§3 Kreisteilungskörper

Bez. $K = \mathbb{Q}$, $L = \mathbb{Q}(\zeta)$, ζ primit. n-te Einheitswurzel.

$[L:\mathbb{Q}] = \varphi(n)$.

1. Ziel: Zeige $\mathcal{O}_L = \mathbb{Z}[\zeta]$.

Lemma 1: Sei $\ell \in \mathbb{P}$ und $n = \ell^\nu$, $\nu \in \mathbb{N}$. Sei $\lambda = 1-\zeta \in \mathcal{O}_L$.

i) Das Hauptideal $(\lambda) \subset \mathcal{O}_L$ ist PI über ℓ mit Trägheitsgrad 1 und

$$\ell\mathcal{O}_L = (\lambda)^d, \quad d = \varphi(\ell^\nu) = [L:\mathbb{Q}].$$

ii) Die Basis $1, \zeta, \ldots, \zeta^{d-1}$ von $L/\mathbb{Q}$ hat Diskr.

$$d(1,\zeta,\ldots,\zeta^{d-1}) = \pm \ell^s, \quad s = \ell^{\nu-1}(\nu\ell-\nu-1).$$

Bew: i) Das Minpol von ζ über $\mathbb{Q}$ ist das n-te Kreisteilungspol

$$\Phi_n(X) = \frac{X^{\ell^\nu}-1}{X^{\ell^{\nu-1}}-1} = X^{\ell^{\nu-1}(\ell-1)} + \ldots + X^{\ell^{\nu-1}} + 1.$$

Setze $X = 1$ $\Rightarrow$

$$(*) \quad \ell = \prod_{\substack{\alpha \in L \\ \text{primit.} \\ n\text{-te EW}}} (1-\alpha) = \prod_{g \in (\mathbb{Z}/n\mathbb{Z})^*} (1-\zeta^g)$$

Es ist

$$1-\zeta^g = \frac{1-\zeta^g}{1-\zeta}\cdot(1-\zeta)$$

mit $\varepsilon_g := \frac{1-\zeta^g}{1-\zeta} = \zeta^{g-1} + \ldots + \zeta + 1 \in \mathcal{O}_L$

Ist $g' \in \mathbb{N}$ mit $gg' \equiv 1 \ (m)$, so gilt

$$\varepsilon_g := \frac{1-\zeta}{1-\zeta^g} = \frac{1-\zeta^{gg'}}{1-\zeta^g} = \zeta^{g(g'-1)} + \ldots + \zeta^g + 1 \in \mathcal{O}_L$$

$\Rightarrow \varepsilon_g \in \mathcal{O}_L^*$.

$$\overset{(*)}{\Rightarrow} \quad \ell = \varepsilon(1-\zeta)^{\varphi(m)} \quad \text{mit } \varepsilon = \prod_g \varepsilon_g \in \mathcal{O}_L^*$$

$$\Rightarrow \quad \ell\mathcal{O}_L = (\lambda)^{\varphi(m)}$$

Mit $[L:K] = e f r$, $e = [L:K]$, $r = 1$ folgt f = Trägheitsgrad $= 1$.

ii) Seien $\zeta = \zeta_1, \zeta_2, \ldots, \zeta_d$ die Konj. von ζ.

Dann ist $\phi_L(X) = \prod_{i=1}^{d} (X - \zeta_i)$

$$\overset{\text{Kap. zu Disk.}}{\Rightarrow} \quad d(1, \zeta, \ldots, \zeta^{d-1}) = \prod_{i \neq j} (\zeta_i - \zeta_j)$$

$$= \prod_{i=1}^{d} \phi_L'(\zeta_i)$$

$$= N_{L/\mathbb{Q}}(\phi_L'(\zeta)).$$

Leite

$$(X^{\ell^{\nu-1}} - 1)\phi_L(X) = X^{\ell^\nu} - 1 \quad \text{ab}$$

$$\Rightarrow \quad \ell^{\nu-1} X^{\ell^{\nu-1}-1} \phi_L(X) + (X^{\ell^{\nu-1}} - 1)\phi_L'(X) = \ell^\nu X^{\ell^\nu - 1}$$

$$\overset{X=\zeta}{\Rightarrow} \quad (\zeta^{\ell^{\nu-1}} - 1)\phi_L'(\zeta) = \ell^\nu \zeta^{\ell^\nu - 1} = \ell^\nu \zeta^{-1}$$

