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

34- Monday November 28, 2011.

Definition 34.1: If E is a field, a *primitive* mth root of unity is an element $a \in E^*$ which generates a (cyclic) group of order m consisting of the m roots of $x^m - 1 = 0$.

Remark 34.2: If a primitive mth root of unity a exists, then there are $\varphi(m)$ primitive mth roots of unity, of the form a^k with $(k, m) = 1$.

For $E = \mathbb{C}$ (or any algebraically closed field) a primitive mth root of unity exists for every $m \geq 1$. For $E = \mathbb{R}$ or $E = \mathbb{Q}$, a primitive mth root of unity exists only for $m = 1, 2$.

Lemma 34.3: If E is a finite field with q elements (and $q = p^k$, where p is the characteristic of E and $k \geq 1$), then a primitive mth root of unity exists if and only if m divides $q - 1$.
Proof: Since the multiplicative group E^* is cyclic, it is generated by an element a, which has order $q-1$. If an mth root $b \neq 1$ exists, it means $b^m = 1$, and one writes $b = a^j$ for some j which is unique modulo $q-1$, so that one may choose $j \in \{1, \ldots, q-2\}$, and one defines $d = (m, q-1)$. Since $a^{m\,j} = b^m = 1$, $m\,j$ is a multiple of $q-1$, and if one writes $m = d\,n$, $q - 1 = d\,r$ with $(n, r) = 1$, one deduces that $n\,j$ is a multiple of r, so that j is a multiple of r since n and r are relatively prime; because a^r has order d, and the powers of b are among the powers of a^r, one deduces that there are at most d distinct powers of b. One deduces that if a primitive mth root $b \neq 1$ exists, then $m = d$ is a divisor of $q-1$. Conversely, if $q - 1 = m\,r$, then a^r is a primitive mth root.

Definition 34.4: A field extension F of E is called *simple* if $F = E(\theta)$ for some $\theta \in F$.

Lemma 34.5: If E is a finite field, then for any finite extension F of E with $[F\!:\!E] = \ell$, there exists $a \in F$ such that $\{1, a, \ldots, a^{\ell-1}\}$ is a power basis (of F as an E-vector space), hence $F = E(a)$.
Proof: Let a be any of the $\varphi(q-1)$ generators of the multiplicative group E^* (with $q = |E|$), and l Let P_a be the minimal polynomial of a (i.e. the monic irreducible polynomial satisfying $P_a(a) = 0$). One wants to show that P_a has degree ℓ. The $\ell + 1$ elements $1, a, \ldots, a^\ell$ are E-linearly dependent, since they belong to an E-vector space of dimension ℓ, and the non-zero E-linear combination which is 0 gives a polynomial Q of degree $\leq \ell$ such that $Q(a) = 0$, but Q is then a multiple of P_a, whose degree is then $\leq \ell$. If P_a had degree $d < \ell$, all the powers of a would be E-linear combinations of $1, a, \ldots, a^{d-1}$, and since these powers form all of E^*, one would deduce that the dimension of F over E is $\leq d$.

Lemma 34.6: If E is a finite field with q elements, and F is a field extension of E, then for every $a \in F$ which is algebraic over E, $\varphi_q(a)$ has the same minimal polynomial than a.
Proof: Since E is isomorphic to a splitting field extension for $x^q - x$ over $\mathbb{Z}_p$, one deduces that $\varphi_q(e) = e$ for all $e \in E$. If $a \in F$ is algebraic over E, it has a minimal polynomial $P \in E[x]$, but since the coefficients of P are fixed by φ_q which is a ring-homomorphism from F into itself, one finds that $P\big(\varphi_q(a)\big) = \varphi_q\big(P(a)\big) = 0$. Of course, this is just using the fact that $\varphi_q \in Aut_E(F)$.

Remark 34.7: Consider $E = \mathbb{Z}_2$ and F ($\simeq F_8$), so that $[F : E] = 3$, and since $\varphi(7) = 6$, all the non-zero elements except 1 generate F^*, and there are then two irreducible polynomials of degree 3 over $\mathbb{Z}_2$. Let ξ be any of these generators, so that the minimal polynomial of ξ is $P = (x - \xi)\,(x - \xi^2)\,(x - \xi^4)$, which has the form $x^3 + a\,x^2 + b\,x + 1$ (since $\xi^7 = 1$ and $-1 = 1$), and the minimal polynomial of ξ^3 is $Q = (x - \xi^3)\,(x - \xi^6)\,(x - \xi^{12})$, but since ξ^3 is the inverse of ξ^4, ξ^6 is the inverse of ξ, and $\xi^{12} = \xi^5$ is the inverse of ξ^2, one has $Q = x^3 P\big(\frac{1}{x}\big) = x^3 + b\,x^2 + a\,x + 1$. Then, since $x^7 - 1 = (x-1)\,P\,Q$, one has $P\,Q = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$, but the coefficient of x^5 in $P\,Q$ is then $a + b$, and $a + b = 1$ has the symmetric solutions $a = 1, b = 0$ or $a = 0, b = 1$, so that one finds that the two irreducible polynomials of degree 3 over $\mathbb{Z}_2$ are $x^3 + x^2 + 1$ and $x^3 + x + 1$.

