Cyclotomic Extensions.

Loosely speaking a cyclotomic extension of a field k is a field $k(\zeta)$ where $\zeta^n = 1$. Cyclotomic extensions have abelian Galois groups, and cyclotomic extensions are pretty much the only method of constructing such over arbitrary fields.

Recall: $X^n - 1$ is separable over k

$$\iff \begin{cases} \text{char } k = 0 \\ \text{or} \\ \text{char } k \nmid n. \end{cases}$$

Which we will assume from now on.

Then the set μ_n of roots of $X^n - 1$ has n elements and is a cyclic group.

Thus $k(\mu_n)$ is the splitting field of $X^n - 1$ and thus a Galois extension of k.

We are going to determine $\mathrm{Gal}(k(\mu_n)/k)$ in two cases, namely $k = \mathbb{Q}$ and $k = \mathbb{F}_p$.

Now let ζ be a <u>primitive n'th root of 1</u> that is, a generator of μ_n. Hence

$$\begin{array}{ccc} \mathbb{Z}/n\mathbb{Z} & \longrightarrow & \mu_n \\ k & \longmapsto & \zeta^k \end{array}$$

is an isomorphism.

Any automorphism $\sigma \in \mathrm{Aut}(\mu_n)$ is determined by $\sigma(\zeta) = \zeta^a$, $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ and this establishes an isomorphism

$$\mathrm{Aut}(\mu_n) \xrightarrow{\sim} (\mathbb{Z}/n\mathbb{Z})^\times.$$

Thus we obtain an injective group homomorphism:

$$\mathrm{Gal}(\mathbb{Q}(\mu_n)/\mathbb{Q}) \longrightarrow (\mathbb{Z}/n\mathbb{Z})^\times$$
$$\sigma \longmapsto a_\sigma$$

where $\sigma(\zeta) = \zeta^{a_\sigma}$.

The following proof is due to Dedekind (1857)

Thm IV.26 $\mathrm{Gal}(\mathbb{Q}(\mu_n)/\mathbb{Q}) \longrightarrow (\mathbb{Z}/n\mathbb{Z})^\times$ is an isomorphism.

Proof: Let ζ be a primitive n'th root of 1 and ζ^a, $(a,n)=1$ another such. Let f be the min. pol of ζ and g the min. polyn. of ζ^a (both over $\mathbb{Q}$). We will show that $f=g$.

Since $\mathbb{Q}(\mu_n) = \mathbb{Q}(\zeta) = \mathbb{Q}(\zeta^a)$ this will imply the existence of $\sigma \in Gal(\mathbb{Q}(\mu_n)/\mathbb{Q})$ with $\sigma(\zeta) = \zeta^a$ and prove the theorem.

The first observation is that we may assume a to be a prime $p \nmid n$.

Indeed: writing $a = p_1 \cdots p_r$ we have that the successive pairs

$$\zeta, \zeta^{p_1}, \zeta^{p_1 p_2}, \cdots, \zeta^{p_1 \cdots p_r} = \zeta^a$$

have same minimal polynomial.

Thus let ζ be any primitive n^{th} root of 1 and p a prime not dividing n.

Assume that $f = irr(\zeta, \mathbb{Q})$ and $g = irr(\zeta^p, \mathbb{Q})$ are different:

$$f \neq g.$$

Observe that any monic factor of $X^n - 1$ that is in $\mathbb{Q}[X]$ is in $\mathbb{Z}[X]$ (Gauss).

Thus $f, g \in \mathbb{Z}[X]$ and since $f \neq g$ we have

$$X^n - 1 = f(X)\, g(X)\, h(X)$$

with $h \in \mathbb{Z}[X]$.

Reduce everything modulo p:

$$X^n - 1 = \bar{f}(X)\, \bar{g}(X)\, \bar{h}(X)$$

in $\mathbb{F}_p[X]$.

