5.2.2. $(*)$ ist injektiv.

Sei also $g^i(1+p)^j \equiv 1 \bmod p^\nu$, $\Rightarrow g^i \equiv 1 \bmod p$,

$\Rightarrow p-1 \mid i \Rightarrow i \bmod (p-1) = 0$. – Wegen $(**)$

damit auch $(1+p)^j \equiv 1 \bmod p^\nu \xrightarrow[\text{nach F4}]{\operatorname{ord}((1+p) \bmod p^\nu) = p^{\nu-2}} p^{\nu-2} \mid j$,

$\Rightarrow j \bmod p^{\nu-1} = 0$.

Die Zyklizität von $(\mathbb{Z}/p^\nu\mathbb{Z})^\times$ folgt jetzt aus

Bem. Das direkte Produkt $G_1 \times G_2 \times \dots \times G_r$ zyklischer Gruppen G_i mit paarw. teilerfremden Ordnungen m_i ist wieder zyklisch (von der Ordnung $m_1 m_2 \dots m_r$).

Bew. $G_i \simeq \mathbb{Z}/m_i$

$G_1 \times \dots \times G_r = \mathbb{Z}/m_1 \times \dots \times \mathbb{Z}/m_r \overset{\text{Chin. Restsatz}}{\simeq} \mathbb{Z}/m_1 m_2 \dots m_r$

F5: Seien $G_1, G_2, \dots, G_r$ endliche (abelsche) Gruppen der Ordnungen $m_1, m_2, \dots, m_r$. Wenn $G := G_1 \times \dots \times G_r$ zyklisch ist, so sind die $m_1, \dots, m_r$ paarw. teilerfremd (und die G_i sind zyklisch, vgl. F6 u.ä.)

Bew: $e(G) \mid kgV(m_1, m_2, \dots, m_r) \mid m_1 m_2 \dots m_r = \operatorname{ord}(G)$ $\otimes$

Ann. $m_1, m_2, \dots, m_r$ nicht paarw. teilerfremd. Damit ist die Teilbarkeit $\otimes$ echt (vgl. §1, F8), und es folgt

$e(G) < \operatorname{ord}(G)$, und damit G nicht zyklisch. W!

F6: Sei G eine zyklische Gruppe der Ordnung n. Dann ist jede Untergruppe H von G zyklisch mit $\mathrm{ord}(H) \mid n$. Die Abbildung

$$H \longmapsto \mathrm{ord}(H)$$

ist eine Bijektion zwischen der Menge aller Untergruppen H von G und der Menge aller natürlichen Teiler d von n, und zwar ist $H_d := \{x \in G \mid x^d = 1\}$ die Untergruppe der Ordnung d von G. Es ist

$$H_{\frac{n}{d}} = \{x \in G \mid x^{\frac{n}{d}} = 1\} \overset{!}{=} \{y^d \mid y \in G\}$$

die Untergruppe der d-ten Potenzen in G.

Bew.: 1) $G = \langle \alpha \rangle$. Sei k die kleinste nat. Zahl mit $\alpha^k \in H$.
Sei $\alpha^j \in H$; $j = qk + r$ mit $0 \le r < k$

$\alpha^r = \alpha^{j-qk} = \alpha^j (\alpha^{kq})^{-1} \in H$, $\Rightarrow r = 0$, also $k \mid j$.

$\Rightarrow \alpha^j - \alpha^{kq} \in \langle \alpha^k \rangle$, $\Rightarrow H = \langle \alpha^k \rangle$

Ferner: Da $\alpha^n = 1 \in H \Rightarrow k \mid n$

$d := \mathrm{ord}(H) = \mathrm{ord}(\alpha^k) = \frac{n}{(n,k)} = \frac{n}{k}$, also $d \mid n$

2) Sei $d \mid n$ $(n \in \mathbb{N})$. Betrachte $H = H_d := \{x \in G \mid x^d = 1\}$; ist Untergruppe von G. Nach 1):

$H = \langle \alpha^k \rangle$ mit $k \mid n$, $\mathrm{ord}(H) = \mathrm{ord}(\alpha^k) = \frac{n}{k}$

