21-373, Algebraic Structures, Department of Mathematical Sciences, Carnegie Mellon University
Fall 2011: (Math Studies Section) Monday, Wednesday, Friday, 10:30 am, Porter Hall 226B.
Luc TARTAR, University Professor of Mathematics, Wean Hall 6212, tartar@cmu.edu

35- Wednesday November 30, 2011.

Lemma 35.1: Φ_n is irreducible in $\mathbb{Q}[x]$, so that $[\mathbb{Q}(e^{2i\,\pi/n}):\mathbb{Q}] = \varphi(n)$.
Proof: If n is a prime p, one can use Eisenstein criterion after a translation: $\Phi_p(x+1) = \frac{(x+1)^p-1}{x} = x^{p-1} + \sum_{j=1}^{p-1} \binom{p}{j} x^{j-1}$ so that all coefficients but the first are multiple of p, and the constant coefficient is p, hence not a multiple of p^2.

By Gauss's lemma, Φ_n is irreducible in $\mathbb{Q}[x]$ if and only if it is irreducible in $\mathbb{Z}[x]$ (since the content of a monic polynomial is 1). If Φ_n is reducible in $\mathbb{Z}[x]$, then $\Phi_n = f\,g$, with $f, g \in \mathbb{Z}[x]$ monic, and one may assume that f is irreducible. Let ξ be a primitive nth root of 1 which is a root of f, and let p be any prime not dividing n, so that ξ^p is another primitive nth root of 1, hence either a root of f or a root of g; one assumes that $g(\xi^p) = 0$ in order to arrive at a contradiction, and deduce then that $f(\xi^p) = 0$. Since $g(x^p)$ has ξ as a root, it must be a multiple of f, hence $g(x^p) = f(x)\,h(x)$ for some $h \in \mathbb{Z}[x]$, since one deals with monic polynomials and Euclidean division works. Reducing this equation modulo p, one obtains $\overline{g}(x^p) = \overline{f}(x)\,\overline{h}(x)$ in $\mathbb{Z}_p[x]$, but in $\mathbb{Z}_p[x]$ one has $\overline{g}(x^p) = \big(\overline{g}(x)\big)^p$, so that $\overline{g}^p = \overline{f}\,\overline{h}$, and since $\mathbb{Z}_p[x]$ is a PID hence a UFD, $\overline{f}$ and $\overline{g}$ have a common factor, and using $\overline{\Phi_n} = \overline{f}\,\overline{g}$, one deduces that $\overline{\Phi_n} \in \mathbb{Z}_p[x]$ has a repeated factor; the same is then true of $x^n - 1$, which is a multiple of $\overline{\Phi_n}$, but it is a contradiction since its derivative $n\,x^{n-1}$ is not 0 (since n is not a multiple of p), and the gcd of $x^n - 1$ and $n\,x^{n-1}$ in $\mathbb{Z}_p[x]$ is then 1.

Since this argument applies to every root of f, one may repeat the argument and one finds that ξ^m is a root of f for any integer $m = p_1 \cdots p_k$ for (not necessarily distinct) primes not dividing n, i.e. for any m relatively prime with n, and that means that ξ^m can be any of the $\varphi(n)$ primitive roots of 1, i.e. $f = \Phi_n$.

Remark 35.2: GAUSS had showed that if $n = 2^{2^k} + 1$ is a (Fermat) prime, one can construct a regular polygon with n sides by straightedge and compass, so that one can do it if $n = 2^\ell p_1 \cdots p_m$ if $p_1, \ldots, p_m$ are distinct Fermat primes. It was WANTZEL who proved that it is necessary, and this follows from Lemma 35.1, since it is necessary that the dimension of the cyclotomic extension over $\mathbb{Q}$ be a power of 2 for the construction of $e^{2i\,\pi/n}$ to be possible with straightedge and compass. Suppose that $n = 2^k q_1^{\alpha_1} \cdots q_\ell^{\alpha_\ell}$ (with $q_1, \ldots, q_\ell$ distinct primes and $\alpha_1, \ldots, \alpha_\ell \geq 1$) has the property that $\varphi(n)$ is a power of 2; then, since $\varphi(2^k q_1^{\alpha_1} \cdots q_\ell^{\alpha_\ell}) = \varphi(2^k)\,\varphi(q_1^{\alpha_1}) \cdots \varphi(q_\ell^{\alpha_\ell})$ and $\varphi(2^k) = 2^{k-1}$, it is necessary that $\varphi(q_i^{\alpha_i})$ is a power of 2 for $i = 1, \ldots, \ell$; since $\varphi(q_i^{\alpha_i}) = (q_i - 1)\,q_i^{\alpha_i - 1}$, it is a power of 2 if $q_i - 1$ is a power of 2, and $\alpha_i - 1 = 0$; then one notices that if $2^m + 1$ is prime, then m is a power of 2 (since $2^{a\,b} + 1$ is divisible by $2^b + 1$ if a is odd), i.e. each q_i is a Fermat prime, and it appears with power 1.

