§ 9. Primitivwurzeln

9.1. Satz. *Sei G eine zyklische Gruppe der Ordnung m und $g \in G$ ein erzeugendes Element. Das Element $a := g^k$, $k \in \mathbb{Z}$, ist genau dann ein erzeugendes Element von G, wenn k zu m teilerfremd ist, d.h.* $\gcd(k, m) = 1$.

Bemerkung. Es folgt, dass eine zyklische Gruppe der Ordnung m genau $\varphi(m)$ erzeugende Elemente besitzt.

Beweis. a) Sei zunächst vorausgesetzt, dass $\gcd(k, m) = 1$. Dann gibt es ganze Zahlen λ, μ mit $\lambda k + \mu m = 1$. Daraus folgt

$$g = g^{\lambda k + \mu m} = (g^k)^\lambda (g^m)^\mu = a^\lambda e^\mu = a^\lambda.$$

Dies bedeutet, dass g in der von a erzeugten Untergruppe $\langle a \rangle \subset G$ liegt. Dann liegen aber auch alle Potenzen von g in $\langle a \rangle$, d.h. $\langle a \rangle = G$.

b) Sei a erzeugendes Element von G. Dann lässt sich insbesondere g als Potenz von a schreiben, es gibt also $\lambda \in \mathbb{Z}$ mit

$$g = a^\lambda = g^{k\lambda} \quad \Longrightarrow \quad g^{k\lambda - 1} = e \quad \Longrightarrow \quad k\lambda - 1 \equiv 0 \bmod m.$$

Es gibt also eine ganze Zahl μ mit $k\lambda - 1 = \mu m$, d.h. $\lambda k + \mu m = 1$. Daraus folgt aber $\gcd(k, m) = 1$, q.e.d.

9.2. Definition. Sei m eine positive ganze Zahl. Eine zu m teilerfremde ganze Zahl g heißt *Primitivwurzel* modulo m, wenn die Restklasse von g in $(\mathbb{Z}/m)^*$ ein erzeugendes Element dieser Gruppe ist.

Wir u.a. werden zeigen:

a) Zu jeder Primzahl p gibt es eine Primitivwurzel modulo p.

b) Ist p eine ungerade Primzahl, so gibt es zu jeder Primzahlpotenz p^k, $(k \geqslant 1)$, eine Primitivwurzel modulo p^k.

Zunächst rechnen wir einige numerische Beispiele.

(1) $m = p = 7$.
Wir berechnen die Ordnungen aller Elemente von $(\mathbb{Z}/7)^* = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}\}$.

x	x^2	x^3	x^4	x^5	x^6	$\operatorname{ord}(x)$
1						1
2	4	1				3
3	2	6	4	5	1	6
4	2	1				3
5	4	6	2	3	1	6
6	1					2

Dabei entsteht z.B. die Zeile für $x = 5$ folgendermaßen:

$$x^2 \equiv 5 \cdot 5 \equiv 21 + 4 \equiv 4, \quad x^3 \equiv 4 \cdot 5 \equiv 14 + 6 \equiv 6,$$
$$x^4 \equiv 6 \cdot 5 \equiv 28 + 2 \equiv 2, \quad x^5 \equiv 2 \cdot 5 \equiv 7 + 3 \equiv 3,$$
$$x^6 \equiv 3 \cdot 5 \equiv 14 + 1 \equiv 1.$$

Aus der Tabelle entnimmt man, dass 3 und 5 Primitivwurzeln modulo 7 sind.
Man sieht auch, dass es zu jedem Teiler d der Gruppenordnung 6 ein Element gibt, das die Ordnung d hat.

(2) $m = 8 = 2^3$.

Hier ist $(\mathbb{Z}/8)^* = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}$.

x	x^2	ord(x)
1		1
3	1	2
5	1	2
7	1	2

Es gibt also keine Primitivwurzel modulo 8.
Bemerkenswert ist auch, dass im Ring $\mathbb{Z}/8$ das quadratische Polynom $X^2 - 1$ insgesamt 4 Nullstellen hat und zwar alle invertierbaren Elemente von $\mathbb{Z}/8$. (In einem Körper hat ein Polynom vom Grad n höchstens n Nullstellen.)

9.3. Satz. *Sei G eine endliche Untergruppe der multiplikativen Gruppe $K^* = K \setminus \{0\}$ eines Körpers K. Dann ist G zyklisch.*

Wendet man den Satz auf die multiplikative Gruppe $(\mathbb{Z}/p)^*$ des Körpers $\mathbb{F}_p = \mathbb{Z}/p$ an, erhält man:

Folgerung. *Zu jeder Primzahl p gibt es eine Primitivwurzel g modulo p.*

Nach Satz 9.1 gibt es dann insgesamt $\varphi(p-1)$ Primitivwurzeln modulo p.

