Math 121. Construction of a regular 17-gon

1. Introduction

Let $K = \mathbf{Q}(\zeta)$ with ζ a primitive 17th root of unity, so ζ has minimal polynomial over $\mathbf{Q}$ equal to $\Phi_{17} = X^{16} + X^{15} + \cdots + X + 1 \in \mathbf{Q}[X]$ and $G := \mathrm{Gal}(K/\mathbf{Q}) = (\mathbf{Z}/17\mathbf{Z})^\times$. In particular, the 16 elements

$$\{\zeta, \ldots, \zeta^{16}\} = \{\zeta^j\}_{1 \le j < 17}$$

are *linearly independent* over $\mathbf{Q}$, as any nontrivial $\mathbf{Q}$-linear dependence relation would (upon division by ζ) give a nontrivial polynomial relation for ζ over $\mathbf{Q}$ of degree $< 16 = \deg \Phi_{17}$, a contradiction.

Let $\sigma \in G$ correspond to $3 \in (\mathbf{Z}/17\mathbf{Z})^\times$ (so $\sigma(z) = z^3$ for all 17th roots of unity $z \in K$). This is a generator. Indeed, we just need to check that $\sigma^8 \neq 1$ (as the order of any proper subgroup of a cyclic group of order 16 must divide 8), or equivalently that $3^8 \not\equiv 1 \bmod 17$. Since $3^2 = 9$, so $3^4 = 81 \equiv -4 \bmod 17$, we have $3^8 \equiv 16 \equiv -1 \bmod 17$.

Thus, we get a chain of subgroups $G_i = \langle \sigma^{2^i} \rangle$ for $0 \le i \le 4$, so $G_0 = G$, $G_4 = 1$, and G_j has index 2 in G_{j-1} for $1 \le j \le 4$, Explicitly,

$$G_0 = G, G_1 = \langle 9 \rangle, G_2 = \langle -4 \rangle, G_3 = \langle -1 \rangle, G_4 = 1.$$

Let $K_i = K^{G_i}$, so $K_0 = \mathbf{Q}$, $K_4 = K$, and $[K_i : K_{i-1}] = 2$ for $1 \le i \le 4$. In particular, as we saw in class, $K_3 = K^{\langle -1 \rangle} = \mathbf{Q}(\zeta + 1/\zeta) = \mathbf{Q}(\cos(2\pi/17))$.

Our aim in this handout is to make *explicit* the fields K_1, K_2, K_3 in the sense that we find

- an explicit $x_i \in K_i \subset \mathbf{Q}(\zeta)$ for $0 \le i \le 3$ such that $K_i = \mathbf{Q}(x_i)$ and $x_3 = \zeta + 1/\zeta$,
- the quadratic minimal polynomial $f_i \in K_{i-1}[T] = \mathbf{Q}(x_{i-1})[T]$ for x_i over K_{i-1} $(1 \le i \le 3)$,
- for the embedding $K_3 \hookrightarrow \mathbf{R}$ carrying $\zeta + 1/\zeta$ to $2\cos(2\pi/17)$ (induced by $\iota : K = K_4 \hookrightarrow \mathbf{C}$ carrying ζ to $e^{\pm 2\pi i/17}$), the exact sign in the quadratic formula expressing x_i in terms of elements of $\mathbf{Q}(x_{i-1})$ with square roots in $\mathbf{R}$.

In this way, we get an explicit formula for x_3 via iterated square roots inside $\mathbf{R}$, thereby providing a construction of a regular 17-gon via straightedge and compass. Exercise 14 in §14.5 of the course text gives another description of this calculation, and the explicit formula on page 602 of the course text looks nicer than the one we will obtain. (There is no inconsistency, as there are numerous ways to give an iterated quadratic tower "formula" for any specific element of K_3.)

2. The primitive elements

To find an explicit primitive element $x_i \in K_i = K^{G_i}$ over $\mathbf{Q}$ for $0 \le i \le 3$, we use the "sum over an orbit" method: let's define $x_i = \sum_{g \in G_i} g(\zeta)$ and hope for the best. By design certainly x_i is G_i-invariant, so $x_i \in K_i$. For example,

$$x_0 = \sum_{g \in G} g(\zeta) = \sum_{j=0}^{16} \zeta^j = \Phi_{17}(\zeta) - 1 = -1 \in \mathbf{Q} = K_0.$$

Also, $x_3 = \sum_{g \in G_3} g(\zeta) = \zeta + \zeta^{-1}$. The cases of x_1 and x_2 are more interesting, and we'll make them explicit in a moment. But first let's show by the Fundamental Theorem that the inclusion $\mathbf{Q}(x_i) \subset K_i$ is an equality for all $0 \le i \le 3$.