Lemma 35.3: If n is odd ≥ 3, then $\Phi_{2n}(x) = \Phi_n(-x)$, and $\Phi_2(x) = x + 1 = -\Phi_1(-x)$.
Proof: The formula for Φ_{2n} is true for $n = 3$ (and $n = 5, 7$ from the list in Remark 34.13), and one uses an induction upon n. Since n is odd, the divisors of $2n$ are the divisors d of n, and $2d$ for the divisors d of n, so that by Lemma 34.12 one has $\prod_{d|n} \Phi_d(x) = x^n - 1$ and $\prod_{d|n} \Phi_d(x)\,\Phi_{2d}(x) = x^{2n} - 1$, from which one deduces that $\prod_{d|n} \Phi_{2d}(x) = \frac{x^{2n}-1}{x^n-1} = x^n + 1$. Since $\prod_{d|n} \Phi_d(-x) = -x^n - 1$ (as n is odd), one deduces that $\prod_{d|n} \frac{\Phi_{2d}(x)}{\Phi_d(-x)} = -1$; for $d = 1$, the ratio $\frac{\Phi_2(x)}{\Phi_1(-x)}$ is -1, and then by the induction hypothesis the ratio $\frac{\Phi_{2d}(x)}{\Phi_d(-x)}$ is $+1$ for $1 < d < n$, so that the ratio $\frac{\Phi_{2n}(x)}{\Phi_n(-x)}$ is $+1$.

Lemma 35.4: (Möbius inversion formula) If $a_1, a_2, \ldots, a_n, \ldots \in E^*$ for a field E, and one defines the sequence $b_1, b_2, \ldots, b_m, \ldots \in E^*$ by $b_m = \prod_{d|m} a_d$ for all $m \geq 1$, then $a_n = \prod_{d|n} b_{n/d}^{\mu(d)}$ for all $n \geq 1$, where μ is the Möbius function.[1]
Proof: In the product $\prod_{d|n} b_{n/d}^{\mu(d)}$, if one replaces each $b_{n/d}$ by its definition as a product, one only finds values of a_j for j dividing n, and the exponent of a_j is $\sum_d \mu(d)$ for the values of d such that j divides $\frac{n}{d}$, i.e. d

[1] The Möbius function is defined by $\mu(1) = 1$ and if $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ for distinct primes $p_1, \ldots, p_k$, with $\alpha_1, \ldots, \alpha_k \geq 1$, by $\mu(n) = (-1)^k$ if $\alpha_j = 1$ for all j, and $\mu(n) = 0$ if $\alpha_j \geq 2$ for some j. It is used for inverting $g = 1 \star f$ by $f = \mu \star g$, so that $1 \star \mu = \delta$ the identity for convolution, i.e. $\delta(1) = 1$ and $\delta(m) = 0$ for $m \geq 2$.

divides $\frac{n}{j}$, so that the sum is $(1 \star \mu)\big(\frac{n}{j}\big)$, and then one uses $1 \star \mu = \delta$ defined by $\delta(1) = 1$ and $\delta(m) = 0$ for $m \geq 2$.

Lemma 35.5: If n is odd ≥ 1, $\Phi_{2^k n}(x) = \Phi_{2n}\big(x^{2^{k-1}}\big)$ for all $k \geq 1$, and more generally, if $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ for distinct primes $p_1, \ldots, p_k$, with $\alpha_1, \ldots, \alpha_k \geq 1$, and if r is the radical of n, i.e. $r = p_1 \cdots p_k$, then $\Phi_n(x) = \Phi_r(x^{n/r})$.

Proof: One applies Lemma 35.4 to Lemma 34.12, with $E = \mathbb{Q}(x)$, and $a_n = \Phi_n$ for all $n \geq 1$, so that $b_m = x^m - 1$ for all $m \geq 1$, and one obtains $\Phi_n(x) = \prod_{d|n}(x^{n/d} - 1)^{\mu(d)}$. Then one notices that $\mu(d) \neq 0$ imposes that no prime factor from $\{p_1, \ldots, p_k\}$ appears with exponent ≥ 2 in d, so that it means that d divides r, and it gives $\Phi_n(x) = \prod_{d|r}(x^{n/d} - 1)^{\mu(d)} = \prod_{d|r}(y^{r/d} - 1)^{\mu(d)}$ with $y = x^{n/r}$, i.e. $\Phi_n(x) = \Phi_r(y)$.