Constructing the 17-gon:
In these notes, I'll give a proof that the 17-gon is constructible. I'll also take the opportunity to correct something that I didn't get right in the lecture.

Let $\boldsymbol{F}_{\boldsymbol{R}}$ denote the field of numbers $\alpha \in \boldsymbol{R}$ such that there is a finite "tower" of fields

$$\boldsymbol{Q} = F_0 \subset F_1 \subset ... \subset F_n$$

with $\alpha \in F_n$ and $[F_k : F_{k+1}] = 2$ for all k. What I said incorrectly in class is that $F_n = \boldsymbol{Q}[\alpha]$, but this need not be the case.

Lemma 0.1 $\boldsymbol{F}_{\boldsymbol{R}}$ *is a field.*

Proof: Suppose $\alpha, \beta \in \boldsymbol{F}_{\boldsymbol{R}}$. Then there are towers $F_0 \subset ... \subset F_m$ and $F'_0 \subset ... \subset F'_n$ associated to α and β respectively. Consider the tower

$$F_0 \subset ... \subset F_m = \langle F_m, F'_0 \rangle \subset ... \subset \langle F_m, F'_n \rangle$$

Here $\langle F_m, F'_k \rangle$ is the field generated by F_m and F'_k. Note that $\alpha + \beta$ and $\alpha\beta$ and α/β all belong to the last field. We just have to check that the degree of each field over the previous one is at most 2. We have $F'_{k+1} = F'_k(\sqrt{a})$ for some $a \in F_k$. But then

$$F'_{k+1} \subset \langle F_m, F'_k(\sqrt{a}) \rangle.$$

Since

$$F_m \subset \langle F_m, F'_k(\sqrt{a}) \rangle$$

as well, we have

$$\langle F_m, F'_{k+1} \rangle \subset \langle F_m, F'_k(\sqrt{a}) \rangle = \langle F_m, F'_k \rangle(\sqrt{a}).$$

But this gives us what we want. ♠

The field $\boldsymbol{F}_{\boldsymbol{C}}$ is defined in the same way, except that it involves $\alpha \in \boldsymbol{C}$, the complex field. In class we showed that

$$\boldsymbol{F}_{\boldsymbol{C}} = \boldsymbol{F}_{\boldsymbol{R}}(i). \qquad (1)$$

So, if we want to show that $x \in \boldsymbol{F}_{\boldsymbol{R}}$ it suffices to find $z \in \boldsymbol{F}_{\boldsymbol{C}}$ such that x is the real part of z.

Showing that the regular 17-gon is constructible is the same as showing that $\cos(2\pi/17) \in \boldsymbol{F}_{\boldsymbol{R}}$. To prove this, it suffices to prove that

$$\omega = \exp(2\pi i/17) \in \boldsymbol{F}_{\boldsymbol{C}}.$$

Define

$$\omega_k = \omega^{3^k}. \tag{2}$$

For instance $\omega_2 = \omega^9$ and $\omega_3 = \omega^{27} = \omega^{10}$.

Given a positive integer m and $k \in \{0, ..., m-1\}$ define

$$\alpha_{mk} = \sum_{j \equiv k \ (m)} \omega_j. \tag{3}$$

The sum is over an irredundant set of j congruent to k mod m. For instance

$$\alpha_{20} = \omega_0 + \omega_2 + ... + \omega_{14} = \omega^1 + \omega^9 + \omega^{13} + \omega^{15} + \omega^{16} + \omega^8 + \omega^4 + \omega^2.$$

Define the following fields.

- $F_0 = \boldsymbol{Q}$.
- $F_1 = F_0(\alpha_{20}, \alpha_{21})$.
- $F_{21} = F_1(\alpha_{41}, \alpha_{43})$.
- $F_2 = F_1(\alpha_{40}, \alpha_{41}, \alpha_{42}, \alpha_{43}) = F_{21}(\alpha_{40}, \alpha_{42})$.
- $F_3 = F_2(\alpha_{80}, \alpha_{84})$.
- $F_4 = F_3(\omega, \omega^{16})$.

Use the notation $A \to B$ to mean that $A \subset B$ and $[A : B] \leq 2$. The following chain proves that every element of F_4 is constructible:

$$F_0 \to F_1 \to F_{21} \to F_2 \to F_3 \to F_4. \tag{4}$$

The rest of these notes is devoted to establish this chain, one link at a time.

Lemma 0.2 *$F_0 \to F_1$.*

Proof: We have $\alpha_{20} + \alpha_{21} = -1$ and a calculation shows that $\alpha_{20}\alpha_{21} = -4$. Therefore α_{20} and α_{21} are roots of a degree 2 polynomial in $F_0[x]$. ♠

Lemma 0.3 $F_1 \to F_{21}$.

Proof: We have $\alpha_{41} + \alpha_{43} = \alpha_{21}$ and a calculation shows that $\alpha_{41}\alpha_{43} = -1$. Therefore α_{41} and α_{43} are roots of a degree 2 polynomial in $F_1[x]$. ♠

Lemma 0.4 $F_{21} \to F_2$.

Proof: Note that $F_2 = F_{21}[\alpha_{40}, \alpha_{42}]$. We have $\alpha_{40} + \alpha_{42} = \alpha_{20}$, and a calculation shows that $\alpha_{40}\alpha_{42} = -1$. Therefore α_{40} and α_{42} are roots of a degree 2 polynomial in $F_1[x]$. But then, *a forteriori*, α_{40} and α_{42} are roots of a degree 2 polynomial in. $F_{21}[x]$. ♠

Lemma 0.5 $F_2 \to F_3$.

Proof: We have $\alpha_{80} + \alpha_{84} = \alpha_{40}$, and a calculation shows that $\alpha_{80}\alpha_{84} = \alpha_{41}$. Therefore α_{80} and α_{84} are roots of a degree 2 polynomial in $F_2[x]$. ♠

Lemma 0.6 $F_3 \to F_4$.

Proof: Note that $\omega = \omega_0$ and $\omega^{16} = \omega_8$. We have $\omega + \omega^{16} = \alpha_{80}$ and $\omega\omega^{16} = 1$. But then ω and ω^{16} are roots of the degree 2 polynomial i $F_3[x]$. ♠

That's the end of the proof.