It suffices (why?) to check that if $\gamma \notin G_i$ then $\gamma(x_i) \neq x_i$. (In view of the cyclicity of G, it suffices to check this for just a single $\gamma \in G_{i-1} - G_i$.) But $\gamma(x_i) = \sum_{g \in G_i} \gamma(g(\zeta))$ whereas $x_i = \sum_{g \in G_i} g(\zeta)$,

so if $\gamma(x_i) = x_i$ then

$$\sum_{g \in \gamma G_i} g(\zeta) - \sum_{g \in G_i} g(\zeta) = 0. \tag{1}$$

But γG_i and G_i are *disjoint* subsets of $G = (\mathbf{Z}/17\mathbf{Z})^\times$ since G_i is a subgroup and $\gamma \notin G_i$. Since the G-orbit $\{\zeta, \zeta^2, \ldots, \zeta^{16}\} = \{\zeta^j\}_{1 \le j \le 16}$ is *linearly independent* over $\mathbf{Q}$, a relation such as (1) is impossible (and more generally, *no* difference among sums of two disjoint subsets of this G-orbit can vanish). Hence, we have proved that $\mathbf{Q}(x_i) = K_i$ for all i.

Explicitly, since $G_1 = \{1, \sigma^2, \sigma^4, \sigma^6, \ldots, \sigma^{14}\} = \{1, 9 = -8, -4, -2, -1, 8, 4, 2\}$, we have

$$\begin{aligned} x_1 &= \zeta + \sigma^2(\zeta) + \sigma^4(\zeta) + \sigma^6(\zeta) + \cdots + \sigma^{14}(\zeta) \\ &= \zeta + \zeta^{-8} + \zeta^{-4} + \zeta^{-2} + \zeta^{-1} + \zeta^8 + \zeta^4 + \zeta^2 \\ &= (\zeta + \zeta^{-1}) + (\zeta^2 + \zeta^{-2}) + (\zeta^4 + \zeta^{-4}) + (\zeta^8 + \zeta^{-8}). \end{aligned}$$

Hence, for $\theta = 2\pi/17$, the embedding $\iota : K \hookrightarrow \mathbf{C}$ via $\zeta \mapsto e^{\pm 2\pi i/17} = e^{\pm i\theta}$ carries x_1 to

$$2(\cos\theta + \cos(2\theta) + \cos(4\theta) + \cos(8\theta)) \tag{2}$$

which is *positive* (proof: $\cos(\theta), \cos(2\theta) > 1/\sqrt{2}$ since $2/17 < 1/8$, and $\cos(4\theta) > 0$ since $4/17 < 1/4$). We will use this positivity to identity $\iota(x_1)$ as an explicit quadratic irrationality over $\mathbf{Q}$ inside $\mathbf{R}$ below. (Recall that $[K_1 : \mathbf{Q}] = [K_1 : K_0] = 2$, so the field $K_1 = \mathbf{Q}(x_1)$ is real quadratic.)

Likewise, since $G_2 = \{1, \sigma^4, \sigma^8, \sigma^{12}\} = \{1, -4, -1, 4\}$, we have

$$x_2 = \zeta + \sigma^4(\zeta) + \sigma^8(\zeta) + \sigma^{12}(\zeta) = \zeta + \zeta^{-4} + \zeta^{-1} + \zeta^4 = (\zeta + \zeta^{-1}) + (\zeta^4 + \zeta^{-4}).$$

Hence, the embedding ι as above carries x_2 to $2(\cos\theta + \cos(4\theta))$. The nontrivial Galois conjugate for x_2 over K_1 is $\sigma^2(x_2) = (\zeta^2 + \zeta^{-2}) + (\zeta^8 + \zeta^{-8})$ since σ^2 generates $\mathrm{Gal}(K_2/K_1) = \langle\sigma^2\rangle/\langle\sigma^4\rangle$ (or more explicitly, $\{2, -2, 8, -8\} = G_1 - G_2$), so ι carries the K_1-conjugate $\sigma^2(x_2)$ to $2(\cos(2\theta) + \cos(8\theta))$. But for $\theta = 2\pi/17$ we have seen $\cos\theta, \cos(4\theta) > 0$, so

