

Let

$$r_2 = \zeta + \zeta^{\sigma^4} + \zeta^{\sigma^8} + \zeta^{\sigma^{12}}.$$

Then r_2 is σ^4-invariant but not σ^2-invariant, so that the quadratic polynomial

$$f_2(X) = (X - r_2)(X - r_2^{\sigma^2})$$

is σ^2-invariant. That is,

$$f_2(X) = X^2 + b_2 X + c_2 \in \mathbb{Q}(r_1)[X],$$

where

$$b_2 = -r_2 - r_2^{\sigma^2} = -r_1,$$

and

$$c_2 = r_2 r_2^{\sigma^2}.$$

Compute that

$$\begin{aligned} r_2 &= \zeta + \zeta^4 + \zeta^{13} + \zeta^{16} = 2(\cos(2\pi/17) + \cos(8\pi/17)), \\ r_2^{\sigma^2} &= \zeta^2 + \zeta^8 + \zeta^9 + \zeta^{15} = 2(\cos(4\pi/17) + \cos(16\pi/17)). \end{aligned}$$

Thus

$$\begin{aligned} \tfrac{1}{4} r_2 r_2^{\sigma^2} &= \cos(2\pi/17)\cos(4\pi/17) + \cos(2\pi/17)\cos(16\pi/17) \\ &\quad + \cos(8\pi/17)\cos(4\pi/17) + \cos(8\pi/17)\cos(16\pi/17), \end{aligned}$$

and so the trigonometry identity $2\cos a \cos b = \cos(a+b) + \cos(a-b)$ gives

$$\begin{aligned} \tfrac{1}{2} r_2 r_2^{\sigma^2} &= \cos(6\pi/17) + \cos(2\pi/17) + \cos(16\pi/17) + \cos(14\pi/17) \\ &\quad + \cos(12\pi/17) + \cos(4\pi/17) + \cos(10\pi/17) + \cos(8\pi/17) \\ &= -1/2. \end{aligned}$$

In sum, the polynomial

$$f_2(X) = X^2 - r_1 X - 1 \in \mathbb{Q}(r_1)[X]$$

has roots

$$r_2 = \frac{r_1 + \sqrt{r_1^2 + 4}}{2}, \qquad r_2^{\sigma^2} = \frac{r_1 - \sqrt{r_1^2 + 4}}{2}.$$

(Again it is easy to see which is larger.)

Since $r_2 + r_2^\sigma = r_1$, our choice for the second field can be written in abbreviated form, naturally containing the other polynomial roots as well,

$$k_2 = \mathbb{Q}(r_1, r_2) = \mathbb{Q}(r_1, r_1^\sigma, r_2, r_2^{\sigma^2}).$$

We have not yet considered another pair of σ^4-invariants that are exchanged by σ^2,

$$\begin{aligned} r_2^\sigma &= \zeta^3 + \zeta^5 + \zeta^{12} + \zeta^{14}, \\ r_2^{\sigma^3} &= \zeta^6 + \zeta^7 + \zeta^{10} + \zeta^{11}. \end{aligned}$$

They satisfy the quadratic polynomial

$$f_2^\sigma(X) = X^2 - r_1^\sigma X - 1.$$

However, r_2^σ and $r_2^{\sigma^2}$ can be expressed in terms of r_1 and r_2. Since $r_2^\sigma + r_2^{\sigma^2} = r_1^\sigma = -1 - r_1$, it suffices to consider r_2^σ. To see this, compute (skipping many steps) that

$$r_1 r_2 = 2 - r_2 + r_2^\sigma - r_2^{\sigma^3} = 3 - r_2 + 2r_2^\sigma + r_1,$$

so that

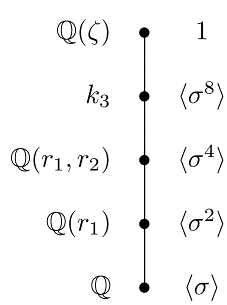
$$2r_2^\sigma = r_1 r_2 - r_1 + r_2 - 3.$$

(Of course we also have the formulas

$$r_2^\sigma = \frac{r_1^\sigma + \sqrt{(r_1^\sigma)^2 + 4}}{2}, \qquad r_2^{\sigma^3} = \frac{r_1^\sigma - \sqrt{(r_1^\sigma)^2 + 4}}{2},$$

but besides costing us another square root computationally, the formulas don't show that r_2^σ and $r_2^{\sigma^3}$ lie in the field generated by r_1 and r_2.)

Now we have climbed the second step up the tower of fields,



And here the new field is in fact $\mathbb{Q}(r_1, r_1^\sigma, r_2, r_2^\sigma, r_2^{\sigma^2}, r_2^{\sigma^3})$.

4. Constructing the Third Extension Field

Let

$$r_3 = \zeta + \zeta^{\sigma^8}.$$

Then r_3 is σ^8-invariant but not σ^4-invariant, so that the quadratic polynomial

$$f_3(X) = (X - r_3)(X - r_3^{\sigma^4})$$

is σ^4-invariant. That is,

$$f_3(X) = X^2 + b_3X + c_3 \in \mathbb{Q}(r_1, r_2)[X],$$

where

$$b_3 = -r_3 - r_3^{\sigma^4} = -r_2,$$

and

$$c_3 = r_3r_3^{\sigma^4} = (\zeta + \zeta^{16})(\zeta^4 + \zeta^{13}) = \zeta^3 + \zeta^5 + \zeta^{12} + \zeta^{14} = r_2^{\sigma}.$$

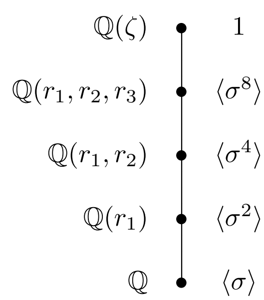
In sum, the polynomial

$$f_3(X) = X^2 - r_2X + r_2^{\sigma} \in \mathbb{Q}(r_1, r_2)[X]$$

has roots

$$r_3 = \frac{r_2 + \sqrt{r_2^2 - 4r_2^{\sigma}}}{2}, \qquad r_3^{\sigma^4} = \frac{r_2 - \sqrt{r_2^2 - 4r_2^{\sigma}}}{2}$$

(again it is easy to see which is larger). We have climbed the third step,



5. The Endgame

Finally, ζ and $\zeta^{\sigma^8} = \zeta^{-1}$ satisfy the polynomial

$$f_4(X) = X^2 - r_3X + 1.$$

Specifically,

$$\zeta = \frac{r_3 + \sqrt{r_3^2 - 4}}{2}, \qquad \zeta^{-1} = \frac{r_3 - \sqrt{r_3^2 - 4}}{2}.$$

Only at this last step do we take an imaginary square root. In sum, we consecutively compute

$$r_1 = \frac{-1 + \sqrt{17}}{2},$$

$$r_2 = \frac{r_1 + \sqrt{r_1^2 + 4}}{2},$$

$$r_3 = \frac{r_2 + \sqrt{r_2^2 - 4r_2^{\sigma}}}{2},$$

$$\zeta_{17} = \frac{r_3 + \sqrt{r_3^2 - 4}}{2}.$$