18.702 May 4, 2011

Constructing the 17-gon

The computations are taken farther than what is in the text.

Gauss showed that one can contruct the 17-gon with ruler and compass. To prove that this is possible, it suffices to construct $\cos\theta$, $\theta = \frac{2\pi}{17}$, which we can write in terms of the primitive 17th root of unity. If $\zeta = e^{i\theta}$ and $\gamma = \zeta + \zeta^{-1}$, then $\cos\theta = \frac{1}{2}\gamma$.

What we know about ruler and compass constructions is that γ can be constructed if and only if it lies in a field that is obtained from the rational numbers by repeatly adjoining real square roots.

Let $F = \mathbb{Q}$ and $K = F(\zeta)$. The irreducible polynomial for ζ over F is

$$f(x) = x^{16} + x^{15} + \cdots + x + 1.$$

The Galois group G of K over F is a cyclic group of order 16, isomorphic to the multiplicative group $\mathbb{F}_{17}^{\times}$.

The multiplicative group is generated by the residue of 3, i.e., the powers of 3,

$$3^0 = 1,\ 3^1 = 3,\ 3^2 = 9,\ 3^3 = 10,\ ...,$$

list the elements of $\mathbb{F}_{17}^{\times}$. Taking the corresponding powers of ζ lists the powers of ζ different from 1 in this order: (We represent congruence classes modulo 17 by the integers between -8 and 8.)

$$\zeta^1, \zeta^3, \zeta^{-8}, \zeta^{-7}, \zeta^{-4}, \zeta^5, \zeta^{-2}, \zeta^{-6}, \zeta^{-1}, \zeta^{-3}, \zeta^8, \zeta^7, \zeta^4, \zeta^{-5}, \zeta^2, \zeta^6.$$

These are the roots of f. Their sum is -1.

There is a corresponding generator σ for the cyclic Galois group $G = C_{-1}$, namely the automorphism such that $\sigma\zeta = \zeta^3$ and $\sigma\zeta^i = \zeta^{3i}$. This automorphism permutes the powers cyclically in the order above:

$$\begin{aligned}\zeta^1 \to \zeta^3 \to \zeta^{-8} \to \zeta^{-7} \to \zeta^{-4} \to \zeta^5 \to \zeta^{-2} \to \zeta^{-6} \to \\ \to \zeta^{-1} \to \zeta^{-3} \to \zeta^8 \to \zeta^7 \to \zeta^4 \to \zeta^{-5} \to \zeta^2 \to \zeta^6 \ \ (\to \zeta^1).\end{aligned}$$

Next, the subgroups of G are the cyclic groups

$$C_{16} \supset C_8 \supset C_4 \supset C_2 \supset C_1$$

generated by $\sigma, \sigma^2, \sigma^4, \sigma^8$, and $\sigma^{16} = 1$ respectively.
Galois Theory tells us that the subfields of K are the fixed fields of these subgroups, and that these fixed fields form a chain

$$F = L_0 \overset{2}{\subset} L_1 \overset{2}{\subset} L_2 \overset{2}{\subset} L_3 \overset{2}{\subset} L_4 = K,$$

where $L_1 = K^{<\sigma^2>}$, etc. Moreover, there are no other subgroups, and therefore no other intermediate fields. Each of the four extensions making up this chain has degree 2, so the tower of fields can be constructed by repeatedly adjoining square roots.

Notice that, with $\gamma = \zeta^1 + \zeta^{-1}$ as above, ζ is a root of the quadratic polynomial

$$(z - \zeta)(z - \zeta^{-1}) = z^2 - \gamma z + 1,$$

which has coefficients in $F(\gamma)$. Therefore K has degree 1 or 2 over $F(\gamma)$. Since γ is a real number but ζ is not real, $F(\gamma) \subset \mathbb{R}$, and $K \not\subset \mathbb{R}$. Therefore the degree of K over $F(\gamma)$ is equal to 2, from which it follows that $F(\gamma) = L_3$. Since $\gamma \in L_3 \subset \mathbb{R}$, the square roots needed to reach the field L_3 are real. This proves that the 17-gon can be constructed by ruler and compass.

It isn't too hard to compute the necessary square roots explicitly. First, L_1 is the fixed field of σ^2. Since σ^2 sends

$$\zeta \rightsquigarrow \zeta^{-8} \rightsquigarrow \zeta^{-4} \rightsquigarrow \zeta^{-2} \rightsquigarrow \zeta^{-1} \rightsquigarrow \zeta^{8} \rightsquigarrow \zeta^{4} \rightsquigarrow \zeta^{2},$$

the sum of these powers, which we'll denote by α, is fixed by σ^2. It seems cumbersome to carry all of these ζ's along, so we abbreviate, writing the sum symbolically as $\alpha = [1, -8, -4, -2, -1, 8, 4, 2]$. The remaining powers of ζ form another orbit whose sum is $\alpha' = [3, -7, 5, -6, -3, 7, -5, 6]$. Then $\alpha + \alpha' = -1$. We expand $\alpha\alpha'$, obtaining a sum of 64 terms $\zeta^{1+3} + \zeta^{1-7} + \cdots$. The exponent $0 = 17$ does not occur among these powers. Since $\alpha\alpha'$ is a rational number, and the powers different from 1 form an orbit under the group, they occur the same number of times, i.e., 4 times, and $\alpha\alpha' = -4$. Then α and α' are roots of

$$g(x) = x^2 + x - 4 \ : \qquad \alpha, \alpha' = \tfrac{1}{2}(-1 \pm \sqrt{17}).$$