$$\cos\theta + \cos(4\theta) > 0 > \cos(2\theta) + \cos(8\theta)$$

(since $(1/2) - 8/17 < 2/17$, or stare at a 17-gon). Hence, once we compute the minimal polynomial f_2 for x_2 over $\mathbf{Q}(x_1) = K_1$, $\iota(x_2)$ must be the *larger* root of $\iota(f_2) \in \mathbf{R}[T]$; i.e., $\iota(x_2)$ is given by the *positive* square root in the quadratic formula for the roots of $\iota(f_2) \in \iota(K_1)[T] \subset \mathbf{R}[T]$ in $\mathbf{R}$.

3. Quadratic polynomials

Now we compute the minimal quadratic polynomial $f_i \in K_{i-1}[T]$ for x_i with $1 \le i \le 3$. Since G_{i-1} is generated by $\sigma^{2^{i-1}}$, so

$$\mathrm{Gal}(K_i/K_{i-1}) = G_{i-1}/G_i = \langle\sigma^{2^{i-1}}\rangle/\langle\sigma^{2^i}\rangle,$$

this quotient group of order 2 is represented by $\{1, \sigma^{2^{i-1}}\}$. Hence, the $\mathrm{Gal}(K_i/K_{i-1})$-orbit of the primitive generator x_i of K_i over K_{i-1} is $\{x_i, \sigma^{2^{i-1}}(x_i)\}$. It follows that

$$f_i(T) = (T - x_i)(T - \sigma^{2^{i-1}}(x_i)) = T^2 - (x_i + \sigma^{2^{i-1}}(x_i))T + x_i\sigma^{2^{i-1}}(x_i) \in K_{i-1}[T].$$

By definition, x_i is the sum over the G_i-orbit of ζ, so $\sigma^{2^{i-1}}(x_i)$ is the sum over the orbit of ζ under the subset $\sigma^{2^{i-1}}G_i \subset G_{i-1}$ that is *exactly* the nontrivial G_i-coset in G_{i-1}, Hence,

$$x_i + \sigma^{2^{i-1}}(x_i) = \sum_{g \in G_{i-1}} g(\zeta) = x_{i-1},$$

so

$$f_i = T^2 - x_{i-1}T + x_i\sigma^{2^{i-1}}(x_i) \in K_{i-1}[T].$$

We need to make the constant term explicit in terms of the description $\mathbf{Q}(x_{i-1})$ of K_{i-1} (for $1 \leq i \leq 3$) in order to give a "quadratic formula" expression for x_i over $\mathbf{Q}(x_{i-1})$ (and then bring in positivity work in $\mathbf{R}$ from the previous section to pin down the correct sign in the quadratic formula when working with the embedding $\iota : K \to \mathbf{C}$ sending ζ to $e^{\pm 2\pi i/17} = e^{\pm i\theta}$).

We have already seen that $x_0 = -1$, so

$$f_1 = T^2 + T + (x_1\sigma(x_1)) \in K_0[T] = \mathbf{Q}[T].$$

Hence, we have to identity $x_1\sigma(x_1)$ as an explicit rational number. It was seen above that

$$x_1 = \zeta + \zeta^{-8} + \zeta^{-4} + \zeta^{-2} + \zeta^{-1} + \zeta^8 + \zeta^4 + \zeta^2,$$

so since $\sigma(\zeta) = \zeta^3$ we see that $\sigma(x_1)$ is given by multiplying these exponents by 3. That is,

$$\sigma(x_1) = \zeta^3 + \zeta^{-7} + \zeta^5 + \zeta^{-6} + \zeta^{-3} + \zeta^7 + \zeta^{-5}.$$

Now expand the product $x_1\sigma(x_1)$ of two 8-fold sums as a sum of $8 \times 8 = 64$ terms by massive application of the distributive law. This yields by a miracle (check!) that each ζ^j $(1 \leq j \leq 16)$ appears exactly 4 times, so

$$x_1\sigma(x_1) = 4(\zeta + \zeta^2 + \zeta^3 + \cdots + \zeta^{16}) = -4.$$

To summarize, $f_1 = T^2 + T - 4$, so its root $\iota(x_1)$ in $\mathbf{R}$ has the form $(-1 \pm \sqrt{17})/2$ for a sign to be determined. (In particular, the unique quadratic subfield K_1 of $\mathbf{Q}(\zeta)$ is $\mathbf{Q}(\sqrt{17})$.) Our positivity work with cosines showed that $\iota(x_1) > 0$, so

$$\iota(x_1) = (-1 + \sqrt{17})/2$$

(which numerically agrees with the expression in (2), as it must).

