JOURNAL OF NUMBER THEORY 4, 70–77 (1972)

Einseinheitengruppen und prime Restklassengruppen in quadratischen Zahlkörpern

FRANZ HALTER-KOCH

Mathematical Institute, University of Cologne, Weyertal 86, 5 Cologne, Germany

Communicated by P. Roquette

Received March 20, 1970

In this note we calculate explicitly bases of the group of einseinheiten in local quadratic number fields and apply the result for the description of the structure of the prime residue class groups modulo prime divisor powers in an arbitrary quadratic number field.

Bei der Untersuchung der klassenkörpertheoretischen Struktur und der Zerlegungsgesetze von Diederkörpern bin ich auf folgendes Problem gestoßen, für das ich in der Literatur keine explizite Lösung finden konnte.

Gegeben sei ein quadratischer Zahlkörper $K = \mathbf{Q}(\sqrt{d})$ (d quadratfrei in $\mathbf{Z}$) und ein Primdivisor $\mathfrak{p}$ von K; $K_\mathfrak{p}$ sei die vollständige Hülle zu $\mathfrak{p}$.

Gesucht sind: 1. Eine Basis der Einseinheitengruppe $H_\mathfrak{p}$ von $K_\mathfrak{p}$.

2. Die Ordnungen der Basiselemente von $H_\mathfrak{p}$ mod $\mathfrak{p}^s$ für $s \geqslant 1$.

3. Basiselemente und ihre Ordnungen für die Gruppe $P(\mathfrak{p}^s)$ der primen Restklassen mod $\mathfrak{p}^s$ in K.

Grundsätzlich sind diese Probleme durch Hensel [2, 3, 4] gelöst, jedoch macht die bis ins letzte explizite Beschreibung doch einige Schwierigkeiten. Im hier behandelten Falle quadratischer Zahlkörper werden damit weitere Daten für die rechnerische Beherrschung dieser Körper geliefert. Der Fall $K_\mathfrak{p} = \mathbf{Q}_p$ ist trivial und wird im folgenden weggelassen. Grundlegend für das Folgende ist die Hensel'sche Theorie, wie sie in Hasse [1, §15], dargestellt ist. Die Bezeichnungen sind wie dort gewählt (mit Ausnahme der Standardbezeichnungen $\mathbf{Q}$ and $\mathbf{Z}$); insbesondere sei p die Charakteristik von $\mathfrak{R}$, dem Restklassenkörper mod $\mathfrak{p}$, $\mathbf{Q}_p$ der Körper der p-adischen Zahlen und $\mathbf{Z}_p$ der Ring der ganzen p-adischen Zahlen.

Die Gruppe $P(\mathfrak{p}^s)$ ist das direkte Produkt einer zyklischen Gruppe $\langle w_s \rangle$, erzeugt von einer mod $\mathfrak{p}^s$ geeignet normierten Primitivwurzel w_s mod $\mathfrak{p}$, mit der Gruppe $H(\mathfrak{p}^s)$ der Einseinheiten mod $\mathfrak{p}^s$. Ist $\{\eta_1, \ldots, \eta_r\}$

eine $\mathbf{Z}_p$-Basis von $H_\mathfrak{p}$, so ist $\{\eta_1, ..., \eta_r\}$ zwar ein Erzeugendensystem, jedoch im allgemeinen keine Basis von $H(\mathfrak{p}^s)$. Man gewinnt daraus aber eine Basis unter Benutzung des folgenden Sachverhalts:

Ist G eine endliche abelsche Gruppe der Ordnung $|G| = N$, und ist $\{\eta_1, ..., \eta_r\}$ ein Erzeugendensystem von G, so ist $\{\eta_1, ..., \eta_r\}$ genau dann eine Basis von G, wenn für die Ordnungen $v(\eta_i)$ von η_i in G gilt:

$$N = \prod_{i=1}^{r} v(\eta_i).$$

1. $p = 2$

Fall 1: $d \equiv 5 \bmod 8$

$K_\mathfrak{p} = \mathbf{Q}_2(\sqrt{d}) = \mathbf{Q}_2(\sqrt{-3})$; $2 \simeq \mathfrak{p}$, $\mathfrak{e} = 1$, $\mathfrak{f} = 2$, $\mathfrak{n} = 2$. $\mathfrak{R}$ wird über $\mathbf{F}_2$ (dem Restklassenkörper von $\mathbf{Q}_2$) erzeugt durch die Wurzeln des Polynoms $X^2 + X + 1$ und hat die Elemente $\bar{0}, \bar{1}, \bar{\rho}, \bar{\rho}^2$. Als Vertreter für $\bar{\rho}$ in $K_\mathfrak{p}$ kann $\rho = (-1 + \sqrt{d})/2$ gewählt werden; $\{\bar{1}, \bar{\rho}\}$ ist eine Basis für $\mathfrak{R}/\mathbf{F}_2$. $\pi = 2$, $-2 = \pi \cdot (-1)$, also ist $\epsilon = -1$; $\mu = \bar{\mu} = 1$, $\mathfrak{e}_0 = 1$. Die Lösungsgruppe $\mathfrak{X}_0$ von $\bar{\xi}^2 + \bar{\xi} = \bar{0}$ in $\mathfrak{R}$ besteht aus $\bar{0}$ und $\bar{1}$; also ist $\bar{1}$ ein Basiselement für $\mathfrak{X}_0$, $\bar{\rho}$ ein Basiselement für $\mathfrak{R}^+/\mathfrak{X}_0$.

$\mathfrak{R}^{+2} - \bar{\epsilon}\mathfrak{R}^+ = \mathfrak{R}^{+2} + \mathfrak{R}^+ = \{\bar{0}, \bar{1}\}$; also ist $\bar{\rho}$ auch Basiselemente für $\mathfrak{R}^+/(\mathfrak{R}^{+2} - \bar{\epsilon}\mathfrak{R}^+)$.

Eine Basis von $H_\mathfrak{p}$ ist nun gegeben durch

$$\eta_{11} = -1, \qquad \eta_{21} = 1 + \omega_2\pi, \qquad \eta_* = 1 + \omega_0\pi^2.$$

Dabei sind ω_2 und ω_0 beliebige Vertreter von Basiselementen für $\mathfrak{R}^+/\mathfrak{X}_0$ und $\mathfrak{R}^+/(\mathfrak{R}^{+2} - \bar{\epsilon}\mathfrak{R}^+)$; daher kann

$$\omega_2 = \omega_0 = \frac{-1 + \sqrt{d}}{2}$$

gewählt werden. Man erhält als Basiselemente für $H_\mathfrak{p}$:

$$\eta_{11} = -1, \qquad \eta_{21} = \sqrt{d}, \qquad \eta_* = -1 + 2\sqrt{d}.$$

Die Ordnungen $v_s(\eta)$ der Basiselemente η mod $\mathfrak{p}^s$ berechnen sich wie folgt:

$$v_s(\eta_{11}) = \begin{cases} 1 & \text{falls } s = 1, \\ 2^1, & \text{falls } s \geqslant 2, \end{cases}$$

$$v_s(\eta_{21}) = 2^{s-1},$$

$$v_s(\eta_*) = 2^{s-2}.$$

Dabei soll $2^n = 1$ für $n \leqslant 0$ gesetzt sein. Wegen

$$v_s(\eta_{11}) \cdot v_s(\eta_{21}) \cdot v_s(\eta_*) = 2^{2s-2} = |H(\mathfrak{p}^s)|$$

ist $\{\eta_{11}, \eta_{21}, \eta_*\}$ eine Basis von $H(\mathfrak{p}^s)$. Eine Basis von $P(\mathfrak{p}^s)$ erhält man durch Hinzunahme einer auf $w_s^3 \equiv 1 \bmod \mathfrak{p}^s$ normierten Primitivwurzel $w_s \bmod \mathfrak{p}$. Eine solche ist z.B.

$$w_s = \omega_0^{2^{s-2}} \qquad \text{mit} \quad \omega_0 = \frac{-1 + \sqrt{d}}{2}.$$

Die primen Restklassen mod $\mathfrak{p}^s$ aus $\mathbf{Q}$ werden in $P(\mathfrak{p}^s)$ erzeugt von η_{11}, η_{21}^2.