Beweis. Es sei n die Ordnung der Gruppe G. Es ist zu zeigen, dass es in G ein Element der Ordnung n gibt. Wir benützen dazu die in Satz 7.6 bewiesene Gleichung

$$\sum_{d|n} \varphi(d) = n.$$

Sei $x \in G$ ein beliebiges Element. Die Ordnung $d := \text{ord}(x)$ ist jedenfalls ein Teiler von n. Die von x erzeugte Untergruppe $H := \langle x \rangle \subset G$ ist zyklisch von der Ordnung d. Jedes Element von H ist Nullstelle des Polynoms $X^d - 1$. Da dieses Polynom über dem Körper K höchstens d Nullstellen hat, hat $X^d - 1$ auch keine anderen Nullstellen als die Elemente von H. Daraus folgt, dass jedes Element $y \in G$ der Ordnung d bereits in der zyklischen Gruppe H enthalten ist. Nach Satz 9.1 gibt es somit $\varphi(d)$ Elemente

der Ordnung d in G. Für die Gesamtzahl m der Elemente aus G, deren Ordnung $< n$ ist, gilt deshalb

$$m \leqslant \sum_{\substack{d|n \\ d<n}} \varphi(d) = n - \varphi(n) < n.$$

Deshalb gibt es mindestens ein Element der Ordnung n, q.e.d.

9.4. Satz. *Ein Element a einer Gruppe G hat genau dann die Ordnung $r \in \mathbb{N}_1$, wenn folgende beiden Bedingungen erfüllt sind:*

(1) $a^r = e$,

(2) $a^{r/q} \neq e$ *für alle Primteiler $q \mid r$.*

Beweis. a) Beide Bedingungen sind offenbar notwendig.

b) Seien jetzt (1) und (2) vorausgesetzt und sei $s := \mathrm{ord}(a)$. Aus (1) folgt, dass $s \mid r$. Wäre $s \neq r$, gäbe es einen mindestens einen Primteiler $q \mid r$, so dass $s \mid (r/q)$. Daraus würde aber folgen, dass $a^{r/q} = e$, was im Widerspruch zu (2) steht. Also muss doch $s = r$ gelten, q.e.d.

9.5. Corollar. *Sei p eine Primzahl. Eine ganze Zahl $g \not\equiv 0 \bmod p$ ist genau dann eine Primitivwurzel modulo p, wenn*

$$g^{(p-1)/q} \not\equiv 1 \bmod p \quad \textit{für alle Primteiler } q \mid p-1.$$

Beweis. Dies folgt unmittelbar aus dem Satz 9.4 mit $r = p - 1$, da nach dem kleinen Satz von Fermat die Bedingung (1) automatisch erfüllt ist.

Bemerkung. Falls die Primfaktorzerlegung von $p-1$ bekannt ist, liefert das Corollar 9.5 ein effizientes Verfahren, um eine Primitivwurzel modulo p zu finden. Man testet der Reihe nach $g = 2, 3, \ldots$, ob das Kriterium des Corollars erfüllt ist (die Potenzen können mittels des schnellen Potenzierungs-Algorithmus berechnet werden). Da es insgesamt $\varphi(p-1) = (p-1)\prod_{q|(p-1)}(1-\frac{1}{q})$ Primitivwurzeln gibt, stößt man im allgemeinen schnell auf eine Primitivwurzel. Häufig ist bereits 2 eine Primitivwurzel. Nach einer noch unbewiesenen Vermutung von Artin ist 2 Primitivwurzel für unendlich viele Primzahlen p.

Übrigens kann man bem Testen die Quadratzahlen auslassen, denn eine Quadratzahl $a = b^2$ kann niemals Primitivwurzel einer Primzahl $p \geqslant 3$ sein, denn $a^{(p-1)/2} = b^{p-1} \equiv 1 \bmod p$, also ist die Ordnung von a mod p ein Teiler von $(p-1)/2$.