Moving on to $f_2 = T^2 - x_1T + (x_2\sigma^2(x_2)) \in K_1[T]$, since $\sigma^2(\zeta) = \zeta^9 = \zeta^{-8}$ we deduce from the formula

$$x_2 = \zeta + \zeta^{-4} + \zeta^{-1} + \zeta^4$$

that $\sigma^2(x_2) = \zeta^{-8} + \zeta^{-2} + \zeta^8 + \zeta^2$. Thus, expanding the product $x_2\sigma^2(x_2)$ of two 4-fold sums as a sum of $4 \times 4 = 16$ terms yields

$$x_2\sigma^2(x_2) = \zeta + \zeta^2 + \zeta^3 + \cdots + \zeta^{16} = -1.$$

In other words, $f_2 = T^2 - x_1T - 1$, so by the quadratic formula

$$x_2 = \frac{x_1 \pm \sqrt{x_1^2 + 4}}{2}.$$

But recall from the previous section that under $\iota : K \to \mathbf{C}$ (carrying K_3 onto $\mathbf{Q}(\cos(2\pi/17)) \subset \mathbf{R}$), the root $\iota(x_2)$ of $\iota(f_2) \in \mathbf{R}[T]$ is the *larger* of the two roots (the other root being $\iota(\sigma^2(x_2))$). Hence, $\iota(x_2)$ is given by the quadratic formula using the positive square root:

$$\iota(x_2) = \frac{\iota(x_1) + \sqrt{\iota(x_1)^2 + 4}}{2}$$

in $\mathbf{R}$ with $\iota(x_1) = (-1 + \sqrt{17})/2$.

Finally, we come to the crux of the matter: identifying the constant term of

$$f_3 = T^2 - x_2T + (x_3\sigma^4(x_3)) \in \mathbf{Q}(x_2)[T]$$

which has as one of its roots $x_3 = \zeta + 1/\zeta$, with $\iota(x_3) = 2\cos(\theta)$ for $\theta = 2\pi/17$. Since $x_3 = \zeta + \zeta^{-1}$ and $\sigma^4(x_3) = \zeta^{-4} + \zeta^4$ (as $3^4 \equiv -4 \bmod 17$), so $\iota(x_3) = 2\cos(\theta)$ and $\iota(\sigma^4(x_3)) = 2\cos(4\theta)$, the easy geometric (or numerical) fact that $\cos(\theta) > \cos(4\theta)$ shows that $\iota(x_3)$ is the *larger* of the two roots of $\iota(f_3)$. Hence, once we explicitly compute $x_3\sigma^4(x_3)$ as an element of $K_2 = \mathbf{Q}(x_2)$ we can conclude

that the real number $\iota(x_3) = 2\cos(2\pi/17)$ is given by the quadratic formula for the roots of $\iota(f_3)$ using the *positive* square root. It all now comes down to computing $x_3\sigma^4(x_3)$ in

$$K_3^{\langle\sigma^4\rangle} = K_3^{G_2} = K_2 = \mathbf{Q}(x_2) = \mathbf{Q} \oplus \mathbf{Q}x_2 \oplus \mathbf{Q}x_2^2 \oplus \mathbf{Q}x_2^3.$$

(Note that $[K_2 : \mathbf{Q}] = [G : G_2] = 4$.) This is ultimately just a bit of linear algebra over $\mathbf{Q}$, given our knowledge of the $\mathbf{Q}$-linear dependence relations among powers $\{\zeta^j\}_{0\leq j<17}$.