Fall 2: $d \not\equiv 1 \bmod 4$

$K_\mathfrak{p} = \mathbf{Q}_2(\sqrt{d})$; $2 \simeq \mathfrak{p}^2$, $\mathfrak{e} = 2$, $\mathfrak{f} = 1$, $\mathfrak{n} = 2$. $\mathfrak{R} = \mathbf{F}_2$; als Vertreter von Basiselementen können beliebige $\omega \in K_\mathfrak{p}$ mit $\omega \not\equiv 0 \bmod \mathfrak{p}$ gewählt werden. $\pi \in K_\mathfrak{p}$ sei ein Primelement für $\mathfrak{p}$, $-2 = \epsilon \cdot \pi^2$. Im Falle $d \equiv -1 \bmod 8$ ist $\mu = \bar{\mu} = 2$, sonst $\mu = 1$, $\bar{\mu} = 2$; in jedem Falle ist $\mathfrak{e}_0 = 1$.

Ein Erzeugendensystem von $H_\mathfrak{p}$ ist dann gegeben durch

$$\eta_{11} = 1 + \omega_1\pi, \qquad \eta_{13} = 1 + \omega_2\pi^3, \qquad \eta_* = 1 + \omega_3\pi^4.$$

Dabei sind die ω_i beliebige Einheiten aus $K_\mathfrak{p}$. Dieses Erzeugendensystem ist genau dann eine Basis, wenn $\mu = \bar{\mu} = 2$, also $d \equiv -1 \bmod 8$, ist und η_{11} geeignet normiert wird. Andernfalls ist $-\eta_{11}^2$ durch η_{13} und η_* ausdrückbar.

Fall a: $d \equiv -1 \bmod 8$. Es ist $K_\mathfrak{p} = \mathbf{Q}_2(\sqrt{d}) = \mathbf{Q}_2(\sqrt{-1})$, $\pi = 1 - \sqrt{d}$, $\epsilon = -[(1 + d)/2 - \sqrt{d}]^{-1}$. Setzt man $\eta_{11} = \sqrt{-1} \in K_\mathfrak{p}$, so ist $\{\eta_{11}, \eta_{13}, \eta_*\}$ eine Basis von $H_\mathfrak{p}$. Mit $\omega_2 = \epsilon$ und $\omega_3 = \epsilon^2$ erhält man folgende Basiselemente:

$$\eta_{11} = \sqrt{-1}, \qquad \eta_{13} = -1 + 2\sqrt{d}, \qquad \eta_* = 1 + 2^2 = 5.$$

Die Ordnungen mod $\mathfrak{p}^s$ berechnen sich wie folgt:

$$v_s(\eta_{11}) = \begin{cases} 1, & \text{falls } s = 1, \\ 2^1, & \text{falls } s = 2, \\ 2^2, & \text{falls } s \geqslant 3; \end{cases}$$

$$v_s(\eta_{13}) = \begin{cases} 2^{s_0-1}, & \text{falls } s = 2s_0, \\ 2^{s_0-1}, & \text{falls } s = 2s_0 + 1; \end{cases}$$

$$v_s(\eta_*) = \begin{cases} 2^{s_0-2}, & \text{falls } s = 2s_0, \\ 2^{s_0-1}, & \text{falls } s = 2s_0 + 1. \end{cases}$$

Wegen

$$v_s(\eta_{11}) \cdot v_s(\eta_{13}) \cdot v_s(\eta_*) = 2^{s-1} = |H(\mathfrak{p}^s)|$$

ist $\{\eta_{11}, \eta_{13}, \eta_*\}$ eine Basis von $H(\mathfrak{p}^s)$, also auch von $P(\mathfrak{p}^s) = H(\mathfrak{p}^s)$. Eine in K liegende Basis von $P(\mathfrak{p}^s)$ erhält man, wenn man η_{11} durch eine primitive 4. Einheitswurzel ζ_s mod $\mathfrak{p}^s$ ersetzt. Dei primen Restklassen mod $\mathfrak{p}^s$ aus $\mathbf{Q}$ werden in $P(\mathfrak{p}^s)$ erzeugt von η_{11}^2 und η_*.