Since $X^n - 1$ has no repeated roots, $\bar{f}, \bar{g}$ are coprime. Also $\bar{f}, \bar{g}$ are not constant (!) since f, g are monic of $\deg > 0$.

But: $g(\zeta^p) = 0$, hence $g(X^p)$ has ζ as a root which implies that

$$g(x^p) = f(x)\,k(x), \qquad k \in \mathbb{Z}[x]$$

monic.

Thus

$$\bar{g}(x^p) = \bar{f}(x)\,\bar{k}(x)$$

But: $\bar{g}(x^p) = \bar{g}(x)^p$

$$= \bar{f}(x)\,\bar{k}(x)$$

which contradicts that $\bar{g}$ and $\bar{f}$ are relatively prime. ∎

Def. IV.27 The n'th cyclotomic polynomial is

$$\Phi_n(x) := \prod_{(a,n)=1} (x - \zeta^a)$$

i.e. the product is over all primitive n'th root of 1.

Corollary IV.28 $\Phi_n \in \mathbb{Z}[X]$ and is irreducible

Proof: By the above thm., and since $\mathbb{Q}(\mu_n) = \mathbb{Q}(\zeta)$ we have that

$$\Phi_n(X) = \prod_{\sigma \in Gal(\mathbb{Q}(\mu_n)/\mathbb{Q})} (X - \sigma(\zeta))$$

and hence by Galois theory $\Phi_n \in \mathbb{Q}[X]$; it is also the minimal polynomial of ζ, for instance since Gal acts transitively on its roots. In addition since $\zeta^n - 1 = 0$, Φ_n divides $X^n - 1$ and hence by Gauss's lemma $\Phi_n \in \mathbb{Z}[X]$. ∎

Degree of ϕ_n : $\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$

By Chinese Remainder, if $(n,m)=1$,

$$\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}/nm\mathbb{Z} \quad \text{as rings (!)}$$

hence $\varphi(nm) = \varphi(n)\varphi(m)$.

And $\varphi(p^r) = p^r - p^{r-1} = p^{r-1}(p-1)$.

Here is the list of the first ten cyclotomic polynomials:

$\phi_1(T) = T-1$ $\qquad$ $\phi_2(T) = T+1$

$\phi_3 = T^2+T+1$ $\qquad$ $\phi_4 = T^2+1$

$\phi_5 = T^4+\cdots+1$ $\qquad$ $\phi_6 = T^2-T+1$

$\phi_7 = T^6+\cdots+1$ $\qquad$ $\phi_8 = T^4+1$

$\phi_9 = T^6+T^3+1$ $\qquad$ $\phi_{10} = T^4-T^3+T^2-T+1$.

etc..., one has to wait for ϕ_{105} to see a coefficient not $1, 0, -1$.

Here are a few properties:

Prop. IV. 29

(1) $T^n - 1 = \prod_{d \mid n} \Phi_d(T)$

(2) $\Phi_n(T) = T^{\varphi(n)} \Phi_n\left(\frac{1}{T}\right)$, $n \geq 2$

(3) $\Phi_p(T) = T^{p-1} + \cdots + 1$

(4) $\Phi_{p^r}(T) = \Phi_p(T^{p^{r-1}})$

(5) n odd: $\Phi_{2n}(T) = \Phi_n(-T)$

(6) $\Phi_{p_1^{r_1} \cdots p_k^{r_k}}(T) = \Phi_{p_1 \cdots p_k}(T^{p_1^{r_1-1} \cdots p_k^{r_k-1}})$.

Proof:

(1) ~~Array~~ $T^n - 1 = \prod_{\zeta \in \mu_n} (T - \zeta)$.

But now any $\zeta \in \mu_n$ is a primitive

d'th root for some $d \mid n$. Group the factors according to primitive d'th roots to obtain (1).

(2) [illegible]

First one shows that for $n \geq 2$: $\phi_n(0) = 1$.