9.6. Satz. *Sei p eine ungerade Primzahl.*

a) *Eine ganze Zahl g ist genau dann Primitivwurzel modulo p^2, wenn folgende beiden Bedingungen erfüllt sind:*

(1) *g ist Primitivwurzel modulo p*

(2) $\quad g^{p-1} \not\equiv 1 \bmod p^2$.

b) *Ist g Primitivwurzel modulo p, aber nicht Primitivwurzel modulo p^2, so ist $\tilde{g} := g+p$ Primitivwurzel modulo p^2.*

Beweis. a) Natürlich sind die beiden Bedingungen notwendig. Sei umgekehrt vorausgesetzt, dass (1) und (2) gilt und sei x eine beliebige nicht durch p teilbare ganze Zahl. Wir müssen zeigen, dass eine natürliche Zahl n existiert mit $x \equiv g^n \bmod p^2$. Wegen (1) gibt es ein k mit

$$x \equiv g^k \bmod p.$$

Modulo p^2 ist dann

$$x \equiv (g^k + \alpha p) \bmod p^2$$

mit einer gewissen ganzen Zahl α. Da g^k modulo p invertierbar ist, gibt es eine ganze Zahl β mit $g^k\beta \equiv \alpha \bmod p$. Damit gilt dann

$$x \equiv g^k\,(1 + \beta p) \bmod p^2 \qquad (*)$$

Nach Voraussetzung (2) ist

$$g^{p-1} \equiv 1 + \gamma p \bmod p^2 \quad \text{mit } \gamma \not\equiv 0 \bmod p,$$

Daraus folgt mit dem binomischen Lehrsatz für alle $\ell \geqslant 1$

$$g^{(p-1)\ell} \equiv (1 + \gamma p)^\ell \equiv 1 + \ell\gamma p \bmod p^2.$$

Da γ invertierbar modulo p, kann man ℓ so wählen, dass $\ell\gamma \equiv \beta \bmod p$. Dann ist

$$g^{(p-1)\ell} \equiv (1 + \beta p) \bmod p^2.$$

Setzt man dies in $(*)$ ein, erhält man

$$x \equiv g^k g^{(p-1)\ell} \equiv g^{k+(p-1)\ell} \bmod p^2, \quad \text{q.e.d.}$$

b) Ist g Primitivwurzel modulo p, aber nicht modulo p^2, so ist nach Teil a)

$$g^{p-1} \equiv 1 \bmod p^2.$$

Für $\tilde{g} = g + p$ folgt dann wieder mit dem binomischen Lehrsatz

$$\tilde{g}^{p-1} \equiv (g+p)^{p-1} \equiv g^{p-1} + (p-1)pg^{p-2} \equiv 1 - pg^{p-2} \not\equiv 1 \bmod p^2.$$

Also ist nach a) $\tilde{g}$ eine Primitivwurzel modulo p^2, q.e.d.

Beispiel. Die Zahl 2 ist Primitivwurzel modulo 3, da $(\mathbb{Z}/3)^* = \{\overline{1}, \overline{2}\}$. Wegen

$$2^2 \equiv 4 \not\equiv 1 \bmod 9$$

ist 2 auch Primitivwurzel modulo 9.

9.7. Satz. *Sei p eine ungerade Primzahl und g eine Primitivwurzel modulo p^2. Dann ist g auch Primitivwurzel modulo allen Potenzen p^k, $k \geqslant 2$.*

Bemerkung. Zusammen mit Satz 9.6 ergibt sich daraus, das für alle Primzahlpotenzen p^k, $p \geqslant 3$, Primitivwurzeln existieren.

Beweis. ...

Wir wenden uns jetzt den Potenzen der Primzahl 2 zu. Trivialerweise sind

$$(\mathbb{Z}/2)^* = \{\overline{1}\} \quad \text{und} \quad (\mathbb{Z}/4)^* = \{\overline{1}, \overline{3}\}$$

zyklisch. Dies gilt nicht mehr für höhere Potenzen, wie wir schon für $(\mathbb{Z}/8)^*$ gesehen haben.

9.8. Satz. *Die Gruppe $(\mathbb{Z}/2^k)^*$ ist für $k \geqslant 3$ nicht zyklisch. Die Elemente der Form*

$$x \equiv 1 \bmod 4$$

bilden eine zyklische Untergruppe der Ordnung 2^{k-2}, die von der Restklasse $5 \bmod 2^k$ erzeugt wird. Man hat einen Gruppen-Isomorphismus

$$\begin{aligned} (\mathbb{Z}/2, +) \times (\mathbb{Z}/2^{k-2}, +) &\longrightarrow (\mathbb{Z}/2^k)^*, \\ (\mu \bmod 2 \ , \ \nu \bmod 2^{k-2}) &\mapsto (-1)^\mu 5^\nu \bmod 2^k. \end{aligned}$$

Beweis. ...