Hier ist $\alpha = \zeta^{\ell^{\nu-1}}$ eine prim. ℓ-te EW.

$$\Rightarrow N_{L/\mathbb{Q}}(\alpha-1) = (N_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\alpha-1))^{\zeta-\dots-1}$$

$$\overset{(i)}{=} \pm \zeta^{\zeta-\dots-1}$$

$$N_{L/\mathbb{Q}}(\zeta) = \pm 1 \qquad d(1,\zeta,\dots,\zeta^{\varphi-1}) = \pm N_{L/\mathbb{Q}}(\Phi_L'(\zeta))$$

$$= \pm \frac{N_{L/\mathbb{Q}}(\zeta^{\dots}-\zeta^{\dots-1})}{N_{L/\mathbb{Q}}(\alpha-1)}$$

$$= \pm \zeta^{-\dots\alpha} \cdot \zeta^{-\zeta^{\dots-1}}$$

$$= \pm \zeta^{-\dots\zeta^{\dots-1}-\dots\zeta^{\dots-1}-\zeta^{\dots-1}}$$

$$= \pm \zeta^{s}$$

□

Satz 2:
Als $\mathbb{Z}$-Modul ist der Ring $\mathcal{O}_L$ für $L=\mathbb{Q}(\zeta)$ speziell durch

$$\mathcal{O}_L = \mathbb{Z} + \mathbb{Z}\zeta + \dots + \mathbb{Z}\zeta^{\alpha} = \mathbb{Z}[\zeta],$$

wobei $\alpha = \varphi(n)$.

Bew: Wir beweisen die Aussage hier nur für den Fall $n = \ell^{\nu}$ mit $\ell \in \mathbb{P}\setminus\{2\}$. Der allg. Fall kann daraus zusammengesetzt werden. (Übung)

Nach Lemma 1 ist

$$d(1,\zeta,\dots,\zeta^{\alpha-1}) = \pm \ell^{s}, \quad s = \ell^{\nu-1}(\nu\ell-\nu-1)$$

Kap II, §4, Lemma 4

$$\ell^{s}\mathcal{O}_L \subset \mathbb{Z}[\zeta] \subset \mathcal{O}_L \qquad (*)$$

Sei $\lambda = 1-\zeta$. Lemma 1 $\Rightarrow$ $(\lambda) \subset O_L$ PI u.
$O_L/\lambda O_L \cong \mathbb{Z}/\ell\mathbb{Z}$

Insbes. ist $\mathbb{Z} \to O_L/\lambda O_L$ surj.

$\Rightarrow O_L = \mathbb{Z} + \lambda O_L$

$\Rightarrow \lambda O_L + \mathbb{Z}[\zeta] = O_L$

$\Rightarrow \lambda^2 O_L + \underbrace{\lambda \mathbb{Z}[\zeta]}_{\subset \mathbb{Z}[\zeta]} = \lambda O_L$

$\Big\} \Rightarrow \lambda^2 O_L + \mathbb{Z}[\zeta] = O_L$

induktiv $\Rightarrow \lambda^t O_L + \mathbb{Z}[\zeta] = O_L \quad \forall\, t \in \mathbb{N}$.

Für $t = s\cdot\varphi(n)$: $\lambda^t O_L = (\lambda^{\varphi(n)})^s O_L \overset{\text{Lem. 1(i)}}{=} \ell^s O_L \overset{(*)}{\subset} \mathbb{Z}[\zeta]$

$\Rightarrow \mathbb{Z}[\zeta] = O_L$ $\square$

Satz 3: Sei $n = \prod p^{\nu_p}$ die Primfaktorzerlegung von n. Für jede PZ p sei

$$f_p = \min\{f \in \mathbb{N};\ p^f \equiv 1 \ (n/p^{\nu_p})\}.$$

Dann hat p in $\mathbb{Q}(\zeta)$ die PI-Zerl.

$$p = (\mathfrak{p}_1 \cdots \mathfrak{p}_r)^{\varphi(p^{\nu_p})},$$

mit versch. PI $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ mit Trägheitsgrad f_p.

Bsp. 4, $n=4$, $L = \mathbb{Q}(i)$

Es gilt dabei $r\cdot\varphi(p^{\nu_p})\cdot f_p = \varphi(n)$.

Bew: • Satz 2 $\Rightarrow O_L = \mathbb{Z}[\zeta]$.
$\Rightarrow \mathbb{Z}[\zeta]$ hat Führer (1).
$\Rightarrow$ Können §1, Satz 4 benutzen $\forall$ PZ p.

