To construct a regular 17-gon we need to express the real number $\xi_{17} + \xi_{17}^{-1}$ in terms of (repeated) square roots of rational numbers. (Here as usual, $\xi_{17} = \cos(2\pi/17) + i \sin(2\pi/17)$ is the primitive 17-th root of 1.) The extension $\mathbb{Q}(\xi_{17})$ has degree 16, and to accomplish our goal, we shall construct a series of intermediate field extensions of $\mathbb{Q} \subset K_1 \subset K_2 \subset K_3 \subset \mathbb{Q}(\xi_{17})$ each of the degree 2 over the previous one. The construction also vividly illustrates the main theorem of the Galois theory. The group of automorphisms of $\mathbb{Q}(\xi_{17})$ (the Galois group) is isomorphic to $G = (\mathbb{Z}/17\mathbb{Z})^\times = \{1, 2, \ldots, 16\}$, the multiplicative group of the finite field $\mathbb{Z}/17\mathbb{Z}$. Indeed, every integer $a$ relatively prime to 17, corresponds to an automorphism $\sigma_a$ of $\mathbb{Q}(\xi_{17})$ defined by $\sigma_a(\xi_{17}) = \xi_{17}^a$.

Note that $\sigma_a \circ \sigma_b = \sigma_{ab}$ as claimed. (Don’t worry if you do not understand some of the statements. They will not be needed in the construction.)

The group $(\mathbb{Z}/17\mathbb{Z})^\times$ is cyclic, and generated by the powers of 3 (check it!). Let $G_1 = \{\pm1, \pm2 \pm 4, \pm8\}, G_2 = \{\pm1, \pm4\}, G_3 = \{\pm1\}$ be the unique subgroups of $G$ of index 2, 4 and 8, respectively. The fields $K_i$ can now be described as follows: Put $K_0 = \mathbb{Q}$, and let $K_i = K_{i-1}(\alpha_i)$ where $\alpha_i = \sum_{a \in G_i} \xi_{17}^a$.

Each field $K_i$ can also be described as the set of all elements in $\mathbb{Q}(\xi_{17})$ fixed by $G_i$. Moreover, the group of automorphisms of $\mathbb{Q}(\xi_{17})$ over $K_i$ is $G_i$. Your task is, for every $i$, to obtain a quadratic equation for $\alpha_i$ with coefficients in $K_{i-1}$. This is not too difficult. Simply calculate the square $\alpha_i^2$, and then express it as a combination of 1 and $\alpha_i$ with coefficients in $K_{i-1}$. Combining these equations, express finally $\alpha_3 = 2 \cos(2\pi/17)$ as a repeated square root involving rational numbers. This part may be a bit messy, but it is certainly doable.

Date: March 07, 2003.