dass
$$\prod_{\substack{d \mid n \\ d > 1}} \Phi_d(0) = 1. \quad (*)$$

Aus $\Phi_p(0) = 1$ folgt mittels $(*)$ und Induktion über n, dass für $n \geq 2$:
$$\Phi_n(0) = 1.$$

$\boxed{\S}$

Wir enden diesen Abschnitt mit:

<u>Thm IV.30</u>:

Falls $(p, n) = 1$ dann ist das Bild
$$\mathrm{Gal}(\mathbb{F}_p[n]/\mathbb{F}_p) \longrightarrow \left(\mathbb{Z}/_{n\mathbb{Z}}\right)^{\times}$$
die durch $p \bmod n$ erzeugte zyklische Untergruppe.

<u>Beweis</u>: Wir wissen, dass $\mathrm{Gal}(\mathbb{F}_p[n]/\mathbb{F}_p) = \langle \varphi_p \rangle$, erzeugt vom Frobenius

Automorphismus $\varphi_p(\zeta) = \zeta^p$. Angewendet auf ζ = n^{te} Primitive Einheitswurzel von 1 zeigt: Unter obiger Abbildung geht φ_p zu

$p \in (\mathbb{Z}/n\mathbb{Z})^\times$ $\boxed{\zeta}$

<u>Korollar IV.31</u> Falls $(p,n) = 1$ so folgt:

$[\mathbb{F}_p[n] : \mathbb{F}_p] =$ ~~Ordnung~~, Exponent von $p \bmod n$ in $(\mathbb{Z}/n\mathbb{Z})^\times$.

Was die Struktur der Gruppe $(\mathbb{Z}/n\mathbb{Z})^\times$ angeht gilt:

<u>Thm IV.32</u> (1) $(n,m) = 1$, $(\mathbb{Z}/mn\mathbb{Z})^\times \cong (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$

(2) p ungerade Primzahl:

$$(\mathbb{Z}/p^r\mathbb{Z})^\times \cong \mathbb{Z}/p^{r-1}\mathbb{Z} \times \mathbb{Z}/(p-1)\mathbb{Z}$$

(3) $\left(\mathbb{Z}/_{2^s\mathbb{Z}}\right)^{\times} \cong \mathbb{Z}/_{2\mathbb{Z}} \times \left(\mathbb{Z}/_{2^{s-2}\mathbb{Z}}\right)$.

Beispiele IV.33

$n = 7$ $\quad \left(\mathbb{Z}/_{7\mathbb{Z}}\right)^{\times} = \{1, 2, 3, 4, 5, 6\} \cong \mathbb{Z}/_{6\mathbb{Z}}$

Die möglichen Exponenten sind:

$$1, 2, 3, 6.$$

① $p = 2$: $\quad 2^3 = 8 \equiv 1$, Exponent 3

So ist

$$[\mathbb{F}_2[\zeta_7] : \mathbb{F}_2] = 3$$

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

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

② $\underline{p=3}$: Exponent 6. Folglich ist Φ_7 mod 3 irreduzibel!

③ $\underline{p=13}$: Ordnung 2;

$$13^2 = 169 = 24 \cdot 7 + 1.$$

$$\Phi_7(T) = (T^2+3T+1)(T^2+5T+1)(T^2+6T+1)$$

④ $\underline{p=29}$: Ordnung 1.

$$\Phi_7(T) = (T-7)(T-16)(T-20)(T-23)(T-24).$$
$$(T-25).$$

$\underline{\text{Thm IV. 34}}$ Falls $(p,n)=1$, dann sind die (unitären) irreduziblen Faktoren von Φ_n in $\mathbb{F}_p[X]$ alle verschieden und haben den selben Grad, nämlich die Ordnung von p modulo n in $(\mathbb{Z}/_{n\mathbb{Z}})^\times$.

Beweis:

Da $X^n - 1$ keine mehrfachen Nullstellen besitzt gilt das selbe für $\Phi_n(X)$. Also müssen alle irreduziblen Faktoren verschieden sein.

Zur zweiten Behauptung: da $\mathbb{F}_p[\eta]$ ein Zerf.-Körper von $X^n - 1$ ist, zerfällt insbesondere $\Phi_n(X)$ in lineare Faktoren in $\mathbb{F}_p[\eta][X]$. Also sind die irreduziblen Faktoren von $\Phi_n(X)$ in $\mathbb{F}_p[X]$ von der Form

$$\operatorname{irr}(\alpha, \mathbb{F}_p)$$

wobei ~~$\Phi_n(\alpha)$~~ $\alpha \in \mathbb{F}_p[\eta]$, $\Phi_n(\alpha) = 0$.