$\alpha^k \in H$, $\Rightarrow \alpha^{kd} = 1$, $\Rightarrow n \mid kd \Rightarrow \frac{n}{k} \mid d$

$\langle \alpha^{\frac{n}{d}} \rangle \subseteq H$, $\Rightarrow \mathrm{ord}(\alpha^{\frac{n}{d}}) \mid \mathrm{ord}(H)$, $\Rightarrow d \mid \frac{n}{k}$

$\mathrm{ord}(\alpha^{\frac{n}{d}}) = \frac{n}{n/d} = d$; $\mathrm{ord}(H) = \frac{n}{k}$

Also $\frac{n}{k} = d$, d.h. $\mathrm{ord}(H) = d$.

Somit $\quad d \mapsto H_d \mapsto \operatorname{ord}(H_d) = d$

Ist H eine bel. Untergruppe der Ordnung d, so gilt $x^d = 1$ für alle $x \in H$, also $H \subseteq H_d$. Wegen $\operatorname{ord}(H) = d = \operatorname{ord}(H_d)$ folgt $H = H_d$.

Somit $\quad H \mapsto d = \operatorname{ord}(H) \mapsto H_d = H$.

Also ist $d \mapsto H_d$ die Umkehrabb. zu $H \mapsto \operatorname{ord}(H)$.

3) $H' := \{ g^d \mid g \in G \} \overset{G = \langle \alpha \rangle}{=} \langle \alpha^d \rangle$, also

$\operatorname{ord}(H') = \operatorname{ord}(\alpha^d) = \frac{n}{d}$. Somit $H' = H_{\frac{n}{d}}$.

<u>Korollar:</u> Für bel. $n \in \mathbb{N}$ gilt

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

[Summe über alle natürlichen Teiler d von n]

<u>Bew.</u> Sei G eine zyklische Gruppe der Ordnung n (z.B. $G \simeq \mathbb{Z}/n\mathbb{Z}$).

$\psi(d) := \#\{ x \in G \mid \operatorname{ord}(x) = d \}$ [mit $d \mid n$, $d \in \mathbb{N}$]

Jedes $x \in G$ mit $\operatorname{ord}(x) = d$ liegt in $H_d = \{ x \in G \mid x^d = 1 \}$. Also

(*) $\quad \psi(d) = \#\{ x \in H_d \mid \operatorname{ord}(x) = d \} = \varphi(d)$

(zyklisch von der Ordnung d)

Für jedes <u>$x \in G$</u> ist $\operatorname{ord}(x)$ ein Teiler von n. Es folgt

$$n = \sum_{x \in G} 1 = \sum_{d \mid n} \psi(d) \overset{(*)}{=} \sum_{d \mid n} \varphi(d)$$

q.e.d.

FZ: Sei G eine beliebige endliche Gruppe der Ordnung n. Folgende Aussagen sind äquivalent:

$d \in \mathbb{N}$

(i) Für jedes $d \mid n$ gilt $\#\{x \in G \mid x^d = 1\} \leq d$.

(ii) Für jedes $d \mid n$ hat G höchstens eine Untergruppe der Ordnung d.

(iii) G ist zyklisch.

Bew. Gelte (iii). Dann ist $H_d := \{x \in G \mid x^d = 1\}$ eine Untergruppe von G mit $\#H_d = d$, vgl. F6. Also gilt (i).

Gelte (i). Seien H, H' Ugrn von G mit $\#H = \#H' = d$. Für alle $x \in H \cup H'$ gilt $x^d = 1$. Aus (i) folgt dann $\#(H \cup H') \leq d$, und es folgt $H = H'$.

Gelte (ii). Für jedes $d \mid n$ setze $\psi(d) = \psi_G(d) := \#\{x \in G \mid \operatorname{ord}(g) = d\}$. Für jedes $x \in G$ ist $\operatorname{ord}(x)$ ein Teiler von n. Es folgt

