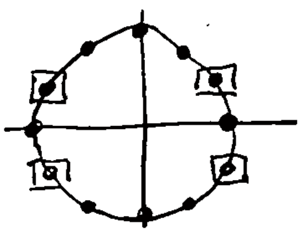
3/10 ~~Algebraic~~ Cyclotomic Extensions §5.8

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. $\blacksquare$

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 $d \mid n$. $\square$

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 $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\zeta_n)) \subseteq \{\varphi_k : 1 \le k \le n,\ \gcd(n,k) = 1\}$.

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 nontrivial 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 $\varphi(n) = \#\{1 \le k \le n : \gcd(n,k) = 1\}$ 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. $(\mathbb{Z}/8\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.

//

3/12

Cyclic Extensions §5.7

We are almost ready to study the solvability of polynomials by radicals. We just need one more preparatory result...

Def'n An algebraic, Galois extension L/K is called abelian if $\mathrm{Aut}_K(L)$ is abelian, it is called cyclic if $\mathrm{Aut}_K(L)$ is cyclic, and it is called cyclic of degree n if $\mathrm{Aut}_K(L)$ is $\mathbb{Z}/n\mathbb{Z}$.

Remark: We have seen that the cyclotomic extension $\mathbb{Q}(\zeta_n)$ of $\mathbb{Q}$ is always abelian, and sometimes cyclic (e.g. if n is prime) although not always.

In general it is hard to classify cyclic extensions, but there is a nice situation where we can do this.

Def'n For an arbitrary field K, $u \in K$ is called an n^{th} root of unity if $u^n = 1 \in K$, and is called a primitive n^{th} root of unity if $u^0, u^1, \dots, u^{n-1}$ are all distinct (hence are all the n^{th} roots of unity).

For subfields of $\mathbb{C}$, this agrees with our previous definition...

Thm Let K be a field containing a primitive n^{th} root of unity ζ_n for some $n \geq 1$. Then the following are equivalent for L/K:

1) L/K is cyclic of degree d, for some $d \mid n$.
2) L/K is the splitting field of a polynomial of form $f(x) = x^n - a \in K[x]$, in which case $L = K(u)$ for u a root of $f(x)$.
3) L/K is splitting field of irreducible polynomial of form $f(x) = x^d - a$ for some $d \mid n$, in which case $L = K(u)$ for u root of $f(x)$.

E.g. Any degree 2 extension of $\mathbb{Q}$ is the splitting field of a polynomial of the form $x^2 - d$ where d is not a square in $\mathbb{Q}$, and this extension has Galois group $\mathbb{Z}/2\mathbb{Z}$.

prim. 3^{rd} root of unity

E.g.: On a previous homework you showed that if $L = \mathbb{Q}(\omega, \sqrt[3]{2})$ is the splitting field of $x^3 - 2$ over $K = \mathbb{Q}$, then $\mathrm{Aut}_K(L) \simeq S_3$, which is not cyclic (not even abelian!). But $\mathbb{Q}$ does not have a prim. 3^{rd} root of unity! If we instead take $K = \mathbb{Q}(\omega)$, then $\mathrm{Aut}_K(L) = \mathbb{Z}/3\mathbb{Z}$.

In the theorem, 2) and 3) are easily seen to be equivalent, just having to do with whether $x^n - a$ is irreducible, equivalently whether a has a d^{th} root in K for some $d \mid n$. The main point is showing 3) $\Leftrightarrow$ 1). In fact we will mostly care about 3) $\Rightarrow$ 1), which we will prove now; we just need:

Lemma If K is a field with a primitive n^{th} root of unity ξ, then for any $d \mid n$, $\eta = \xi^{n/d}$ is a primitive d^{th} root of 1. And if L is an extension of K such that $u \in L$ is a root of $x^d - a \in K[x]$, then all the roots of $x^d - a$ are $u, \eta u, \eta^2 u, \ldots, \eta^{d-1} u$ (all distinct).

Pf: Straightforward exercise. ☒

Pf of 3) $\Rightarrow$ 1) in thm: By the lemma, the roots of $x^d - a$ in L are $u, \eta u, \ldots, \eta^{d-1} u$ where u is any root and $\eta = \xi^{n/d}$ as above. So any $\sigma \in \mathrm{Aut}_K(L)$ is determined by where it sends u (since $\eta \in K$ is fixed by σ). Since $x^d - a$ is irreducible, there must be some σ with $\sigma(u) = \eta u$, and this σ generates all of $\mathrm{Aut}_K(L)$ since $\sigma^k(u) = \eta^k u$, which give all the possible automorphisms in the Galois group by the previous sentence. ☒

We will only sketch the ideas that go into the pf of 1) $\Rightarrow$ 3):

Def'n Let L/K be a finite, Galois extension, and suppose that $\mathrm{Aut}_K(L) = \{\sigma_1, \dots, \sigma_n\}$. For any $u \in L$, the norm of u is $N(u) = \sigma_1(u) \cdot \sigma_2(u) \cdot \cdots \cdot \sigma_n(u)$.