Fall b: $d \equiv 3 \bmod 8$. Es ist $K_\mathfrak{p} = \mathbf{Q}_2(\sqrt{d}) = \mathbf{Q}_2(\sqrt{-5})$, $\pi = 1 - \sqrt{d}$, $\epsilon = -[(1+d)/2 - \sqrt{d}]^{-1}$. Mit $\omega_1 = -1$, $\omega_2 = \epsilon$ und $\omega_3 = \epsilon^2$ erhält man folgendes Erzeugendensystem:

$$\eta_{11} = \sqrt{d}, \qquad \eta_{13} = -1 + 2\sqrt{d}, \qquad \eta_* = 1 + 2^2 = 5.$$

Wegen $-\eta_{11}^2 \equiv \eta_* \bmod \mathfrak{p}^6$ und $\eta_* \not\equiv 1 \bmod \mathfrak{p}^6$ hat η_* in der Darstellung von $-\eta_{11}^2$ durch η_{13} und η_* nicht durch 2 teilbaren Exponenten $\alpha \in \mathbf{Z}_2$, kann also durch $\zeta = -1$ ersetzt werden. Eine Basis von $H_\mathfrak{p}$ ist demnach gegeben durch

$$\zeta = -1, \qquad \eta_{11} = \sqrt{d}, \qquad \eta_{13} = -1 + 2\sqrt{d}.$$

Die Ordnungen mod $\mathfrak{p}^s$ berechnen sich wie folgt:

$$v_s(\zeta) = \begin{cases} 1 & \text{falls } s \leqslant 2, \\ 2^1, & \text{falls } s \geqslant 3, \end{cases}$$

$$v_s(\eta_{11}) = \begin{cases} 1, & \text{falls } s = 1, \\ 2^1, & \text{falls } s = 2, \\ 2^2, & \text{falls } s = 3, 4, \\ 2^{s_0-1}, & \text{falls } s = 2s_0 \geqslant 6, \\ 2^{s_0}, & \text{falls } s = 2s_0 + 1 \geqslant 5; \end{cases}$$

$$v_s(\eta_{13}) = \begin{cases} 2^{s_0-1}, & \text{falls } s = 2s_0, \\ 2^{s_0-1}, & \text{falls } s = 2s_0 + 1. \end{cases}$$

Für $s \geqslant 5$ ist

$$v_s(\zeta) \cdot v_s(\eta_{11}) \cdot v_s(\eta_{13}) = 2^{s-1} = |H(\mathfrak{p}^s)|.$$

Also ist für $s \geqslant 5$ $\{\zeta, \eta_{11}, \eta_{13}\}$ eine Basis für $H(\mathfrak{p}^s) = P(\mathfrak{p}^s)$. Wegen $\eta_{11}^2 \equiv -1 \bmod \mathfrak{p}^4$ fällt für $s \leqslant 4$ das Basiselement ζ weg, und man erhält $\{\eta_{11}, \eta_{13}\}$ als Basis. Die primen Restklassen mod $\mathfrak{p}^s$ aus $\mathbf{Q}$ werden in $P(\mathfrak{p}^s)$ erzeugt durch ζ und η_{11}^2.

Fall c: $d \equiv 2 \bmod 4$. Es ist $K_\mathfrak{p} = \mathbf{Q}_2(\sqrt{d})$, $\pi = \sqrt{d}$, $\epsilon = -2/d$. Mit $\omega_1 = 1$, $\omega_2 = -\epsilon$ und $\omega_3 = \epsilon^2$ erhält man folgendes Erzeugendensystem:

$$\eta_{11} = 1 + \sqrt{d}, \qquad \eta_{13} = 1 + 2\sqrt{d}, \qquad \eta_* = 1 + 2^2 = 5.$$

Wegen $-\eta_{11}^2 \equiv \eta_{13} \bmod \mathfrak{p}_2^4$ und $\eta_{13} \not\equiv 1 \bmod \mathfrak{p}^4$ hat η_{13} in der Darstellung von $-\eta_{11}^2$ durch η_{13} und η_* nicht durch 2 teilbaren Exponenten $\alpha \in \mathbf{Z}_2$, kann also durch $\zeta = -1$ ersetzt werden. Eine Basis von $H_\mathfrak{p}$ ist demnach gegeben durch

$$\zeta = -1, \qquad \eta_{11} = 1 + \sqrt{d}, \qquad \eta_* = 5.$$

Die Ordnungen mod $\mathfrak{p}^s$ berechnen sich wie folgt:

$$v_s(\zeta) = \begin{cases} 1, & \text{falls } s \leqslant 2, \\ 2^1, & \text{falls } s \geqslant 3; \end{cases}$$

$$v_s(\eta_{11}) = \begin{cases} 1, & \text{falls } s = 1, \\ 2^1, & \text{falls } s = 2, \\ 2^2, & \text{falls } s = 3, \\ 2^{s_0}, & \text{falls } s = 2s_0 \geqslant 4, \\ 2^{s_0}, & \text{falls } s = 2s_0 + 1 \geqslant 5; \end{cases}$$

$$v_s(\eta_*) = \begin{cases} 2^{s_0-2}, & \text{falls } s = 2s_0, \\ 2^{s_0-1}, & \text{falls } s = 2s_0 + 1. \end{cases}$$