Remark 34.8: Consider $E = \mathbb{Z}_2$ and F ($\simeq F_{16}$), so that $[F : E] = 4$, and since $\varphi(15) = \varphi(3)\varphi(5) = 2 \cdot 4 = 8$, there are 8 generators. Let ξ be any of these generators, so that the minimal polynomial of ξ is $P = (x - \xi)\,(x - \xi^2)\,(x - \xi^4)\,(x - \xi^8)$, which has the form $x^4 + a\,x^3 + b\,x^2 + c\,x + 1$ (since $\xi^{15} = 1$); the minimal polynomial of ξ^3 is $Q = (x - \xi^3)\,(x - \xi^6)\,(x - \xi^{12})\,(x - \xi^{24})$, but since $\xi^{24} = \xi^9$ and $\eta = \xi^3$ is a fifth root of unity different from 1, one has $Q = (x-\eta)\,(x-\eta^2)\,(x-\eta^3)\,(x-\eta^4) = \frac{x^5-1}{x-1} = x^4+x^3+x^2+x+1$; the minimal polynomial of ξ^5 is $R = (x-\xi^5)\,(x-\xi^{10})$ since $\xi^{20} = \xi^5$, and because $\zeta = \xi^5$ is a third root of unity different from 1, one has $R = (x-\zeta)\,(x-\zeta^2) = \frac{x^3-1}{x-1} = x^2+x+1$; the minimal polynomial of ξ^7 is $S = (x-\xi^7)\,(x-\xi^{14})\,(x-\xi^{28})\,(x-\xi^{56})$, but since ξ^7 is the inverse of ξ^8, ξ^{14} is the inverse of ξ, $\xi^{28} = \xi^{13}$ is the inverse of ξ^2, and $\xi^{56} = \xi^{11}$ is the inverse of ξ^4, one has $S = x^3 P\big(\frac{1}{x}\big) = x^4 + c\,x^3 + b\,x^2 + a\,x + 1$. There are then three irreducible polynomials of degree 4 over $\mathbb{Z}_2$.

One has $x^{15}-1 = (x-1)\,P\,Q\,R\,S$, and $(x-1)\,Q = x^5-1$, so that $P\,R\,S = \frac{x^{15}-1}{x^5-1} = x^{10}+x^5+1$ (by using $x^5 = y$), hence $P\,S = \frac{x^{10}+x^5+1}{x^2+x+1}$, and in $\mathbb{Z}_2[x]$ this quotient is $x^8+x^7+x^5+x^4+x^3+x+1$; identifying then the coefficients of powers x^7, x^6, x^5, x^4 (since those of x^3, x^2, x coincide then with those of x^5, x^6, x^7), one obtains $1 = a+c$, $0 = 2b + a\,c$, $1 = (a+c)\,(1+b)$, and $1 = a^2+b^2+c^2$ which gives the symmetric solutions $a = 1, b = 0, c = 0$ and $a = 0, b = 0, c = 1$, so that, besides $x^4+x^3+x^2+x+1$, the two other irreducible polynomials of degree 4 over $\mathbb{Z}_2$ are x^4+x^3+1 and x^4+x+1.

Remark 34.9: Using the monic irreducible polynomial $P = x^4+x+1 \in \mathbb{Z}_2[x]$ just obtained, one lets ξ be any of its four roots, and one uses the basis $1, \xi, \xi^2, \xi^3$ for F ($\simeq F_{16}$) over F_2, and since $\xi^4 = 1+\xi$ one constructs easily by induction the formula expressing ξ^j:

$$\begin{array}{ccc} \xi^4 = 1+\xi & \xi^8 = 1+\xi^2 & \xi^{12} = 1+\xi+\xi^2+\xi^3 \\ \xi^5 = \xi+\xi^2 & \xi^9 = \xi+\xi^3 & \xi^{13} = 1+\xi^2+\xi^3 \\ \xi^6 = \xi^2+\xi^3 & \xi^{10} = 1+\xi+\xi^2 & \xi^{14} = 1+\xi^3 \\ \xi^7 = 1+\xi+\xi^3 & \xi^{11} = \xi+\xi^2+\xi^3 & \xi^{15} = 1 \end{array}.$$