It isn't difficult to see, by sketching the 17th roots of 1, that $\alpha > \alpha'$. So the sign is + for α. Anyway, L_1 is the quadratic extension $F(\sqrt{17})$ of F.

Next, L_2 is the fixed field of σ^4, and σ^4 sends

$$\zeta \rightsquigarrow \zeta^{-4} \rightsquigarrow \zeta^{-1} \rightsquigarrow \zeta^{4}.$$

The sum of these elements is fixed by σ^4. Let

$$\beta_1 = [1, -4, -1, 4], \quad \beta_2 = [3, 5, -3, -5], \quad \beta_3 = [-8, -2, 8, 2], \quad \beta_4 = [-7, -6, 7, 6].$$

Each of these sums is fixed by σ^4, and therefore is in L_2. Then $\beta_1 + \beta_3 = \alpha$, and $\beta_1\beta_3 = -1$. So β_1 and β_3 are roots of

$$h(y) = y^2 - \alpha y - 1.$$

Similarly, β_2 and β_4 are roots of $h_1(y) = y^2 - \alpha' y - 1$. The discriminants of h and h' are $\alpha^2 + 4 = 8 - \alpha = \frac{1}{2}(17 - \sqrt{17})$ and $8 - \alpha' = \frac{1}{2}(17 + \sqrt{17})$ respectively. Let

$$\eta = \sqrt{\tfrac{1}{2}(17 - \sqrt{17})}, \qquad \eta' = \sqrt{\tfrac{1}{2}(17 + \sqrt{17})}.$$

Either of these elements will generate the field L_2.

Incidentally, the elements η, η' give us another example of nested square roots with cyclic Galois group. There is only one intermediate field of degree 2. Here $\eta\eta' = \sqrt{\frac{1}{4}(17^2 - 17)} = \sqrt{\frac{1}{4}(17 \cdot 16)} = 2\sqrt{17}$.

We continue, solving the quadratic equations for β_i:

$$\beta_1, \beta_3 = \tfrac{1}{2}(\alpha \pm \eta), \quad \text{and} \quad \beta_2, \beta_4 = \tfrac{1}{2}(\alpha' \pm \eta').$$

Here $\beta_1 > \beta_3$ and $\beta_2 > \beta_4$, so

$$\beta_1 = \tfrac{1}{2}(\alpha + \eta), \quad \text{and} \quad \beta_2 = \tfrac{1}{2}(\alpha' + \eta').$$

The subfield of K of degree 4 over F is generated by η. Since there is a unique subfield of degree 4, η' generates the same field.

Finally, let

$$\gamma = [1, -1], \quad \text{and} \quad \gamma' = [-4, 4] = \sigma^4\gamma.$$

Then $\gamma + \gamma' = \beta_1$, and $\gamma\gamma' = [-3, 5, -5, 3] = \beta_2$. So γ, γ' are roots of

$$k(z) = z^2 - \beta_1 z + \beta_2.$$

The field extension generated by γ is obtained from $F(\beta_1)$ by adjoining the square root of the discriminant $\Delta = \beta_1^2 - 4\beta_2$. Expanding the sum for β_1^2, one finds $\beta_1^2 = \beta_3 + 2\beta_2 + 4$, so

$$\Delta = \beta_3 - 2\beta_2 + 4 = \tfrac{1}{2}(\alpha - \eta) - (\alpha' + \eta') + 4 = \tfrac{1}{4}(17 + 3\sqrt{17}) - \tfrac{1}{2}\eta - \eta'.$$

We compute η' in terms of η finding that $\eta' = -\frac{1}{2}\alpha'\eta = \frac{1}{4}(1 + \sqrt{17})\eta$. Then

$$4\Delta \;=\; 17 + 3\sqrt{17} - 3\eta - \sqrt{17}\eta \;=\; \left(3 + \sqrt{17}\right)\left(\sqrt{17} - \sqrt{\tfrac{1}{2}(17 - \sqrt{17})}\right).$$

Unless I've made an error, the field $F(\gamma)$ is generated by

$$\sqrt{\left(3 + \sqrt{17}\right)\left(\sqrt{17} - \sqrt{\tfrac{1}{2}(17 - \sqrt{17})}\right)}.$$

I haven't computed γ explicitly.

18.702 Algebra II
Spring 2011