Thm: If F is a field, $G \leq F^\times$, and $|G| < \infty$, then G is cyclic.

Pf: FTFAG $\Rightarrow$ $G \cong \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}$ for some

$k \in \mathbb{N}$, $n_1, \dots, n_k \in \{2, 3, \dots\}$, $n_i \mid n_{i+1}$, $1 \leq i < k$.

Every element $\alpha \in G$ is a root of $x^{n_k} - 1 \in F[x]$.

Since the # of roots of this poly. in F is at most n_k,

we have $k = 1$, so G is cyclic. $\blacksquare$

Cor: $\mathbb{F}_{p^n}^\times$ is cyclic.

Thm: Any finite extension of finite fields is a simple extension.

Pf: Suppose K/F, $|K| < \infty$. Then $K \cong \mathbb{F}_{p^n}$, so $\exists\, \alpha \in K$

s.t. $K^\times = \langle \alpha \rangle$. Then $K = F(\alpha)$. $\blacksquare$

Cor: If F is a finite field and $n \in \mathbb{N}$, there is an irreducible

poly in F of degree n.

Pf: Suppose $|F| = p^m$. Then F is isomorphic to a subfield

of $K = \mathbb{F}_{p^{mn}}$, and $[K:F] = n$. By the thm. above,

$K = F(\alpha)$ for some $\alpha \in K$. Then

$$\deg(\min_F(\alpha)) = [F(\alpha):F] = n, \text{ so}$$

$\min_F(\alpha)$ is an irred. poly in $F[x]$ w/ degree n. $\blacksquare$

Cyclotomic polynomials

The nth roots of unity in $\mathbb{C}$ are

$$\mu_n = \{z \in \mathbb{C} : z^n = 1\} = \{e^{2\pi i a/n} : 1 \le a \le n\}.$$

They are a (multiplicative) cyclic group, and any generator is called a primitive nth root of unity.

The set of primitive nth roots of unity is

$$\{e^{2\pi i a/n} : 1 \le a \le n, (a,n)=1\}.$$

The nth cyclotomic polynomial is

$$\Phi_n(x) = \prod_{\substack{a=1 \\ (a,n)=1}}^{n} (x - e^{2\pi i a/n}) \in \mathbb{C}[x].$$

Observations:

1) $\deg \Phi_n(x) = \varphi(n)$ ← Euler phi function, $\Phi_n(x)$ is monic.

2a) $x^n - 1 = \prod_{d \mid n} \Phi_d(x)$ (every nth root of unity is a prim. dth root of unity for some $d \mid n$).

b) $n = \sum_{d \mid n} \varphi(d)$

3) $\Phi_1(x) = x - 1$

$\Phi_2(x) = x + 1$

$$\Phi_3(x) = \prod_{\substack{a=1 \\ (a,3)=1}}^{3} (x - e^{2\pi i a/3}) = (x - e^{2\pi i/3})(x - e^{4\pi i/3}) = \frac{x^3 - 1}{x - 1} = x^2 + x + 1.$$

If $n=p$ is prime then

$$\Phi_p(x) = \frac{x^p - 1}{x-1} = x^{p-1} + x^{p-2} + \cdots + x + 1. \quad \text{(irreducible)}$$

$n=4$:

$$x^4 - 1 = \prod_{d \mid 4} \Phi_d(x) = \Phi_1(x)\Phi_2(x)\Phi_4(x)$$

$$= (x-1)(x+1)\Phi_4(x)$$

$$\Rightarrow \Phi_4(x) = x^2+1$$

$n=6$: $x^6 - 1 = \Phi_1(x)\Phi_2(x)\Phi_3(x)\Phi_6(x)$

$$= (x-1)(x+1)(x^2+x+1)\Phi_6(x)$$

$$= (x^2-1)(x^2+x+1)\Phi_6(x)$$

$$= (x^4+x^3-x-1)\Phi_6(x)$$

$$\begin{array}{r|l} & x^2 - x + 1 \\ \hline x^4+x^3-x-1 & x^6 - 1 \\ & -(x^6 + x^5 - x^3 - x^2) \\ \hline & -x^5 + x^3 + x^2 - 1 \\ & -(-x^5 - x^4 + x^2 + x) \\ \hline & x^4 + x^3 - x - 1 \end{array}$$

$$\Rightarrow \Phi_6(x) = x^2 - x + 1.$$

$\vdots$

Note: • Coeffs. of Φ_n appear to always be integers.

• Φ_n appears to always be irred.

Thm: $\forall n \in \mathbb{N}$, $\Phi_n \in \mathbb{Z}[x]$.

Pf: Induction on n. True for n=1. Suppose true for $1 \leq m < n$.

Then $x^n - 1 = \prod_{d \mid n} \Phi_d(x) = \Phi_n(x) f(x)$ $(*)$, where $f \in \mathbb{Z}[x]$

by the inductive hypothesis.

By the div. alg. in $\mathbb{Q}[x]$, $\exists q, r \in \mathbb{Q}[x]$ s.t.

$$x^n - 1 = q(x) f(x) + r(x), \text{ and } r = 0 \text{ or } \deg r < \deg f.$$

If $r \neq 0$ then this would also satisfy the div alg.

over $\mathbb{Q}(\zeta_n)[x]$, $\zeta_n = e^{2\pi i/n}$, but that would contradict the

uniqueness of the remainder in the div. alg. (by $(*)$).

(cont. next time...)