Recall that we have proved the following theorem in Lecture 3.

Theorem 1. *$\Phi_n(X) \in \mathbb{Z}[X]$ is irreducible.*

Corollary 2. *$\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$ where ζ is a primitive n-th root of unity.*

Proof. We need to prove that the map $\theta : \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \to (\mathbb{Z}/n\mathbb{Z})^\times$ in the theorem is surjective. **Recall:** Cardinality of $(\mathbb{Z}/n\mathbb{Z})^\times$ is $\phi(n) = \#\{1 \le a < n : (a,n) = 1\}$ the Euler's phi-function. And $\Phi_n(X) = \prod_{\zeta \text{ primitive } n-\text{th root of unity}}(X - \zeta) = \prod_{i:(i,n)=1}(X - \zeta^i)$, thus degree of $\Phi_n(X)$ is $\phi(n)$. Hence $|\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})| = [\mathbb{Q}(\zeta) : \mathbb{Q}] = \phi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$. Therefore the map θ is surjective and hence is bijective. □

Theorem 3. *The regular n-gon is constructible if and only if $n = 2^k p_1 p_2 \cdots p_s$ where p_i's are distinct Fermat primes.*

Remark 4. You might have already seen that, for a prime p, a regular p-gon is constructible if and only if p is a Fermat prime. The above theorem characterizes constructible n-gon for any positive integer n (need not be prime).

Example 5. (1) Regular 17-gon is constructible.
(2) Regular 2^k-gon is constructible for every $k \ge 1$.

Recall: (1) A regular n-gon is constructible if and only if primitive n-th root of unity is constructible.
(2) A number $\alpha \in \mathbb{R}$ is constructible $\Rightarrow [\mathbb{Q}(\alpha) : \mathbb{Q}] = 2^s$ for some $s \in \mathbb{N}$.
(3) When is the converse of (2) true ? If $\mathbb{Q}[\alpha] \subseteq E \subseteq \mathbb{R}$ and $E/\mathbb{Q}$ is a Galois extension with $[E : \mathbb{Q}] = 2^s$ for some integer s, then α is constructible.

Sketch of proof in the case p prime: Suppose p is prime. We know that $\mathbb{Q}[\zeta]/\mathbb{Q}$ is a Galois extension and $\mathrm{irr}(\zeta, \mathbb{Q}) = X^{p-1} + X^{p-2} + \cdots + 1$. Thus $[\mathbb{Q}[\zeta] : \mathbb{Q}] = p - 1$. Therefore regular p-gon is constructible if and only if $[\mathbb{Q}[\zeta] : \mathbb{Q}] = p - 1 = 2^s$ for some s.

Fact: $p = 2^s + 1$ is a prime number if and only if p is a Fermat prime.

Sketch of proof of Theorem 3 Let ζ be a primitive n-th root of unity. We have proved that $\mathbb{Q}[\zeta]/\mathbb{Q}$ is Galois. Therefore ζ is constructible iff $\phi(n) = 2^s$ for some s and then the theorem follows.

Fact: Let $K/\mathbb{Q}$ be a finite Galois extension with $\mathrm{Gal}(K/\mathbb{Q})$ is abelian. Then $K \subset \mathbb{Q}(\zeta)$ for some primitive n-th root of unity ζ.

Definition 6. A finite Galois extension E/F is called cyclic if the group $\mathrm{Gal}(E/F)$ is a cyclic group.

Example 7. (a) $\mathbb{Q}(i)/\mathbb{Q}$ is cyclic of degree 2.
(b) $\mathbb{Q}(\omega)/\mathbb{Q}$ is also cyclic of degree 2 (ω is a cube root of 1).
(c) $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$ is not cyclic since the Galois group is Klein's 4 group which is not a cyclic group.

Theorem 8. *Let F contain a primitive n-th roots of unity, $E = F[\alpha]$ where $\alpha^n \in F$ and let n be the smallest non-negative integer such that $\alpha^n \in F$. Then E/F is Galois with Galois group cyclic of order n.*

Proof. Let $\alpha^n = a \in F$. Then α satisfies the equation $X^n - a \in F[X]$. Let ζ be a primitive n-th root of unity. Then $\alpha, \zeta\alpha, \zeta^2\alpha, \cdots, \zeta^{n-1}\alpha$ are all the roots of $X^n - a$. Therefore $E = F[\alpha]$ is the splitting field of $X^n - a$ and hence is Galois extension. Let μ_n denote the group of nth roots of 1 in F. In order to prove the assertion we establish an isomorphism between $\theta : \mathrm{Gal}(E/F) \longrightarrow \mu_n$. Let $\sigma \in \mathrm{Gal}(E/F)$, then $\sigma : E \to E$ is an automorphism with $\sigma(\alpha) = \zeta^i\alpha$ for some $0 \leq i \leq n-1$. Define a map $\theta : \mathrm{Gal}(E/F) \to \mu_n$ as

$$\sigma \mapsto \frac{\sigma(\alpha)}{\alpha} = \zeta^i.$$

Notice that this map remains same when α is replaced by its conjugate (Suppose $\tau(\alpha)$ is a conjugate of α, say $\tau(\alpha) = \zeta^j\alpha$ for some $0 \leq j \leq n-1$. Then $\frac{\sigma(\tau(\alpha))}{\tau(\alpha)} = \frac{\sigma(\zeta^j\alpha)}{\zeta^j\alpha} = \frac{\zeta^j\sigma(\alpha)}{\zeta^j\alpha} = \frac{\sigma(\alpha)}{\alpha}$ as $\zeta^j \in F$). Moreover, θ is a group homomorphism, i.e.