Es genügt also zu zeigen, dass falls

$\phi_n(\alpha) = 0$ (mit $\alpha \in \mathbb{F}_p[n]$) dann ist α n^{te} primitive Einheitswurzel:

denn dann folgt $\mathbb{F}_p[n] = \mathbb{F}_p(\alpha)$ und $\operatorname{irr}(\alpha, \mathbb{F}_p)$ hat Grad $[\mathbb{F}_p[n] : \mathbb{F}_p]$.

Sei also $\Phi_n(\alpha) = 0$. Falls α nicht primitive n^{te} 1-Wurzel ist, gibt es $1 \leq m < n$ mit:

$$\alpha^m = 1 \text{ und } m \text{ teilt } n.$$

Da nach Satz IV. 29 (1):

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

folgt, dass es $d_0 \mid m$ gibt mit:

$$\phi_{d_0}(\alpha) = 0.$$

Nun ist (IV. 29 (1)):

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

Da $d_0 \mid m$ und somit echter Teiler von n ist, folgt, dass α mindestens doppelte Nullstelle von $X^n - 1$ ist. Ein Widerspruch.

$\boxed{\xi}$

Ein tiefliegender Satz von Dirichlet besagt, dass gegeben $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ es unendlich viele Primzahlen p gibt mit $p \equiv a \mod n$.

Mit $a = 1$ impliziert dieser Satz, dass es unendlich viele Primzahlen p gibt so dass $\phi_n \bmod p$ in $\mathbb{F}_p[x]$ in lineare Faktoren zerfällt.

Diesen Spezialfall von Dirichlet's Theorem können wir mittels Eigenschaften von Zyklotomischen Polynome beweisen.

Der allgemeine Fall benötigt Instrumente aus der Analytischen Zahlentheorie.

<u>Thm IV. 35</u> Sei $n \in \mathbb{N}^*$. Dann gibt es unendlich viele Primzahlen

$$p \equiv 1 \mod n.$$

<u>Beweis:</u>

Genügt zu zeigen: $\forall n \geq 1 \ \exists p$ Primzahl mit $p \equiv 1 \bmod n$.

In der Tat, falls $p_1, \ldots, p_t$, $t \geq 1$ Primzahlen sind mit

$$p_i \equiv 1 \mod n \qquad 1 \leq i \leq t$$

sei dann p eine Primzahl mit

$$p \equiv 1 \mod n \cdot p_1 \cdots p_t \quad . \quad (*)$$

Dann ist insbesondere

$$p \equiv 1 \mod n$$

und $p \notin \{p_1, \ldots, p_t\}$ da aus $(*)$ folgt: $p \equiv 1 \mod p_i \qquad 1 \leq i \leq t$.

Vorbereitende Bemerkung: falls $n \geq 3$ so ist $|\phi_n(n)| \geq 2$:

$$|\phi_n(n)| = \prod |n - \zeta| \geq \prod (n-1) \geq \prod 2 \geq 2 .$$

Also ist für jedes $n \geq 3$, $\phi_n(n) \in \mathbb{Z}$ eine ganze Zahl ~~mit einer~~ $\neq \pm 1$

und enthält also Primzahlfaktoren.

Behauptung: Falls die Primzahl p die ganze Zahl $\Phi_n(n)$ teilt, folgt

$$p \equiv 1 \mod n.$$

Aus dieser Behauptung folgt, dass es $\forall n \geq 3$ eine Primzahl p gibt mit $p \equiv 1 \mod n$, und somit der Satz.

Aus p teilt $\Phi_n(n)$ und $\Phi_n(X)$ teilt $X^n - 1$ folgt p teilt $n^n - 1$.

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

Sei also t die Ordnung von n in $\mathbb{F}_p^\times$. Dann ist n durch t teilbar und wir behaupten, dass $t = n$.

Dies impliziert, dass $p-1$ durch n teilbar ist und beweist die Behauptung.

Falls also $1 \leq t < n$ so folgt:

$$\frac{x^n - 1}{x^t - 1} = \phi_n(x) \prod_d \phi_d(x)$$

wobei d alle echten Teiler von n durchläuft die t nicht teilen.

Folglich ist $\frac{n^n - 1}{n^t - 1}$ durch $\Phi_n(n)$ teilbar. Unter berücksichtigung, dass n teilbar ist durch t folgt:

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

$$\equiv \underbrace{1 + \cdots + 1}_{n/t} \mod p$$

Da $p \mid \Phi_n(n)$ und folglich $\frac{n^n - 1}{n^t - 1}$ teilt

folgt, dass n/t und somit n durch

p teilbar ist. Nun ist aber:

$$\Phi_n(X) = X^{\varphi(n)} + \cdots + 1 \quad (n \geq 2)$$

Also $\Phi_n(n) = n^{\varphi(n)} + \cdots + 1 \equiv 1 \mod p$

ein Widerspruch. $\boxed{\wr}$