$$(1) \qquad \sum_{d \mid n} \psi(d) = n$$

Wir behaupten: Für jedes $d \mid n$ gilt

$$(2) \qquad \psi(d) \leq \varphi(d)$$

Im Falle $\psi(d) = 0$ ist (2) richtig. Sei also $\psi(d) \geq 1$, d.h. es gebe ein $g \in G$ mit $\operatorname{ord}(g) = d$. Dann ist $\langle g \rangle$ eine Untergruppe der Ordnung d. Da mindestens ein bel. Elt. in G mit $\operatorname{ord}(x) = d$, so ist auch $\langle x \rangle$ eine Ugr der Ordnung d. Nach (ii) ist aber $\langle x \rangle = \langle g \rangle$, also insb. $x \in \langle g \rangle$. Alle Elemente der Ordnung d sind somit bereits in der zyklischen Untergruppe $\langle g \rangle$ von G enthalten. Diese hat aber genau $\varphi(d)$ Elemente der Ordnung d, und es folgt $\psi(d) = \varphi(d)$, also insb. (2). – Summation von (2) über alle $d \mid n$ liefert

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

Folglich muß (2) stets mit $\psi(d) = \varphi(d)$ gelten! Insb. für $d = n$, und es folgt $\psi(n) \geq 1$. Also besitzt G ein Element der Ordnung n und ist somit zyklisch.

Da es in einem Körper K höchstens d Elemente mit $x^d = 1$ gibt, folgt aus FZ von neuem Satz 1' (S. 73) und damit der Satz 1 von S. 70).

Satz 4: Sei $m \in \mathbb{N}$, $m > 1$. Genau dann besitzt $(\mathbb{Z}/m\mathbb{Z})^\times$ eine Primitivwurzel, wenn m eine der Zahlen folgender Gestalt ist:

(*) $\qquad 2,\ 4,\ p^\nu,\ 2p^\nu$

mit einer Primzahl $p \neq 2$ (und $\nu \geq 1$)

Bew. 1) $(\mathbb{Z}/2)^\times = \langle \bar{1} \rangle = \{\bar{1}\}$, $(\mathbb{Z}/4)^\times = \langle -\bar{1} \rangle \simeq \mathbb{Z}/2$ sind zyklisch, desgleichen $(\mathbb{Z}/p^\nu)^\times$ nach Satz 2.

$(\mathbb{Z}/2p^\nu)^\times \overset{\text{Chin. Restsatz}}{\simeq} (\mathbb{Z}/2)^\times \times (\mathbb{Z}/p^\nu)^\times \simeq \{\bar{1}\} \times (\mathbb{Z}/p^\nu)^\times \simeq (\mathbb{Z}/p^\nu)^\times$ zyklisch.

2) Für bel. $m \in \mathbb{N}$, $m > 1$ sei $m = p_1^{\nu_1} \cdots p_r^{\nu_r}$ (mit $r > 0$, $\nu_i > 0$) die PFZ von m. Aus dem Chin. Restsatz folgt

$$(\mathbb{Z}/m)^\times \simeq (\mathbb{Z}/p_1^{\nu_1})^\times \times \cdots \times (\mathbb{Z}/p_r^{\nu_r})^\times$$

Sei $(\mathbb{Z}/m)^\times$ zyklisch. Dann nach F5: $\varphi(p_1^{\nu_1}), \ldots, \varphi(p_r^{\nu_r})$ paarw. teilerfremd und jedes $(\mathbb{Z}/p_i^{\nu_i})^\times$ zyklisch.

Sind p_i, p_j ungerade und $i \neq j$, so ist 2 gemeinsamer Teiler von $\varphi(p_i^{\nu_i}) = \underbrace{(p_i - 1)}_{\text{gerade}} p_i^{\nu_i - 2}$ und $\varphi(p_j^{\nu_j}) = \underbrace{(p_j - 1)}_{\text{gerade}} p_j^{\nu_j - 1}$

Es folgt:

Entweder $m = p_1^{\nu_1}$ oder $m = p_1^{\nu_1} p_2^{\nu_2}$ mit $p_1 = 2$.

1. Fall: $\nu_1 \neq 2$, fertig. $\nu_1 = 2$, so $\nu_1 \leq 2$ [denn sonst $(\mathbb{Z}/2^{\nu_1})^\times$ nicht zyklisch (nach Satz 3)]

2. Fall: Wäre $\nu_1 \geq 2$, so $2 \mid \varphi(2^{\nu_1})$, $2 \mid \varphi(p_2^{\nu_2})$ W!

also $m = 2p_2^{\nu_2}$.