Section V.8. Cyclotomic Extensions

Note. In this section we explore splitting fields of $x^n - 1$. The splitting fields turn out to be abelian extensions (that is, algebraic Galois extensions with abelian Galois groups). Theorem V.8.1 is used in the proof of Theorem V.9.4 (which is on radical extensions and solvable groups), but the remainder of this chapter is not needed for what follows and may be skipped if we are short on time.

Definition. A splitting field F over a field K of polynomial $x^n - 1_K \in K[x]$ (where $n \geq 1$) is a *cyclotomic extension of order* n.

Note. If $\text{char}(K)$ divides n, say $\text{char}(K) = p \neq 0$ and $n = mp^t$ where $\gcd(p, m) = (p, m) = 1$ then by the Freshman's Dream (Exercise III.1.11; we can also use the Binomial Theorem, Theorem III.1.6, here)

$$(x^m - 1)^{p^t} = x^{mp^t} - 1^{p^t} = x^n - 1$$

and so a cyclotomic extension of order n coincides with one of order m. So we only consider (without loss of generality) cases where $\text{char}(K)$ does not divide n; that is, cases where either $\text{char}(K) = 0$ or $\text{car}(K) = p$ where $(p, n) = 1$).

Recall. The Euler phi function is defined on $\mathbb{N}$ as $\varphi(n)$ equals the number of elements in the set $\{1, 2, \ldots, n\}$ which are relatively prime to n. For example, for prime p, $\varphi(p) = p - 1$. In Exercise V.8.4 it is shown that the order of the multiplicative group of units in $\mathbb{Z}_n$ is $\varphi(n)$ (recall that an element of a ring is a "unit" if it has a multiplicative inverse).

Theorem V.8.1. Let $n \in \mathbb{N}$, let K be a field such that $\text{char}(K)$ does not divide n, and let F be a cyclotomic extension of K of order n. Then the following hold.

(i) $F = K(\zeta)$ where $\zeta \in F$ is a primitive nth root of unity.

(ii) F is an abelian extension of dimension d where $d \mid \varphi(n)$; if n is prime then F is actually a cyclic extension.

(iii) $\text{Aut}_K(F)$ is isomorphic to a subgroup of order d of the multiplicative group of units of $\mathbb{Z}_n$.

Note. The dimension of F over K in Theorem V.8.1 may be strictly less than $\varphi(n)$. For example, let ζ be a primitive 5th root of unity. Then $[\mathbb{R}(\zeta) : \mathbb{R}] = 2$ (see Corollary V.3.20 and its proof; or find an irreducible second degree polynomial in $\mathbb{R}[x]$ for which the primitive 4th root of unity is a root). But $\varphi(5) = 4$ and so $[\mathbb{R}(\zeta) : \mathbb{R}] = 2 < 4 = \varphi(n)$.

Definition. Let $n \in \mathbb{N}$, let F be a field such that $\text{char}(K)$ does not divide n, and let F be a cyclotomic extension of order n of K. The *nth cyclotomic polynomial* over K is the monic polynomial $g_n(x) = (x - \zeta_1)(x - \zeta_2) \cdots (x - \zeta_r)$ where $\zeta_1, \zeta_2, \ldots, \zeta_r$ are all the distinct primitive nth roots of unity in F.

Example. If $K = \mathbb{Q}$, then the 1th root of unity is 1 (which is trivially a primitive root) and so $g_1(x) = x - 1$. The only primitive 2th root of unity is -1 and so $g_2(x) = x - (-1) = x + 1$. The primitive 3rd roots of unity are $-1/2 + (\sqrt{3}/2)i$ and $-1/2 - (\sqrt{3}/2)i$, so

$$g_3(x) = (x - (-1/2 + (\sqrt{3}/2)i))(x - (-1/2 - (\sqrt{3}/2)i) = x^2 + x + 1.$$

The primitive 4th roots of unity are i and $-i$, so $g_4(x) = (x - i)(x + i) = x^2 + 1$. Since 5 is prime then all 5th roots of unity are primitive except $x = 1$, so

$$g_5(x) = \frac{x^5 - 1}{x - 1} = x^4 + x^3 + x^2 + x + 1.$$

In general, if p is prime then similarly

$$g_p(x) = \frac{x^5 - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots x^2 + x + 1.$$

Theorem V.8.2. Let $n \in \mathbb{N}$, let K be a field such that $\text{char}(K)$ does not divide n, and let $g_n(x)$ be the nth cyclotomic polynomial over K. Then the following hold.