$\Rightarrow$ p zerlegt in $\mathbb{Q}_\ell$ in r_1 wie das Polynom $\Phi_m(X) \in \mathbb{Z}[X]$ bei Red. mod p in r wird zerlegt, d.h.

$$\mathbb{F}_p[X] \Rightarrow \Phi_m(X) = (\bar{P}_1(X) \cdots \bar{P}_r(X))^e \quad (*)$$

$\Rightarrow$ Zz: $e = \varphi(p^{r_1})$ und

$$\bar{P}_1(X), \ldots, \bar{P}_r(X) \in \mathbb{F}_p[X]$$

sind paarw. verschieden vom Grad f_p.

- Schreibe $m = p^{r_1} \cdot n$.
Dann ist $(n, p) = 1$.
Wenn ξ_i durch die ganzen i-ten EW läuft und η_j " " " p^{r_1}-ten " ", so läuft $\xi_i \cdot \eta_j$ durch die ganzen m-ten EW.

$$\Rightarrow \Phi_m(X) = \prod_{i,j} (X - \xi_i \eta_j)$$

- $X^{p^{r_1}} - 1 \equiv (X-1)^{p^{r_1}} \pmod{p}$

$$\Rightarrow 0 \equiv (\eta_j - 1)^{p^{r_1}} \pmod{\mathfrak{p}} \qquad \forall\, \mathfrak{p} \mid p,\ \mathfrak{p} \subset \mathbb{Q}_\ell$$

$$\Rightarrow \eta_j \equiv 1 \pmod{\mathfrak{p}}.$$

$$\Rightarrow \Phi_m(X) \equiv \prod (X - \xi_i)^{\varphi(p^{r_1})} = \Phi_n(X)^{\varphi(p^{r_1})} \pmod{\mathfrak{p}}$$

$$\Rightarrow \Phi_m(X) - \Phi_n(X)^{\varphi(p^{r_1})} \in \mathbb{Z}[X] \cap \mathfrak{p} \cdot \mathbb{Z}[X] = p \cdot \mathbb{Z}[X]$$

$\Rightarrow \Phi_n(X) \equiv \Phi_m(X)^{\varphi(p^{\nu})} \pmod{p}$.

$\Rightarrow$ Genügt Zerlegung (*) zu zeigen
wenn $p \nmid n$ (und damit $m = n$, $p^{\nu} = 1$)

Also ZZ: Für $p \nmid n$ ist

$$\mathbb{F}_p[X] \ni \bar{\Phi}_n(X) = \bar{p}_1(X) \cdots \bar{p}_r(X)$$

mit paarw. versch. irred. Pol. $\bar{p}_i(X) \in \mathbb{F}_p[X]$ vom Grad $f_p = \min\{f \in \mathbb{N} ; p^f \equiv 1 \ (n)\}$.

$\mathrm{char}(\mathcal{O}_L/\mathfrak{p}) = p \nmid n$

$\Rightarrow X^n - 1$ und nX^{n-1} haben keine gemeinsamen Nullst. in $\mathcal{O}_L/\mathfrak{p}$.

$\Rightarrow X^n - 1$ hat keine mehrfach Nullst. in $\mathcal{O}_L/\mathfrak{p}$

$\Rightarrow$ Kan. Hom $\mathcal{O}_L \longrightarrow \mathcal{O}_L/\mathfrak{p}$
induziert Bijektion

$$\mu_n = \{n\text{-te EW in } \mathcal{O}_L\} \xrightarrow{\sim} \{n\text{-te EW in } \mathcal{O}_L/\mathfrak{p}\}$$

$$\Rightarrow \{\text{prim. } n\text{-te EW in } \mathcal{O}_L\} \xrightarrow{\sim} \{\text{prim. .. in } \mathcal{O}_L/\mathfrak{p}\}$$

$$\zeta \longmapsto \bar{\zeta} = \zeta \bmod \mathfrak{p}$$

$\mathbb{F}_{p^f} = \mathcal{O}_L/\mathfrak{p} = \mathbb{F}_p[\bar{\zeta}]$

ist prim. n-te EW
und $\mathcal{O}_L/\mathfrak{p} = \mathbb{F}_p[\bar{\zeta}]$

$p^{f_p} \equiv 1 \ (n)$

$\bar{\zeta}^n = 1$ [illegible]

$\Rightarrow \bar{\zeta}^{p^{f}} = \bar{\zeta}$ [illegible] $\bar{\zeta} \notin \mathbb{F}_{p^{f'}}$ [illegible] $= \min(f ; p^f \equiv 1) = n$

Die kleinste Erweiterung von $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, die ξ enthält ist $\mathbb{F}_{p^{f_p}}$, denn

$\mathbb{F}_{p^{f_p}}^*$ ist zyklisch von Ordnung $p^{f_p}-1$.