This is done by recurrence on n, observing

$$\prod_{\substack{d \mid n \\ d > 1}} \phi_d(0) = 1.$$

and observing $\phi_p(T) = T^{p-1} + \cdots + 1$

(Eisenstein).

Then one just computes $\phi_n(T) =$

$$= \prod_{\zeta^{p^n}=1,\ \zeta\neq 1} (T-\zeta) = T^{\varphi(p^n)} \prod_{\zeta^{p^n}=1,\ \zeta\neq 1} (1-\zeta T^{-1})$$

$$= T^{\varphi(p^n)} \underbrace{\prod_{\zeta^{p^n}=1,\ \zeta\neq 1} (-\zeta)}_{\phi_n(0)} \underbrace{\prod_{\zeta^{p^n}=1,\ \zeta\neq 1} (T^{-1}-\zeta)}_{\phi_n(T^{-1})}$$

$$\phi_n(0) = 1.$$

(3) Use Eisenstein applied to $\phi_n(T+1)$.

□

Remark: One of the deep theorems in the subject is Kronecker-Weber that says that any abelian extension of $\mathbb{Q}$ is contained in a cyclotomic extension.

Now we turn to the case $\mathbb{F}_p$ for p th.

Theorem IV.30

Assume p th. Then the image of $Gal(\mathbb{F}_p(\mu_n)/\mathbb{F}_p) \longrightarrow (\mathbb{Z}/n\mathbb{Z})^\times$ is the (cyclic) subgroup generated by p mod n.

Proof: Recall: pick $\langle \zeta \rangle = \mu_n$, then $\sigma \mapsto a$ is given by $\sigma(\zeta) = \zeta^a$.

Now $\mathbb{F}_p(\mu_n)$ is a finite extension of $\mathbb{F}_p$ and hence $Gal(\mathbb{F}_p(\mu_n)/\mathbb{F}_p) \cong \langle \varphi_p \rangle$ where $\varphi_p(\xi) = \xi^p$ is the Frobenius automorphism. Now just observe that

$$\varphi_p \longmapsto p. \qquad \square$$

Corollary IV.31 : if $p \nmid n$:

$$\left[F_p(\mu_n) : F_p \right] = \text{Order of } p \text{ in } \left(\mathbb{Z}/n\mathbb{Z}\right)^\times.$$

Concerning the structure of $\left(\mathbb{Z}/n\mathbb{Z}\right)^\times$

we have

Thm. IV.32 :

(1) p odd $\quad \left(\mathbb{Z}/p^r\mathbb{Z}\right)^\times \simeq \mathbb{Z}/p^{r-1}\mathbb{Z} \times \mathbb{Z}/(p-1)\mathbb{Z}$

and hence is cyclic since $(p-1, p^{r-1}) = 1$.

(2) $\left(\mathbb{Z}/2^r\mathbb{Z}\right)^\times \simeq \mathbb{Z}/2\mathbb{Z} \times \left(\mathbb{Z}/2^{r-2}\mathbb{Z}\right)$ and

as a result is only cyclic if $r = 1, 2$.

Example IV.33 :

$n = 7$: $\left(\mathbb{Z}/7\mathbb{Z}\right)^{\times} = \{1, 2, 3, 4, 5, 6\} \simeq \mathbb{Z}/6\mathbb{Z}$.

and the possible orders are

$$1, 2, 3, 6$$

They are all realized :

(1) $p = 2$: $2^3 = 8 \equiv 1$, order 3.

So $\left[\mathbb{F}_2(\mu_7) : \mathbb{F}_2\right] = 3$.

And $\phi_7(T) = (T^3 + T + 1)(T^3 + T^2 + 1)$

in $\mathbb{F}_2[T]$.

(2) $p = 3$: Order 6 and

ϕ_7 mod 3 is irreducible.