Für $s \geqslant 4$ ist

$$v_s(\zeta) \cdot v_s(\eta_{11}) \cdot v_s(\eta_*) = 2^{s-1} = |H(\mathfrak{p}^s)|.$$

Also ist für $s \geqslant 4$ $\{\zeta, \eta_{11}, \eta_*\}$ eine Basis von $H(\mathfrak{p}^s) = P(\mathfrak{p}^s)$. Wegen $\eta_{11}^2 \equiv -1 \bmod \mathfrak{p}^3$ fällt für $s \leqslant 3$ das Basiselement ζ weg, und man erhält

Übersicht über die primen Restklassengruppen mod $\mathfrak{p}^s$
für $\mathfrak{p} \mid 2$ und $s \geqslant 2$

Fall		Basiselemente	Typ	Bed.
1	$d \equiv 5 \bmod 8$	w_s, -1, $\sqrt{d}$, $-1+2\sqrt{d}$	$(3, 2^1, 2^{s-1}, 2^{s-2})$	
2*a*	$d \equiv -1 \bmod 8$		$(2^1, 1, 1)$	$s=2$
		ζ_s, 5, $-1+2\sqrt{d}$	$(2^2, 2^{s_0-2}, 2^{s_0-1})$	$s=2s_0 \geqslant 4$
			$(2^2, 2^{s_0-1}, 2^{s_0-1})$	$s=2s_0+1 \geqslant 3$
2*b*	$d \equiv 3 \bmod 8$	$\sqrt{d}$, $-1+2\sqrt{d}$	$(2^{s-1}, 1)$	$s \leqslant 3$
			$(2^2, 2^1)$	$s=4$
		-1, $\sqrt{d}$, $-1+2\sqrt{d}$	$(2^1, s^{s_0-1}, 2^{s_0-1})$	$s=2s_0 \geqslant 6$
			$(2^1, 2^{s_0}, 2^{s_0-1})$	$s=2s_0+1 \geqslant 5$
2*c*	$d \equiv 2 \bmod 4$	$1+\sqrt{d}$	(2^{s-1})	$s \leqslant 3$
		-1, 5, $1+\sqrt{d}$	$(2^1, 2^{s_0-2}, 2^{s_0})$	$s=2s_0 \geqslant 4$
			$(2^1, 2^{s_0-1}, 2^{s_0})$	$s=2s_0+1 \geqslant 5$

$\{\eta_{11}\}$ als Basis ($\eta_* \equiv 1 \bmod \mathfrak{p}^4$!). Die primen Restklassen mod $\mathfrak{p}^s$ aus $\mathbf{Q}$ werden in $P(\mathfrak{p}^s)$ von ζ und η_* erzeugt.

2. $p \neq 2$

Fall 1: $(d/p) = -1$

$K_\mathfrak{p} = \mathbf{Q}_p(\sqrt{d})$; $p \simeq \mathfrak{p}$; $\mathfrak{e} = 1$, $\mathfrak{f} = 2$, $\mathfrak{n} = 2$. $\mathfrak{R} = \mathbf{F}_p(\sqrt{\bar{d}})$ ($\bar{d} = d + p\mathbf{Z}_p$, $\mathbf{F}_p = \mathbf{Z}_p/p\mathbf{Z}_p$); $\{1, \sqrt{\bar{d}}\}$ ist eine Basis für $\mathfrak{R}/\mathbf{F}_p$, $\{1, \sqrt{\bar{d}}\}$ ein Vertretersystem dieser Basis in $K_\mathfrak{p}$, also $\omega_1 = 1$, $\omega_2 = \sqrt{d}$; $\pi = p$, $\mu = 0$.