We seek to compute the unique $a_0, a_1, a_2, a_3 \in \mathbf{Q}$ such that

$$a_0 + a_1x_2 + a_2x_2^2 + a_3x_2^3 \stackrel{?}{=} x_3\sigma^4(x_3) = (\zeta + \zeta^{-1})(\zeta^{-4} + \zeta^4) = \zeta^{-3} + \zeta^5 + \zeta^{-5} + \zeta^3. \tag{3}$$

By definition, $x_2 = \zeta + \zeta^{-4} + \zeta^{-1} + \zeta^4$. Hence, with some help from the distributive law,

$$x_2^2 = 4 + (\zeta^2 + \zeta^{-2} + \zeta^8 + \zeta^{-8}) + 2(\zeta^3 + \zeta^{-3} + \zeta^5 + \zeta^{-5}).$$

Multiplying this against another factor of $x_2 = \zeta + \zeta^{-4} + \zeta^{-1} + \zeta^4$ and using $\sum_{j=1}^{16} \zeta^j = -1$ gives

$$x_2^3 = -1 + 8(\zeta + \zeta^{-1} + \zeta^4 + \zeta^{-4}) + 2(\zeta^2 + \zeta^{-2} + \zeta^6 + \zeta^{-6} + \zeta^7 + \zeta^{-7} + \zeta^8 + \zeta^{-8}).$$

Plugging these descriptions of $x_2, x_2^2, x_2^3 \in \mathbf{Q}(\zeta)$ into the required relation

$$a_0 + a_1x_2 + a_2x_2^2 + a_3x_2^3 = \zeta^3 + \zeta^{-3} + \zeta^5 + \zeta^{-5}$$

from (3) yields the reformulation (upon collecting common appearances of each ζ^j)

$$\begin{aligned} 0 \;=\; & (a_0 - a_3 + 4a_2) + (8a_3 + a_1)(\zeta + \zeta^{-1} + \zeta^4 + \zeta^{-4}) + (2a_3 + a_2)(\zeta^2 + \zeta^{-2} + \zeta^8 + \zeta^{-8}) \\ & + (2a_2 - 1)(\zeta^3 + \zeta^{-3} + \zeta^5 + \zeta^{-5}) + 2a_3(\zeta^6 + \zeta^{-6} + \zeta^7 + \zeta^{-7}). \end{aligned}$$

Observe that *every* ζ^j for $1 \leq j \leq 16$ appears exactly once on the right side. By replacing the "constant term" $a_0 - a_3 + 4a_2$ with the equivalent expression

$$-(a_0 - a_3 + 4a_2)(\zeta + \zeta^2 + \zeta^3 + \cdots + \zeta^{16}),$$

the $\mathbf{Q}$-linear independence of the set $\{\zeta, \zeta^2, \zeta^3, \ldots, \zeta^{16}\}$ implies that *all* of the coefficients

$$8a_3 + a_1, 2a_3 + a_2, 2a_2 - 1, 2a_3$$

are equal to $a_0 - a_3 + 4a_2$. In other words, we arrive at the system of linear equations

$$a_0 - a_3 + 4a_2 = 8a_3 + a_1 = 2a_3 + a_2 = 2a_2 - 1 = 2a_3.$$

Elementary manipulations show that this system has the unique solution

$$(a_0, a_1, a_2, a_3) = (-3/2, 3, 0, -1/2).$$

Hence,

$$f_3 = T^2 - x_2T + ((-1/2)x_2^3 + 3x_2 - 3/2) \in \mathbf{Q}(x_2)[T].$$

Since we have seen that $\iota(x_3)$ is the larger of the two roots of $\iota(f_3) \in \mathbf{Q}(\iota(x_2))[T] \subset \mathbf{R}[T]$, the quadratic formula and some elementary simplifications of the discriminant give the formula

$$2\cos(2\pi/17) = \iota(x_3) = \frac{\iota(x_2) + \sqrt{2\iota(x_2)^3 + \iota(x_2)^2 - 12\iota(x_2) + 6}}{2}$$

using the positive square root, where $\iota(x_2) = (\iota(x_1) + \sqrt{\iota(x_1)^2 + 4})/2$ with $\iota(x_1) = (-1 + \sqrt{17})/2$. This is a formula *inside* $\mathbf{R}$ for $2\cos(2\pi/17)$ via iterated square roots; check it numerically!

The interested reader is invited to adapt this method to the case of the regular 257-gon (PhD thesis of F. Richelot in 1832) and the regular 65537-gon (first done by J. Hermes in 1894, after 10 years of effort). To get you started, conveniently the cyclic groups $(\mathbf{Z}/257\mathbf{Z})^\times$ and $(\mathbf{Z}/65537\mathbf{Z})^\times$ each admit 3 as a generator (since $3^{2^7} \equiv -1 \bmod (2^8 + 1)$ and $3^{2^{15}} \equiv -1 \bmod (2^{16} + 1)$, as one checks by successive squaring modulo $2^8 + 1 = 257$ and $2^{16} + 1 = 65537$ respectively).