Section X.55. Cyclotomic Extensions

Note. In this section we return to a consideration of roots of unity and consider again the cyclic group of roots of unity as encountered in Part I. "Primitive" roots of unity are defined and we classify which regular n-gons are constructible with a straight edge and compass.

Definition 55.1. The splitting field of $x^n - 1$ over field F is the nth *cyclotomic extension* of F.

Note. If α is a zero of $x^n - 1 \in F[x]$, then $x - \alpha$ is a factor of $x^n - 1$ by the Factor Theorem (Corollary 23.3). Consider $g(x) = (x^n - 1)/(x - \alpha)$ (that is, perform the division and cancellation so that $g(x)$ is then a polynomial of degree $n - 1$). Then $g(\alpha) = (n \cdot 1)\alpha^{-1} \neq 0$ provided the characteristic of F does not divide n (see page 303 for the computation). So, under this condition on the characteristic of F, any zero of $x^n - 1$ is a zero of multiplicity 1 and by Note 2 of Section 51, the splitting field of $x^n - 1$ is separable. Therefore, the nth cyclotomic extension of F is a finite normal extension (and so the Main Theorem of Galois Theory, Theorem 53.6, applies).

Note. Recall that the nth roots of unity in $\mathbb{C}$ form the group U_n and U_n is isomorphic to $\mathbb{Z}_n$. So U_n is a cyclic group. The elements of U_n which generate U_n are called *primitive roots of unity* (this definition is given in the exercises of Section 6). By Corollary 6.16, a cyclic group of order n has $\phi(n)$ generators, where ϕ is the Euler phi-function ($\phi(n)$ is the number of positive integers less than n which are relatively prime to n). So U_n has $\phi(n)$ generators—the $\phi(n)$ primitive nth roots of unity.

Definition 55.2. The polynomial

$$\Phi_n(x) = \prod_{i=1}^{\phi(n)} (x - \alpha_i)$$

where the α_i are the primitive nth roots of unity in $\overline{F}$, is the nth *cyclotomic polynomial* over F.

Note. With K as the splitting field of $x^n - 1$ over field F, we know by Corollary 48.5 that an automorphism in the Galois group $G(K/F)$ must permute the primitive nth roots of unity. So the coefficients of $\Phi_n(x)$ are left fixed under such an automorphism and so $\Phi_n(x)$ is left fixed under every element of $G(K/F)$ regarded as extended to $K[x]$. Therefore $\Phi_n(x) \in F[x]$. In particular, in the case when $F = \mathbb{Q}$, we have $\Phi_n(x) \in \mathbb{Q}[x]$ and $\Phi_n(x)$ is a divisor of $x^n - 1$. by Theorem 23.11, we have $\Phi_n(x) \in \mathbb{Z}[x]$. We now claim without proof that $\Phi_n(x)$ is irreducible over $\mathbb{Q}$ (for a proof, see Proposition V.8.3(i) of Thomas Hungerford's *Algebra*, Springer Verlag, 1974).

Example 55.3. Find the primitive 8th roots of unity in $\mathbb{C}$ and find $\Phi_n(x)$.

Solution. We know from Section 1 that the 8th roots of unity are of the form $\cos\left(\frac{2k\pi}{8}\right) + i\sin\left(\frac{2k\pi}{8}\right)$ for $k = 0, 1, 2, \ldots, 7$. By Corollary 6.16, the generators of U_8 (and hence the primitive 8th roots of unity) are given when k is relatively prime to 8. That is, the primitive roots are given by $k = 1, 3, 5, 7$ (notice that $\phi(8) = 4$). With $k = 1$, we have $\zeta = \cos\left(\frac{\pi}{4}\right) + i\sin\left(\frac{\pi}{4}\right) = \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}$. So the primitive 8th roots of unity are

$$\zeta = \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2},\ \zeta^3 = -\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2},\ \zeta^5 = -\frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2},\ \zeta^7 = \frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2}.$$

Then $\Phi_8(x) = (x - \zeta)(x - \zeta^3)(x - \zeta^5)(x - \zeta^7)$. As shown in Exercise 55.1, this reduces to $\Phi_8(x) = x^4 + 1$.

Theorem 55.4. The Galois group of the nth cyclotomic extension of $\mathbb{Q}$ has $\phi(n)$ elements and is isomorphic to the group consisting of the positive integers less than n and relatively prime to n under multiplication modulo n.

Example 55.5. In Example 54.7, we saw that the splitting field K of $\Phi_8(x) = x^4+1$ satisfies $G(K/\mathbb{Q}) = \{\sigma_1, \sigma_3, \sigma_5, \sigma_7\}$ and $G(K/\mathbb{Q}) \cong G_8 = \langle\{1, 3, 5, 7\}, \cdot_8\rangle$.

Corollary 55.6. The Galois group of the pth cyclotomic extension of $\mathbb{Q}$ for a prime p is cyclic of order $p - 1$.

Note. We now have the equipment to address the construction of regular n-gons with a compass and straight edge. Notice that the central angle determined by a side of a regular n-gon is $2\pi/n$. So a regular n-gon is constructible if and only if angle $2\pi/n$ is constructible. By the Lemma to Theorem 32.11 (see the video supplement to Section 32), $2\pi/n$ is constructible if and only if $\cos(2\pi/n)$ is constructible. So a regular n-gon is constructible if and only if $\cos(2\pi/n)$ is constructible.

Definition. A prime number of the form $2^{(2^k)} + 1$ for non-negative integer k is a *Fermat prime.*

Note. The only known Fermat primes are 3, 5, 17, 257, and 65,537 which correspond to $k = 0, 1, 2, 3, 4$, respectively. For $5 \leq k \leq 19$, $2^{(2^k)} + 1$ is a composite number. It is unknown if $k = 20$ produces a composite or a prime number. It is unknown whether the number of Fermat primes is finite or infinite (see page 468).

Lemma 1. If the regular n-gon is constructible with a compass and straight edge then all odd primes dividing n are Fermat primes whose squares do not divide n.

Example 55.7. The regular 7-gon is the smallest (in terms of the number of sides) n-gon which is not constructible. Notice that for $n \leq 20$, the regular n-gon with $n \in \{7, 9, 11, 13, 14, 18, 19\}$ is not constructible.

Lemma 2. If all odd primes dividing n are Fermat primes whose squares do not divide n, then the regular n-gon is constructible with a compass and straight edge.

Note. Lemmas 1 and 2 combine to give us:

Theorem 55.8. The regular n-gon is constructible with a compass and straight edge if and only if all the odd primes dividing n are Fermat primes whose squares do not divide n.

Note. Euclid's *Elements* gives constructions of regular n-gons for $n \in \{3, 4, 5, 6, 15\}$. By combining these results, one could also construct n-gons for $n \in \{8, 10, 12, 16, 20\}$. By Theorem 55.8, this covers all admissible cases where $n \leq 20$, except for $n = 17$. Theorem 55.8 implies that a 17-gon is constructible, since 17 is a Fermat prime. As commented in the notes for Section 33, Gauss *showed* that a regular 17-gon can be constructed with a compass and straight edge. He did not actually give the construction, but only showed that it existed. The first explicit construction of a 17-gon was given by Ulrich von Huguenin in 1803. H. W. Richmond found a simpler version in 1893. (see page 136 of *Why Beauty is Truth: A History of Symmetry* by Ian Stewart, NY: Basic Books, 2007). It seems surprising that a question addressed in Euclid's *Elements* was picked up in the 19th century and taken taken further down the field!

Revised: 4/25/2014