(i) $x^n - 1_K = \prod_{d|n} g_d(x)$.

(ii) The coefficients of $g_n(x)$ lie in the prime subfield P of K. If $\text{char}(K) = 0$ and P is identified with the field $\mathbb{Q}$ of rationals, then the coefficients are actually integers.

(iii) $\text{Deg}(g_n(x)) = \varphi(n)$ where φ is the Euler phi function.

Note. By Theorem V.8.2(i) gives a recursive formula for g_n:

$$g_n(x) = \frac{x^n - 1_K}{\prod_{d|n, d<n} g_d(x)}.$$

As previously observed, if p is prime then

$$g_p(x) = \frac{x^p - 1_K}{g_1(x)} = \frac{x^p - 1_K}{x - 1_K} = x^{p-1} + x^{p-1} + \cdots + x^2 + x + 1.$$

Based on the example above with $K = \mathbb{Q}$:

$$g_6(x) = \frac{x^6 - 1}{g_1(x)g_2(x)g_3(x)} = \frac{x^6 - 1}{(x-1)(x+1)(x^2+x+1)} = x^2 - x + 1,$$

and so

$$g_{12}(x) = \frac{x^{12} - 1}{g_1(x)g_2(x)g_3(x)g_4(x)g_6(x)}$$
$$= \frac{x^{12} - 1}{(x-1)(x+1)(x^2+x+1)(x^2-x+1)} = x^4 - x^2 + 1.$$

Note. If we take the base field as $K = \mathbb{Q}$ (of characteristic 0, of course) then we can refine the previous results, as follows.

Proposition V.8.3. Let F be a cyclotomic extension of order n of the field $\mathbb{Q}$ of rational numbers and $g_n(x)$ the nth cyclotomic polynomial over $\mathbb{Q}$. Then the following hold.

(i) $g_n(x)$ is irreducible in $\mathbb{Q}[x]$.

(ii) $[F : \mathbb{Q}] = \varphi(n)$ where φ is the Euler function.

(iii) $\mathrm{Aut}_{\mathbb{Q}}(F)$ is isomorphic to the multiplicative group of units in the ring $\mathbb{Z}_n$.

Note. The Kronecker-Weber Theorem states that "Every abelian extension of $\mathbb{Q}$ is contained in a cyclotomic extension of $\mathbb{Q}$." An "elementary proof" is given by M. J. Greenberg in "An Elementary Proof of the Kronecker-Weber Theorem," *American Mathematical Monthly*, **81**(6), 601–607 (1974). However, this proof requires results from ramification theory (a branch of commutative algebra). According to Wikipedia (`en.wikipedia.org/wiki/Kronecker-Weber_theorem`; accessed July 9, 2015), the result was first stated by Leopold Kronecker who gave an incomplete proof in 1853. In 1886, Heinrich Martin Weber published a proof with some gaps and errors. The first complete proof was given by David Hilbert in 1896.

Note. Returning to the topic of ruler and compass constructions (from the appendix to Section V.5.1), we can use our knowledge of cyclotomic extensions to give necessary and sufficient conditions by which a regular n-gon can be constructed with a ruler and compass. The conditions (which involve Fermat primes) were originally shown to be necessary by Gauss. However, he did not show the conditions were necessary. The problem was completely solved by Pierre Wantzel in 1837 and published as "Recherches sur les moyens de reconnaître si un Problème de Géométrie peut se résoudre avec la règle et le compas" in *Journal de Mathématiques Pures et Appliquées* **1**(2), 366-372. In this paper he also proved the impossibility of doubling the cube and trisecting an angle. For more details, see my class notes based on Fraleigh's *A First Course in Abstract Algebra*, 7th edition:

`http://faculty.etsu.edu/gardnerr/4127/notes/VI-32.pdf` and

`http://faculty.etsu.edu/gardnerr/4127/notes/X-55.pdf`