$\Rightarrow$ $\mathbb{F}_{p^{f_p}}$ ist Zerf.-Kp. von $\bar{\Phi}_n(X) \in \mathbb{F}_p[X]$.

$\bar{\Phi}_n(X) \mid X^n - 1$ in $\mathbb{F}_p[X]$.

$\Rightarrow$ $\bar{\Phi}_n(X)$ hat keine mehrf. Nullst.

Ist $\bar{\Phi}_n(X) = \bar{p}_1(X) \cdot \ldots \cdot \bar{p}_r(X)$ Faktorisierung in irred. Pol., so ist jedes $\bar{p}_i(X)$ das Mipo. einer primitiven n-ten EW $\xi \in \mathbb{F}_{p^{f_p}}^*$.

$\Rightarrow$ $\deg \bar{p}_i(X) = [\mathbb{F}_{p^{f_p}} : \mathbb{F}_p] = f_p$. □

<u>Kor 4</u>: Eine ungerade PZ p ist verzweigt in $L = \mathbb{Q}(\xi)$ $\Leftrightarrow$ $p \mid n$.

Die PZ 2 ist verzweigt in L $\Leftrightarrow$ $4 \mid n$.

Eine ungerade PZ p zerfällt vollst. in L $\Leftrightarrow$ $p \equiv 1 \ (n)$.

Erläuterung zu $\mathbb{F}_p[\xi] \cong \mathbb{F}_{p^{f}}$ (Zu p. 31)

Für $t \in \mathbb{N}$ ist $\mathbb{F}_{p^t} / \mathbb{F}_p$ eine endl. Galois-Erw. vom Grad t mit Gal-Gruppe $G \cong \mathbb{Z}/t\mathbb{Z}$.

Die Gruppe G wird erzeugt von ~~der Einschr. auf $\mathbb{F}_{p^t}$~~ des Frob. $\sigma: \overline{\mathbb{F}}_p \to \overline{\mathbb{F}}_p$, $x \mapsto x^p$

und als Teilkp. von $\overline{\mathbb{F}}_p$ ist

$\mathbb{F}_{p^t} = \{ x \in \overline{\mathbb{F}}_p ; \ x^{p^t} = x \}$

$=$ Fix-Körper von σ^t.

Folgerung:

Ist $\alpha \in \mathbb{F}_{p^t}$ primit. El., d.h. $\mathbb{F}_{p^t} = \mathbb{F}_p[\alpha]$, so gilt

$t = \min \{ s \in \mathbb{N} ; \ \alpha^{p^s} = \alpha \}$

Folgerung:

Speziell für $\mathcal{O}/\mathfrak{p} = \mathbb{F}_p[\bar{\xi}]$, $\bar{\xi} = \xi + \mathfrak{p}$ primit. n-te EW gilt

$f_p := [\mathbb{F}_p[\bar{\xi}] : \mathbb{F}_p]$

$= \min \{ s \in \mathbb{N} ; \ \bar{\xi}^{p^s} = \bar{\xi} \}$

$= \min \{ s \in \mathbb{N} ; \ \bar{\xi}^{p^s - 1} = 1 \}$

$\bar{\xi}$ primit. n-te EW

$= \min \{ s \in \mathbb{N} ; \ n \mid p^s - 1 \}$

$= \min \{ s \in \mathbb{N} ; \ p^s \equiv 1 \ (\mathrm{mod}\ n) \}$.

Lemma 5: Sei ℓ, p ungerade $\neq 2$, $\ell^* = (-1)^{\frac{\ell-1}{2}}\ell$ und ζ primitive ℓ-te EW. Es gilt

p vollst. zerl. in $\mathbb{Q}(\sqrt{\ell^*}) \Leftrightarrow p$ zerl. in $\mathbb{Q}(\zeta)$ in eine gerade Anz. von $\mathfrak{P}$.