(3) $p = 13$: Order 2, $13^2 = 169 = 24 \cdot 7 + 1$.

$$\phi_7(T) = (T^2 + 3T + 1)(T^2 + 5T + 1)(T^2 + 6T + 1)$$

(4) $p = 29$: Order 1.

$$\phi_7(T) = (T-7)(T-16)(T-20)(T-23)(T-24)(T-25)$$

Thm IV.34 : If $p \nmid n$ then the (monic) irreducible factors of ϕ_n in $\mathbb{F}_p[X]$ are all distinct and have the same degree, equal to the order of $p \bmod n$ in $(\mathbb{Z}/n\mathbb{Z})^\times$.

Proof : Since $p \nmid n$, $T^n - 1$ has no repeated roots and hence so does $\phi_n(T)$. This implies the first statement.

The second will follow from the fol. claim: let α be a root of ϕ_n in ~~some~~ extension. $F_p(\mu_n)$. Then α is a primitive n'th root of 1:

Otherwise $\alpha^m = 1$ with $m < n$ and $m \mid n$. Since

$$T^m - 1 = \prod_{d \mid m} \phi_d(T)$$

we got $\exists\, d \mid m$, $\phi_d(\alpha) = 0$.

But now $T^n - 1 = \phi_n(T) \prod_{\substack{d \mid n \\ d < n}} \phi_d(T)$

Which makes α a multiple root of $T^n - 1$. Contradiction.

Since ~~Thus~~ $F_p(\mu_n) = F_p(\alpha)$ for any α prim. n'th root, we have the conclusion.

□

A rather deep thm. of Dirichlet states that given $(a,n) = 1$ there are infinitely many primes $p \equiv a \pmod{n}$. We can use the properties of cyclotomic polynomials to prove

Thm IV.35 : $n \in \mathbb{N}^*$: There are ∞-many primes $p \equiv 1 \pmod{n}$.

Proof:

It suffices to show that $\forall n \; \exists p \equiv 1 \pmod{n}$.

Indeed: if $p_1, \dots, p_t$ are primes $\equiv 1 \pmod{n}$ let $p \equiv 1 \pmod{n \cdot p_1 \cdots p_t}$. Then $p \equiv 1 \pmod{n}$ and clearly $p \neq p_1, \dots, p_t$. Since

$$p \equiv 1 \pmod{p_i}$$

First, when $n \geq 3$, $|\Phi_n(n)| > 1$.

Indeed: $|\Phi_n(n)| = |\prod(n-\zeta)|$

$$\geq \Pi(n-1) \geq \Pi 2 > 1.$$

Now we show that for every prime

$p \mid \Phi_n(n)$, $p \equiv 1 \pmod n$.

First: since $\Phi_n(0) = \pm 1$ (in fact 1 here)

$p \nmid n$. Next, since $\Phi_n(x) \mid x^n - 1$

$p \mid \Phi_n(n) \mid n^n - 1$ hence

$$n^n = 1 \text{ in } \mathbb{F}_p^\times.$$

Let t = order of n in $\mathbb{F}_p^\times$.

Clearly $t \mid n$, and we claim $t = n$.

This implies $n \mid p-1$ and we are done.

By contradiction: $t < n$, $t \mid n$.

Then $$\frac{x^n - 1}{x^t - 1} = \Phi_n(x) \cdot \prod_d \Phi_d(x)$$

where d runs through all proper divisors of n that do not divide t.

Hence $$\Phi_n(n) \mid \frac{n^n - 1}{n^t - 1}.$$

But $$\frac{n^n - 1}{n^t - 1} = \frac{(n^t)^{n/t} - 1}{n^t - 1} = \underbrace{(n^t)^{\frac{n}{t}-1} + \cdots + 1}_{\frac{n}{t} \text{ terms}}$$

$$\equiv \underbrace{1 + \cdots + 1}_{\frac{n}{t}} \pmod{p}.$$

$\Rightarrow p \mid \frac{n}{t} \Rightarrow p \mid n$. Contr. ∎