Mathematics 352 – Abstract Algebra II
Discussion 3 – Which Regular Polygons are Constructible?
Due: April 30, 2008

Background

Building on the material from Chapter 15 we discussed before Easter, in this discussion, you will derive a complete answer to the question: which regular polygons in $\mathbb{R}^2$ that are constructible by straightedge and compass?

Discussion Questions

A) Show that the regular n-gon is constructible if and only if $[\mathbb{Q}(\zeta_n) : \mathbb{Q}]$ is equal to a power of 2, where $\zeta_n = e^{2\pi i/n}$. (Hint: $\zeta_n = \cos\left(\frac{2\pi}{n}\right) + i \sin\left(\frac{2\pi}{n}\right)$.)

B) Prove that $\mathbb{Q}(\zeta_n)$ is a Galois extension of $\mathbb{Q}$.

C) By looking at the Galois group $Gal_{\mathbb{Q}}(\mathbb{Q}(\zeta_n))$, deduce that the degree $[\mathbb{Q}(\zeta_n) : \mathbb{Q}]$ is equal to the number of integers m, $1 \leq m < n$, that are *relatively prime* to n. (Hint: You can use without proof the fact we mentioned in class that if $\phi_k(x)$ is the minimal polynomial of ζ_k over $\mathbb{Q}$) (the kth cyclotomic polynomial), then

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

Any element of the Galois group $Gal_{\mathbb{Q}}(\mathbb{Q}(\zeta_n))$ must take ζ_n to an nth root of 1 that is *not* a dth root of 1 for any $d < n$; do you see why?)

D) Show that if an integer of the form $2^k + 1$ is prime, then k must be a power of 2: $k = 2^r$ for some $r \geq 0$.

E) If the prime factorization of n in $\mathbb{Z}$ is

$$n = 2^\ell p_1^{e_1} \cdots p_k^{e_k} \ ,$$

where the p_i are odd, then the number of integers m, $1 \leq m < n$, relatively prime to n is given by

$$\phi(n) = 2^{\ell-1} p_1^{e_1-1}(p_1 - 1) \cdots p_k^{e_k-1}(p_k - 1),$$

(the *Euler ϕ-function*). Deduce from this statement and parts A) and D) that a regular n-gon is constructible by straightedge and compass if and only if n is equal to 2^ℓ times a product of *distinct* odd primes of the form $p = 2^{2^r} + 1$. This says, for instance, that the regular $11-$gon, the regular $13-$gon, the regular $19-$gon, etc. are not constructible by straightedge and compass.

Historical Note

The question of which regular polygons are constructible with straightedge and compass was another famous and long-standing problem going back to Euclid (or earlier). In the *Elements*, Proposition 1 is a construction of the equilateral triangle. Squres, regular pentagons, hexagons, octagons, decagons, dodecagons, etc. all have well-known constructions. The general question, though, remained unsolved until a complete answer was found by Gauss in the early 19th century. He was so proud of this work, in fact, that *asked to have a regular 17-gon, which is constructible, carved on his tombstone*! The stonemason he approached "talked him out of it," though, apparently saying that the design would be indistinguishable from a circle(!)

The odd primes in part E are called *Fermat primes*, after the 17th century French mathematician (and lawyer) Pierre de Fermat (of "Fermat's Last Theorem" fame). Only five of them are known to exist: $3 = 2 + 1$ (hence the equilateral triangle is constructible – Euclid's Proposition 1), $5 = 2^2 + 1$, $17 = 2^4 + 1$ (hence Gauss's 17-gon construction mentioned above!), $257 = 2^8 + 1$, and $65537 = 2^{16} + 1$. Fermat apparently thought that *all* the numbers $2^{2^r} + 1$ would be prime. But in fact, in all other cases where the prime factorization of $2^{2^r} + 1$ has been determined, it is a composite number! As of 2007, only the first 12 Fermat numbers have been completely factored, but some prime factors are known for many more of them. For instance,

$$2^{2^5} + 1 = 4294967297 = 641 \cdot 6700417,$$

(where both factors are prime) as was found *by hand* by Euler in 1732(!). Then

$$2^{2^6} + 1 = 67280421310721 \cdot 274177,$$

(both factors are prime), and

$$2^{2^7} + 1 = 5704689200685129054721 \cdot 59649589127497217$$

(both factors prime again). There can be more than two distinct prime factors (in fact this seems to be true for all $2^{2^r} + 1$ with $r \geq 9$). See `http://www.prothsearch.net/fermat.html` for what is know about factorizations of the Fermat numbers.