Bew: Sei $\tau = \sum_{a \in (\mathbb{Z}/\ell\mathbb{Z})^\times} \left(\frac{a}{\ell}\right) \zeta^a \in \mathbb{Q}(\zeta)$ Gauß-Summe

1) Es gilt $\tau^2 = \ell^*$. $\Rightarrow \mathbb{Q}(\sqrt{\ell^*}) \subset \mathbb{Q}(\zeta)$

Denn

$$\tau^2 = \sum_{a,b \in (\mathbb{Z}/\ell\mathbb{Z})^\times} \left(\frac{a}{\ell}\right)\left(\frac{b}{\ell}\right)$$

Legendre-Symbol

Sei p ungerade $\neq 2$ und $a \in \mathbb{Z}$.

Def:

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & p \mid a \\ 1, & p \nmid a \text{ und } a \equiv x^2 \ (p) \text{ hat Lsg } x \in \mathbb{Z}/p\mathbb{Z} \\ -1, & p \nmid a \text{ und } a \equiv x^2 \ (p) \text{ hat keine Lsg } x \in \mathbb{Z}/p\mathbb{Z} \end{cases}$$

Bem 5: Es gelte

i) $\left(\frac{a+p}{p}\right) = \left(\frac{a}{p}\right)$

ii) $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$

iii) $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \quad (p)$

iv) $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$

Bew: Übung

Bsp:

a	0	1	2	3	4	5	6
$\left(\frac{a}{3}\right)$	0	1	-1	0	1	-1	0

a	0	1	2	3	4	5	6
$\left(\frac{a}{5}\right)$	0	1	-1	-1	1	0	1

Lemma 6:
Sei $a \in \mathbb{Z}$ quadratfrei, $a \neq 0, 1$.
Für jede $p \geq 2$ mit $(p, 2a) = 1$ gilt

$\left(\frac{a}{p}\right) = 1 \iff p$ zerlegt in $\mathbb{Q}(\sqrt{a})$

Bew: Sei $L = \mathbb{Q}(\sqrt{a})$.
$\mathcal{O}_L = \mathbb{Z}[\sqrt{a}] \subset \mathcal{O}_L$ Ordnung mit Führer $f \mid (2)$.

$\Rightarrow p$ zerlegt in $\mathbb{Q}(\sqrt{a})$
$\iff X^2 - a \equiv (X-c)(X+c) \in \mathbb{F}_p[X]$
mit $c \in \mathbb{F}_p$.
$\iff a \equiv c^2 \quad (p)$ mit $c \in \mathbb{F}_p$
$\iff \left(\frac{a}{p}\right) = 1$. $\square$

Lemma 7: Seien l, p ungerade PZ, $l^* = (-1)^{\frac{l-1}{2}} l$, und ζ primit. l-te EW. Es gilt

p vollst. zerl. in $\mathbb{Q}(\sqrt{l^*}) \Leftrightarrow p$ zerl. in $\mathbb{Q}(\zeta)$ in eine gerade Anz. von PI.

Bew: Betr. die Gauß-Summe

$$\tau = \sum_{a \in (\mathbb{Z}/l\mathbb{Z})^*} \left(\frac{a}{l}\right) \zeta^a \in \mathbb{Q}(\zeta).$$

1) Es gilt $\tau^2 = l^* \Rightarrow \mathbb{Q}(\sqrt{l^*}) \subset \mathbb{Q}(\zeta)$.

Denn: $\tau^2 = \sum_{a,b \in (\mathbb{Z}/l\mathbb{Z})^*} \left(\frac{a}{l}\right)\left(\frac{b}{l}\right) \zeta^a \zeta^b$

$$= \sum_{a,b} \left(\frac{ab}{l}\right) \zeta^{a+b}$$

$$= \left(\frac{-1}{l}\right) \sum_{a,b} \left(\frac{ab^{-1}}{l}\right) \zeta^{a-b}$$

$$\overset{a \to cb}{=} \left(\frac{-1}{l}\right) \sum_{c,b} \left(\frac{c}{l}\right) \zeta^{bc-b}$$

$$= \left(\frac{-1}{l}\right) \sum_{c} \left(\frac{c}{l}\right) \underbrace{\sum_{b \in (\mathbb{Z}/l\mathbb{Z})^*} \zeta^{b(c-1)}}_{= \begin{cases} l-1, & c \equiv 1 \ (l) \\ -1, & c \not\equiv 1 \ (l) \end{cases}}$$

$$= \left(\frac{-1}{l}\right) \cdot (l-1) - \left(\frac{-1}{l}\right) \underbrace{\sum_{c \neq 1} \left(\frac{c}{l}\right)}_{-1}$$

$$= \left(\frac{-1}{l}\right) \cdot l = l^*.$$

2.) „⇒": Sei $(p) = p_1 p_2$ in $\mathbb{Q}(\sqrt{\ell^*})$ vollst. zerl.