Eine Basis von $H_\mathfrak{p}$ ist gegeben durch

$$\eta_{11} = 1 + \omega_1\pi, \qquad \eta_{21} = 1 + \omega_2,$$

also

$$\eta_{11} = 1 + p, \qquad \eta_{21} = 1 + p\sqrt{d}.$$

Dir Ordnungen $v_s(\eta)$ der Basiselemente η mod $\mathfrak{p}^s$ berechnen sich zu

$$v_s(\eta_{11}) = v_s(\eta_{21}) = p^{s-1}.$$

Wegen $v_s(\eta_{11}) \cdot v_s(\eta_{21}) = p^{2s-2} = |H(\mathfrak{p}^s)|$ ist $\{\eta_{11}, \eta_{21}\}$ eine Basis von $H(\mathfrak{p}^s)$. Eine Basis von $P(\mathfrak{p}^s)$ erhält man durch Hinzunahme einer auf $w_s^{p^2-1} \equiv 1 \bmod \mathfrak{p}^s$ normierten Primitivwurzel w_s mod $\mathfrak{p}$; eine solche ist z.B. $w_s = w_1^{p^{2s-2}}$, wobei w_1 eine Primitivwurzel mod $\mathfrak{p}$ ist. Die primen Restklassen mod $\mathfrak{p}^s$ aus $\mathbf{Q}$ werden in $P(\mathfrak{p}^s)$ von η_{11} und einer geeignet normierten Primitivwurzel mod p erzeugt.

Fall 2: $p \mid d$

$K_\mathfrak{p} = \mathbf{Q}_p(\sqrt{d})$; $p \simeq \mathfrak{p}^2$; $\mathfrak{e} = 2$, $\mathfrak{f} = 1$, $\mathfrak{n} = 2$. $\mathfrak{R} = \mathbf{F}_p$; als Vertreter von Basiselementen können beliebige $\omega_i \in K_\mathfrak{p}$ mit $\omega_i \not\equiv 0 \bmod \mathfrak{p}$ gewählt werden. $\pi = \sqrt{d}$; $-p = \epsilon \cdot \pi^2$ mit $\epsilon = -p/d$. Im Falle $p = 3$ und $d/3 \equiv -1 \bmod 3$ ist $\mu = \bar{\mu} = 1$ und $\mathfrak{e}_0 = 1$, sonst ist stets $\mu = 0$.

Fall a: $p = 3$, $d/3 \equiv -1 \bmod 3$. Es ist $K_\mathfrak{p} = \mathbf{Q}_3(\sqrt{d}) = \mathbf{Q}_3(\sqrt{-3})$. $K_\mathfrak{p}$ enthält die primitive 3. Einheitswurzel $\zeta = (-1 + \sqrt{-3})/2$. Eine Basis von $H_\mathfrak{p}$ ist gegeben durch

$$\eta_{11} = \zeta, \qquad \eta_{12} = 1 + \omega_1\pi^2, \qquad \eta_* = 1 + \omega_2\pi^3.$$

Mit $\omega_1 = \omega_2 = -\epsilon$ erhält man

$$\eta_{11} = \zeta, \qquad \eta_{12} = 1 + 3 = 4, \qquad \eta_* = 1 + 3\sqrt{d}.$$

Die Ordnungen mop $\mathfrak{p}^s$ sind gegeben durch

$$v_s(\eta_{11}) = \begin{cases} 1, & \text{falls } s = 1, \\ 3^1, & \text{falls } s \geqslant 2; \end{cases}$$

$$v_s(\eta_{12}) = \begin{cases} 3^{s_0-1}, & \text{falls } s = 2s_0, \\ 3^{s_0}, & \text{falls } s = 2s_0 + 1; \end{cases}$$

$$v_s(\eta_*) = \begin{cases} 3^{s_0-1}, & \text{falls } s = 2s_0, \\ 3^{s_0-1}, & \text{falls } s = 2s_0 + 1. \end{cases}$$

Wegen

$$v_s(\eta_{11}) \cdot v_s(\eta_{12}) \cdot v_s(\eta_*) = 3^{s-1} = |H(\mathfrak{p}^s)|$$

ist $\{\eta_{11}, \eta_{13}, \eta_*\}$ eine Basis von $H(\mathfrak{p}^s)$. Eine in K liegende Basis von $H(\mathfrak{p}^s)$ erhält man, wenn man η_{11} durch eine primitive 3. Einheitswurzel ζ_s mod $\mathfrak{p}^s$ ersetzt. Eine Basis von $P(\mathfrak{p}^s)$ erhält man durch Hinzunahme der 2. Einheitswurzel -1. Die primen Restklassen mod $\mathfrak{p}^s$ aus $\mathbf{Q}$ werden in $P(\mathfrak{p}^s)$ von η_{12} und -1 erzeugt.