$$\theta(\sigma\tau) = \frac{\sigma(\tau(\alpha))}{\tau\alpha} = \frac{\sigma(\tau(\alpha))}{\tau(\alpha)}\frac{\tau(\alpha)}{\alpha} = \frac{\sigma(\alpha)}{\alpha}\frac{\tau(\alpha)}{\alpha} = \theta(\sigma)\theta(\tau).$$

The map θ is injective: $\theta(\sigma) = 1 \Rightarrow \frac{\sigma(\alpha)}{\alpha} = 1 \Rightarrow \sigma(\alpha) = \alpha \Rightarrow \sigma = id$ (as α generates E). Let $|\mathrm{Gal}(E/F)| = d$. Then $d|n$. Suppose $d < n$ then $(\theta(\sigma))^d = 1$ for all $\sigma \in \mathrm{Gal}(E/F)$. This implies that $\sigma(\alpha^d) = \sigma(\alpha)^d = \alpha^d$ and hence $\alpha^d \in F$ but this is a contradiction (as $d < n$). Thus θ is an isomorphism. □

Theorem 9. *Let F be a field containing a primitive n-th root of unity. If E is a cyclic Galois extension of F of order n then $E = F[\alpha]$ for some $\alpha \in E$ such that $\alpha^n \in F$.*

Proof. Let $G = \mathrm{Gal}(E/F) =< \sigma >$. It is enough to show that there exists $\alpha \in E$ such that $\sigma(\alpha) = \zeta^{-1}\alpha$ (then $\alpha^n \in F$ because $\sigma(\alpha^n) = \sigma(\alpha)^n = (\zeta^{-1}\alpha)^n = \alpha^n \Rightarrow \alpha^n \in F$ and n is the least such integer. Moreover, $F[\alpha] \subseteq E$ and by Theorem 8 $F[\alpha]/F$ is cyclic of order n which gives that $E = F[\alpha]$).
By Dedekind's theorem on the independence of characters $\{id, \sigma, \sigma^2, \cdots, \sigma^{n-1}\}$ is linearly independent. Therefore

$$\sum_{i=0}^{n-1} \zeta^i\sigma^i \neq 0.$$

Hence there exists $\gamma \in E$ such that

$$\alpha := \sum_{i=0}^{n-1} \zeta^i\sigma^i(\gamma) \neq 0$$

Then

$$\sigma(\alpha) = \sum_{i=0}^{n-1} \zeta^i\sigma^{i+1}(\gamma) = \zeta^{-1}\sum_{i=0}^{n-1} \zeta^{i+1}\sigma^{i+1}(\gamma) = \zeta^{-1}\alpha.$$

□

Example 10. Consider $n = 2$. Notice that $\mathbb{Q}$ contains -1 and hence a primitive 2nd root of unity. Therefore for any $a \in \mathbb{Q}$ which is not a square $\mathbb{Q}(\sqrt{a})/\mathbb{Q}$ is cyclic extension of degree 2. Moreover, if K/Q is an extension of degree 2, then $K = \mathbb{Q}(\sqrt{a})$ for some $a \in \mathbb{Q}$.

Question 11. When is $\mathbb{Q}(\sqrt{a}) = \mathbb{Q}(\sqrt{b})$ for $a, b \in \mathbb{Q}$?

Theorem 12. *Let F contain a primitive n-th root of unity. Two cyclic extensions of degree n, say $F[\sqrt[n]{a}]$ and $F[\sqrt[n]{b}]$, are equal if and only if $a = b^r c^n$ (if and only if a and b generate the same subgroup in $F^\times/F^{\times n}$).*

Proof. If $a = b^r c^n$ where $\gcd(r, n) = 1$, then $F[\sqrt[n]{a}] = F[\sqrt[n]{b}]$. (Since $\sqrt[n]{a} = c\sqrt[n]{b^r}$, $F[\sqrt[n]{a}] \subseteq F[\sqrt[n]{b}]$. On the other hand, write $1 = rx + ny$. Then $\sqrt[n]{b} = c(\sqrt[n]{b^{rx+ny}}) = c^{-1}(\sqrt[n]{a})^x b^y$ and hence $F[\sqrt[n]{b}] \subseteq F[\sqrt[n]{a}]$.)

Now, suppose that $F[\sqrt[n]{a}] = F[\sqrt[n]{b}]$. Let $\alpha = \sqrt[n]{a}$, $\beta = \sqrt[n]{b}$, $\mathrm{Gal}(F[\beta]/F) =< \sigma >$ and $\sigma(\beta) = \zeta\beta$ for some primitive n-th root of unity ζ. Then $\sigma(\alpha) = \zeta^j \alpha$ for some positive integer with $\gcd(j, n) = 1$. Write

$$\alpha = \sum_{i=0}^{n-1} c_i \beta^i \qquad \text{for some } c_i \in F.$$

Then $\sigma(\alpha) = \sum_{i=0}^{n-1} c_i \zeta^i \beta^i$. On the other hand, $\sigma(\alpha) = \zeta^j \alpha = \sum_{i=0}^{n-1} \zeta^j c_i \beta^i$. On comparing the coefficients we get $c_i = 0$ for all $i \neq j$. Thus $\alpha = c_j \beta^j$ which gives that $a = c_j^n b$ as required. □