Sei $\sigma \in Gal(\mathbb{Q}(\zeta)/\mathbb{Q})^{=:G}$ mit $\sigma|_{\mathbb{Q}(\sqrt{\ell^*})}$ = Konjugation.

Dann bildet σ

{PI in $\mathbb{Q}(\zeta)$ über p_1} bijektiv

ab auf

{PI in $\mathbb{Q}(\zeta)$ über p_2}.

⇒ # {PI in $\mathbb{Q}(\zeta)$ über p} ist gerade

3.) „⇐". Sei # {PI in $\mathbb{Q}(\zeta)$ über p} gerade.

Sei $G_{\mathfrak{p}} \subset G$ Zerlegungsgruppe von $\mathfrak{p}$ PI über p

$\Rightarrow [G : G_{\mathfrak{p}}] = [Z_{\mathfrak{p}} : \mathbb{Q}]$ ist gerade

Andererseits hat $H = Gal(\mathbb{Q}(\zeta)/\mathbb{Q}(\sqrt{\ell^*})) \subset G$,

indem $[G:H] = 2$.

$G \cong \mathbb{Z}/(\ell-1)\mathbb{Z}$ zyklisch

$$\Rightarrow \quad G_{\mathfrak{p}} \subset H \subset G.$$

$$\Rightarrow \quad \mathbb{Q} \subset \mathbb{Q}(\sqrt{\ell^*}) \subset Z_{\mathfrak{p}}$$

Trägheitsgrad von $\mathfrak{p} \cap Z_{\mathfrak{p}}$ über $\mathbb{Q}$ ist 1 (§2 Satz 5)

⇒ " " $\mathfrak{p} \cap \mathbb{Q}(\sqrt{\ell^*})$ " " "

Das gleiche gilt für die Verzweigungsindizes.

⇒ p total zerlegt in $\mathbb{Q}(\sqrt{\ell^*})$. □

<u>Satz 8</u> (Quadratisches Reziprozitätsgesetz)

Seien ℓ, p verschiedene ungerade PZ.
Es gilt
$$\left(\frac{\ell}{p}\right)\left(\frac{p}{\ell}\right) = (-1)^{\frac{\ell-1}{2}\cdot\frac{p-1}{2}}$$

Bem: Genügt zz: $\left(\frac{\ell}{p}\right) = \left(\frac{p}{\ell}\right)$.

Denn: $\left(\frac{\ell}{p}\right) = \left(\frac{-1}{p}\right)^{\frac{\ell-1}{2}}\left(\frac{\ell}{p}\right) \overset{\text{Bem 5(iv)}}{=} (-1)^{\frac{p-1}{2}\cdot\frac{\ell-1}{2}}\left(\frac{\ell}{p}\right)$.

Es gilt $\left(\frac{\ell}{p}\right) = 1 \overset{\text{Lemma 6}}{\iff}$ p zerlegt sich in $\mathbb{Q}(\sqrt{\ell^*})$
$\overset{\text{Lemma 7}}{\iff}$ p zerlegt in $\mathbb{Q}(\zeta)$ in eine gerade Anzahl von PF ($\zeta = \zeta_\ell$ prim. ℓ-te EW)

Satz 2 $\Rightarrow$ $r = \frac{\varphi(\ell)}{f} = \frac{\ell-1}{f}$, wobei

f = Ordnung von p in $(\mathbb{Z}/\ell\mathbb{Z})^\times$.

$\Rightarrow \left(\frac{\ell}{p}\right) = 1 \iff f \mid \frac{\ell-1}{2}$

$\iff p^{\frac{\ell-1}{2}} \equiv 1 \pmod{\ell}$

$\overset{\text{Bem 5(iii)}}{\iff} \left(\frac{p}{\ell}\right) \equiv 1 \pmod{\ell}$

$\overset{2<\ell}{\iff} \left(\frac{p}{\ell}\right) = 1$

$\Rightarrow \left(\frac{\ell^*}{p}\right) = 1 \iff \left(\frac{p}{\ell}\right) = 1$ ⊣

Satz 9 (Ergänzungssatz 2)
Sei p ungerade PZ. Es gilt
$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

Bem: Übung.