Mathematics 352 – Abstract Algebra II
Solutions for Discussion 3
April 28, 2008

A) The regular n-gon is constructible if and only if the point $\left(\cos\left(\frac{2\pi}{n}\right), \sin\left(\frac{2\pi}{n}\right)\right)$ is constructible, which is true in turn if and only if

$$\left[\mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right) : \mathbb{Q}\right] = 2^m \text{ and } \left[\mathbb{Q}\left(\sin\left(\frac{2\pi}{n}\right)\right) : \mathbb{Q}\right] = 2^{m'} \tag{1}$$

for some $m, m' \geq 0$.

Assume that (1) holds. Note that $x = i\sin\left(\frac{2\pi}{n}\right)$ is a root of the polynomial equation

$$x^2 + \left(1 - \cos^2\left(\frac{2\pi}{n}\right)\right) = 0.$$

For all $n > 2$, this polynomial is irreducible in $\mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right)[x]$ since it has no real roots but $\mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right) \subset \mathbb{R}$. Hence

$$\left[\mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right), i\sin\left(\frac{2\pi}{n}\right)\right) : \mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right)\right] = 2,$$

so

$$\left[\mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right), i\sin\left(\frac{2\pi}{n}\right)\right) : \mathbb{Q}\right] = 2^{m+1}.$$

Now $\mathbb{Q}(\zeta_n)$ is a subfield of $\mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right), i\sin\left(\frac{2\pi}{n}\right)\right)$ so $[\mathbb{Q}(\zeta_n) : \mathbb{Q}]$ is also a power of 2, since that degree must divide 2^{m+1}.

Conversely, assume that $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = 2^\ell$ for some $l \geq 0$. Note that

$$(\zeta_n)^{-1} = \cos\left(\frac{2\pi}{n}\right) - i\sin\left(\frac{2\pi}{n}\right),$$

so

$$\cos\left(\frac{2\pi}{n}\right) = \frac{1}{2}\left(\zeta_n + (\zeta_n)^{-1}\right)$$

is an element of $\mathbb{Q}(\zeta_n)$. It follows that $[\mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right) : \mathbb{Q}]$ divides 2^ℓ, hence is also a power of 2. Hence $\cos\left(\frac{2\pi}{n}\right)$ is constructible. Hence the point $\left(\cos\left(\frac{2\pi}{n}\right), \sin\left(\frac{2\pi}{n}\right)\right)$, and the regular n-gon are constructible.

B) The roots of $x^n - 1 = 0$ in $\mathbb{C}$ are $1, \zeta_n, \zeta_n^2, \ldots, \zeta_n^{n-1}$. Hence $\mathbb{Q}(\zeta_n) = \mathbb{Q}(1, \zeta_n, \zeta_n^2, \ldots, \zeta_n^{n-1})$ is the splitting field of $x^n - 1 \in \mathbb{Q}[x]$. By Theorem 10.15 in Hungerford, $\mathbb{Q}(\zeta_n)$ is a normal extension of $\mathbb{Q}$. It is also a separable extension of $\mathbb{Q}$, since $\mathbb{Q}$ has characteristic zero (Theorem 10.17). It is finite dimensional since $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] < n$. Therefore, $\mathbb{Q}(\zeta_n)$ is a Galois extension of $\mathbb{Q}$ by definition.

C) By the observations in part (B), we know that the roots of $x^n - 1 = 0$ in $\mathbb{C}$ are the numbers ζ_n^k for k with $0 \leq k < n$. Since $\mathbb{Q}(\zeta_n)$ is a Galois extension of $\mathbb{Q}$, it follows by the Fundamental Theorem of Galois Theory (Theorem 11.11) that

$$[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = |\mathrm{Gal}_{\mathbb{Q}}\mathbb{Q}(\zeta_n)|.$$

However, by Theorem 11.3, given k with $0 \leq k < n$, there exists $\sigma \in \mathrm{Gal}_{\mathbb{Q}}\mathbb{Q}(\zeta_n)$ with $\sigma(\zeta_n) = \zeta_n^k$ if and only if ζ and ζ_n^k have the same minimal polynomial, and then by Theorem 11.4 there is exactly one element of the Galois group for each such k. By the equation

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

we see that $\sigma \in \mathrm{Gal}_{\mathbb{Q}}\mathbb{Q}(\zeta_n)$ can only map ζ_n to other roots of the nth cyclotomic polynomial $\phi_n(x)$, since the roots of the other factors are all dth roots of unity for $d < n$. If $c = \gcd(k, n) > 1$, then $(\zeta_n^k)^c = 1$, so ζ_n^k is not a primitive nth root of unity. Hence the roots of $\phi_n(x)$ are precisely the ζ_n^k where $\gcd(n, k) = 1$, which implies what we wanted to show.

D) We will show the contrapositive: If $k > 1$ is not a power of 2, then $2^k + 1$ is not prime. If an integer $k > 1$ is not a power of 2, then it must be divisible by some odd prime $p \geq 3$. Say $k = pq$ where q is some other integer. But then we have, by the factorization of a sum of like odd powers:

$$2^{pq} + 1 = (2^q)^p + 1^p = (2^q + 1)((2^q)^{p-1} - (2^q)^{p-2} + \cdots - 2^q + 1).$$

(Since p is odd, the last term in the second factor here is always $+1$.) Since p is odd and ≥ 3, $2^q + 1 < 2^{pq} + 1$. Hence $2^{pq} + 1$ cannot be a prime because it is divisible by $2^q + 1$.

E) By the given formula for the Euler ϕ-function, if $n = 2^\ell p_1^{e_1} \cdots p_k^{e_k}$, where p_i are odd primes, the degree $[\mathbb{Q}(\zeta_n) : \mathbb{Q}]$, which equals the number of integers k with $1 \leq m < n$ that satisfy $\gcd(k, n) = 1$ by part (C), is given by the equation:

$$[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = 2^{\ell-1} p_1^{e_1-1}(p_1 - 1) \cdots p_k^{e_k-1}(p_k - 1). \tag{2}$$

If the regular n-gon is constructible then $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = 2^m$ for some $m \geq 0$. However (2) gives a factorization of $[\mathbb{Q}(\zeta_n) : \mathbb{Q}]$ and from this and the Unique Factorization Theorem in $\mathbb{Z}$ we see that all $e_i = 1$ (or else p_i divides the degree $[\mathbb{Q}(\zeta_n) : \mathbb{Q}]$) and each $p_i - 1$ must be a power of 2, so $p_i = 2^{2^{r_i}} + 1$ by part (D). This says that n must be a power of 2 times a product of distinct primes of the form $2^{2^r} + 1$.

Conversely, if n is a power of 2 times a product of *distinct* odd primes of the form $2^{2^r} + 1$, then (2) shows that $[\mathbb{Q}(\zeta_n) : \mathbb{Q}]$ equals a power of 2 since all the factors on the right hand side of (2) are powers of 2 (note that our assumptions ensure $e_i = 1$ for all i). Therefore the regular n-gon is constructible by part (A).