E.g. Let $K = \mathbb{R}$ and $L = \mathbb{C}$. Recall that $\mathrm{Aut}_{\mathbb{R}}(\mathbb{C}) = \{1, \sigma\}$ where $\sigma: z \mapsto \bar{z}$ is complex conjugation. So the norm of $z = a+bi \in \mathbb{C}$ is $N(z) = z \cdot \bar{z} = a^2 + b^2$, usual complex norm.

E.g. For $K = \mathbb{Q}$ and $L = \mathbb{Q}(i)$, the same is true: the norm of $a+bi$ is $(a+bi)(a-bi) = a^2 + b^2 \in \mathbb{Q}$.

Prop. If L/K is a finite Galois extension, then the norm $N(u)$ of any $u \in L$ is an element of the base field K.

Pf: For any $\sigma \in \mathrm{Aut}_K(L)$, $\sigma(N(u)) = \sigma\sigma_1(u) \cdot \sigma\sigma_2(u) \cdots \sigma\sigma_n(u)$
$= \sigma_{i_1}(u) \cdot \cdots \sigma_{i_n}(u) = N(u)$
(where $i_1, \dots, i_n$ is some permutation of $1, \dots, n$), so because L/K is Galois, $N(u) \in K$ as claimed. ☒

Remark: We can define the norm for non-Galois extensions too, and it remains true that it belongs to the ground field, but it's a little more technical.

Another important property of the norm is multiplicativity:

Prop. We have $N(u) \cdot N(v) = N(uv)$ for $u, v \in L$.

Pf: Straightforward exercise. ☒

The norm is particularly useful for cyclic extensions...

Thm (Hilbert Theorem 90) Let L/K be a finite cyclic (Galois) extension and let $\sigma \in \mathrm{Aut}_K(L)$ be a generator of the Galois group. Then for $u \in L$, $N(u)=1 \iff u = v/\sigma(v)$ for some $v \in L$.

Pf: One direction is easy: if $u = \frac{v}{\sigma(v)}$ then $N(u) = \frac{\sigma_1(v)\cdots\sigma_n(v)}{\sigma_{i_1}(v)\cdots\sigma_{i_n}(v)} = 1$

The other direction is nontrivial - see the book for a proof! ☒

E.g. Consider $L = \mathbb{Q}(i)$ over $K = \mathbb{Q}$. The elements in $\mathbb{Q}(i)$ of norm 1 are $\frac{p}{r} + \frac{q}{r} i$ with $\frac{p^2}{r^2} + \frac{q^2}{r^2} = 1$, i.e., $p^2 + q^2 = r^2$, $p,q,r \in \mathbb{Z}$. These are Pythagorean triples. Hilbert's Thm 90 says they can all be written in form $\frac{a+bi}{a-bi} = \frac{a^2-b^2}{a^2+b^2} + \frac{2ab}{a^2+b^2} i$, $a,b \in \mathbb{Z}$

It is a classic fact going back to Euclid that (primitive) Pythagorean triples can be parameterized in this way.

With Hilbert's thm 90 we can complete the pf of main thm:

Pf of 1) ⇒ 3): Let $\sigma \in \mathrm{Aut}_K(L)$ be a generator, and let $\eta = \zeta^{n/d}$ be a primitive dth root of unity. Then $N(\eta) = \eta \cdot \sigma(\eta) \cdots \sigma^{d-1}(\eta) = \underbrace{\eta^d}_{=1}$ (since $\eta \in K$)

so by Hilbert 90 we can write $\eta = v/\sigma(v)$ for some $v \in L$. Notice $\sigma(v^d) = (\sigma(v))^d = \left(\frac{v}{\eta}\right)^d = \frac{v^d}{\eta^d} = v^d$ (since $\eta^d = 1$), so because the extension L/K is Galois, this means that $v^d \in K$. Then v is a root of the polynomial $x^d - v^d \in K[x]$, and it can be shown that this polynomial is in fact irreducible over K and that $L = K(v)$ is the splitting field.

☒