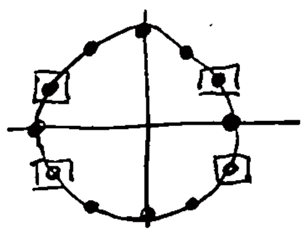
3/10 Cyclotomic ~~[illegible]~~ Extensions §5.8

Our goal now is to study finite extensions of $\mathbb{Q}$ of specific forms, leading up to a treatment of the problem which motivated the development of Galois theory: the solubility of polynomials by radicals.

Def'n Recall that a number $u \in \mathbb{C}$ is called an n^{th} root of unity, for some $n \geq 1$, if $u^n = 1$, i.e., if u is a root of $x^n - 1 \in \mathbb{Q}[x]$. If u is an n^{th} root of unity, it is also a $(mn)^{th}$ root of unity for any $m \geq 1$. We say u is a primitive n^{th} root of unity if it is an n^{th} root of unity but not a k^{th} root of unity for any $k < n$.

Prop. The n^{th} roots of unity are $e^{\frac{2\pi i}{n} \cdot j}$ for $j = 0, 1, \ldots, n-1$. The primitive n^{th} roots of unity are those $e^{\frac{2\pi i}{n} \cdot j}$ with $\gcd(j, n) = 1$.

E.g. We've seen before how the n^{th} roots of unity are equally spaced on the unit circle, for instance for $n = 12$ we get



$\Leftarrow$ the primitive 12^{th} roots of unity are circled: they are $e^{\frac{2\pi i}{12} \cdot j}$ for $j = 1, 5, 7, 11$, the integers coprime to 12.

Pf sketch of prop: That the $e^{\frac{2\pi i}{n} j}$ for $j = 0, 1, 2, \ldots, n-1$ are the n^{th} roots of unity follows from the fact that $e^{\frac{2\pi i}{n} \cdot j} \cdot e^{\frac{2\pi i}{n} \cdot k} = e^{\frac{2\pi i}{n}(j + k \bmod n)}$ (phases of complex #'s add when multiplied).

That the primitive ones are the coprime j's then follows from $e^{\frac{2\pi i}{n} \cdot j}$ is a primitive n^{th} root of unity $\Leftrightarrow$ j is a generator of $(\mathbb{Z}/n\mathbb{Z}, +)$ $\Leftrightarrow$ j is a unit in the ring $\mathbb{Z}/n\mathbb{Z}$ $\Leftrightarrow$ j is coprime to n. You will flesh out this argument on your next HW assignment. ∎

Notice: $\zeta_n = e^{\frac{2\pi i}{n}}$ is always a primitive n^{th} root of unity, and all n^{th} roots of unity are powers of this ζ_n.

Def'n Let $n \geq 1$. The n^{th} cyclotomic polynomial $\Phi_n(x) \in \mathbb{C}[x]$ is $\Phi_n(x) = \prod_{\omega \text{ a primitive } n^{\text{th}} \text{ root of unity}} (x - \omega)$. (The book uses $g_n(x)$.)

E.g. The primitive 3^{rd} roots of unity are $\omega = e^{\frac{2\pi i}{3}} = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$ and $\omega^2 = -\frac{1}{2} - \frac{\sqrt{3}}{2}i$; so $\Phi_3(x) = (x-\omega)(x-\omega^2) = x^2 + x + 1$.

In fact, the first 6 cyclotomic polynomials are:

$\Phi_1(x) = x-1$, $\Phi_2(x) = x+1$, $\Phi_3(x) = x^2+x+1$, $\Phi_4(x) = x^2+1$

$\Phi_5(x) = x^4+x^3+x^2+x+1$, $\Phi_6(x) = x^2 - x + 1$.

Thm $x^n - 1 = \prod_{d \mid n} \Phi_d(x)$.

Pf: Every root of $x^n - 1$ is an n^{th} root of unity, which is a primitive d^{th} root of unity for some $d \mid n$. ☒

Note. Even though $\Phi_d(n)$ is a priori defined as an element of $\mathbb{C}[x]$, looks like it belongs to $\mathbb{Q}[x]$. This is true and we'll prove it! In fact the coefficients are integers, which can get arbitrarily big, but take a while ($\Phi_{105}(x)$ is first with a coeff. not in $\{1,-1\}$).

The way we will show cyclotomic polynomials are rational is by studying the extensions of $\mathbb{Q}$ we get by adjoining their roots.

Def'n The n^{th} cyclotomic extension of $\mathbb{Q}$ is the splitting field of $x^n - 1$. Equivalently, ...

Thm The n^{th} cyclotomic extension is $\mathbb{Q}(\zeta_n)$, where ζ_n is a primitive n^{th} root of unity.

Pf: Since ζ_n is an n^{th} root of unity, it belongs to splitting field of $x^n - 1$. But on other hand, every root of unity is a power of ζ_n, hence in $\mathbb{Q}(\zeta_n)$. ∎

Thm Let $\varphi_k : \mathbb{Q}(\zeta_n) \to \mathbb{Q}(\zeta_n)$ be defined by $\varphi_k(\zeta_n) = \zeta_n^k$. Then $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\zeta_n)) \subseteq \{\varphi_k : 1 \leq k \leq n,\ \gcd(n,k) = 1\}$.

Pf: Any $\sigma \in \mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\zeta_n))$ is determined by where it sends ζ_n, which must be to some ζ_n^k since these are roots of $x^n - 1$. But it cannot be sent to a non-primitive n^{th} root of unity, since it's not a root of any $x^m - 1$ with $m < n$. ∎

Cor The cyclotomic polynomial $\Phi_n(x) \in \mathbb{Q}[x]$.

Pf: $\mathbb{Q}(\zeta_n)$ is a Galois extension, since it's a splitting field, and every $\sigma \in \mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\zeta_n))$ fixes $\Phi_n(x)$ since just permutes roots, so in fact coefficients of $\Phi_n(x)$ are rational. ∎

Thm (Gauss) $\Phi_n(x)$ is irreducible over $\mathbb{Q}$.

Pf: This is non-trivial but I skip it - see the book. ∎

Cor $\Phi_n(x)$ is the minimal polynomial of ζ_n, and every φ_k for $\gcd(n,k)$ is indeed an element of $G = \mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\zeta_n))$.

Hence $G \cong (\mathbb{Z}/n\mathbb{Z})^\times$, the multiplicative group mod n, via the isomorphism $\varphi_k \mapsto k \in (\mathbb{Z}/n\mathbb{Z})^\times$.

Remark: This shows $G \cong (\mathbb{Z}/n\mathbb{Z})^\times$ is an abelian group of order $\varphi(n)$ where $\varphi(n) = \#\{1 \leq k \leq n : \gcd(n,k) = 1\}$ is Euler's totient function. When $n = p$ is prime we have seen that $(\mathbb{Z}/p\mathbb{Z})^\times$ is in fact cyclic (of order $p-1$), but in general it need not be: e.g. $(\mathbb{Z}/8\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.

//