Fall b: $p \neq 3$ *oder* $d/3 \equiv 1 \bmod 3$. $K_\mathfrak{p} = \mathbf{Q}_p(\sqrt{d})$ enthält die p-ten Einheitswurzeln nicht. Eine Basis von $H_\mathfrak{p}$ ist gegeben durch

$$\eta_{11} = 1 + \omega_1\pi, \qquad \eta_{12} = 1 + \omega_2\pi^2.$$

Mit $\omega_1 = 1$ und $\omega_2 = -\epsilon$ erhält man

$$\eta_{11} = 1 + \sqrt{d}, \qquad \eta_{12} = 1 + p.$$

Die Ordnungen der Basiselemente mod $\mathfrak{p}^s$ berechnen sich wie folgt:

$$v_s(\eta_{11}) = \begin{cases} p^{s_0}, & \text{falls } s = 2s_0, \\ p^{s_0}, & \text{falls } s = 2s_0 + 1; \end{cases}$$

$$v_s(\eta_{12}) = \begin{cases} p^{s_0-1}, & \text{falls } s = 2s_0, \\ p^{s_0}, & \text{falls } s = 2s_0 + 1. \end{cases}$$

Wegen $v_s(\eta_{11}) \cdot v_s(\eta_{12}) = p^{s-1} = |H(\mathfrak{p}^s)|$ ist $\{\eta_{11}, \eta_{12}\}$ eine Basis von $H(\mathfrak{p}^s)$. Eine Basis von $P(\mathfrak{p}^s)$ erhält man durch Hinzunahme einer auf $w_s^{p-1} \equiv 1 \bmod \mathfrak{p}^s$ normierten Primitivwurzel w_s mod $\mathfrak{p}$; dabei kann w_s als geeignet normierte Primitivwurzel mod p aus $\mathbf{Z}$ gewählt werden. Die primen Restklassen mod $\mathfrak{p}^s$ aus $\mathbf{Q}$ werden in $P(\mathfrak{p}^s)$ von η_{12} und w_s erzeugt.

Übersicht über die primen Restklassengruppen mod $\mathfrak{p}^s$
für $\mathfrak{p}+2$ und $s \geqslant 1$

Fall		Basiselemente	Typ	Bed.
1	$\left(\frac{d}{p}\right)=-1$	$w_s, 1+p, 1+p\sqrt{d}$	$(p^2-1, p^{s-1}, p^{s-1})$	
2a	$p \mid d, p=3$		$(2, 1, 1, 1)$	$s=1$
		$-1, \zeta_s, 4, 1+3\sqrt{d}$	$(2, 3^1, 3^{s_0-1}, 3^{s_0-1})$	$s=2s_0$
	$\frac{d}{3} \equiv -1 \bmod 3$		$(2, 3^1, 3^{s_0}, 3^{s_0-1})$	$s=2s_0+1$
2b	$p \mid d, p \neq 3$ oder	$w_s, 1+p, 1+\sqrt{d}$	$(p-1, p^{s_0-1}, p^{s_0})$	$s=2s_0$
	$\frac{d}{3} \equiv 1 \bmod 3$		$(p-1, p^{s_0}, p^{s_0})$	$s=2s_0+1$

LITERATUR

1. H. HASSE, "Zahlentheorie," 2. Aufl, Akademie-Verlag, Berlin, 1963.
2. K. HENSEL, Die multiplikative Darstellung der algebraischen Zahlen für den Bereich eines beliebigen Primteilers, *J. Reine Angew. Math.* **146** (1916), 156–160.
3. K. HENSEL, Untersuchung der Zahlen eines algebraischen Körpers für eine beliebige Primteilerpotenz als Modul. *J. Reine Angew. Math.* **146** (1916), 216–228.
4. K. HENSEL, Allgemeine Theorie der Kongruenzklassengruppen und ihrer Invarianten in algebraischen Körpern. *J. Reine Angew. Math.* **147** (1917), 1–15.