Remark 34.10: The preceding remarks show that all the irreducible polynomials of degree d over $\mathbb{Z}_p$ are obtained by considering a field extension F ($\simeq F_q$ with $q = p^d$) of $\mathbb{Z}_p$ with $[F:\mathbb{Z}_p] = d$, and considering the $\varphi(q-1)$ generators, which will correspond to $\frac{\varphi(q-1)}{d}$ such irreducible polynomials of degree d, but that some others may be associated to a non-zero element different from 1 which is not a generator, as in the case $q = 16$. Also, the product of these polynomials divide $x^{q-1}-1$, so that considering the factorization of x^n-1 for a general n is a natural question, which will be considered over $\mathbb{Z}[x]$.

Definition 34.11: The *cyclotomic field* of nth roots of unity over $\mathbb{Q}$ is the splitting field extension for x^n-1 over $\mathbb{Q}$, i.e. $\mathbb{Q}\big(e^{2i\,\pi/n}\big)$ $\big(= \mathbb{Q}\big[e^{2i\,\pi/n}\big]\big)$.

The nth *cyclotomic polynomial* Φ_n is defined by $\Phi_n(x) = \prod_{primitive}(x-\xi_k)$, where the product is taken over the primitive nth roots of unity ξ_k, so that the degree of Φ_n is $\varphi(n)$, where φ is the Euler function.

Lemma 34.12: For all $n \ge 1$, $x^n-1 = \prod_{d|n}\Phi_d(x)$, Φ_n is monic, and $\Phi_n \in \mathbb{Z}[x]$.

Proof: If $1 \le k \le n-1$, then $(k,n) = \delta$ and $d = \frac{n}{\delta}$ are divisors of n, and $e^{2i\,\pi\,k/n}$ is a primitive dth root of unity. Since $x^n-1 = \prod_{0\le k\le n}(x-e^{2i\,\pi\,k/n})$, and $\Phi_1 = x-1$, by grouping the terms $(x-e^{2i\,\pi\,k/n})$ for k a dth root of unity, which must be a divisor of n, one obtains the formula $x^n-1 = \prod_{d|n}\Phi_d(x)$, a consequence of which is $n = \sum_{d|n}\varphi(d)$ by comparing degrees.[1] That the coefficients are integers is easily derived from the formula by induction on n, observing first that it is true for Φ_1 and for $\Phi_p = x^{p-1}+\ldots+1$ when p is a prime; then, one has $x^n-1 = \Psi_n\Phi_n$ and Ψ_n is the product of Φ_d for $d < n$ a divisor of n, so that by induction $\Psi_n \in \mathbb{Z}[x]$, and then since Ψ_n is monic, the Euclidean division of x^n-1 by Ψ_n gives a quotient and a remainder (here 0) in $\mathbb{Z}[x]$.

Remark 34.13: For p prime $\Phi_p = x^{p-1}+\ldots+1$, and for the first composite n, the formula gives $\Phi_4 = x^2+1$, $\Phi_6 = x^2-x+1$, $\Phi_8 = x^4+1$, $\Phi_9 = x^6+x^3+1$, $\Phi_{10} = x^4-x^3+x^2-x+1$, $\Phi_{12} = x^4-x^2+1$, $\Phi_{14} = x^6-x^5+x^4-x^3+x^2-x+1$, $\Phi_{15} = x^8-x^7+x^5-x^4+x^3-x+1$, $\Phi_{16} = x^8+1$, and one observes some simple properties, which will be proved later to be general.

One may think that the coefficients are always -1, 0, or $+1$, but it is not the case: the smallest value of n for which it is not true is $n = 105$, and Φ_{105} has a coefficient equal to -2; $105 = 3\cdot5\cdot7$ is the smallest odd integer with three distinct prime factors, and if n has at most two distinct odd prime factors, then one can show that the coefficients of Φ_n belong to $\{-1, 0, +1\}$.

[1] A consequence of this formula is $\sum_n \frac{n}{n^s} = \sum_n \frac{\varphi(n)}{n^s}\sum_n \frac{1}{n^s}$, i.e. $\sum_n \frac{\varphi(n)}{n^s} = \frac{\zeta(s-1)}{\zeta(s)}$, valid for $\Re(s) > 2$.