

### Teil III. Kreisteilungskörper.

Sei  $n \in \mathbb{N}_1$ . Mit  $\omega = \omega_n$  bezeichnen wir eine primitive  $n$ -te Einheitswurzel in  $\mathbb{C}$ , zum Beispiel  $\omega = \exp(2\pi i/n)$ . Es ist

$$X^n - 1 = \prod_{1 \leq s \leq n} (X - \omega^s).$$

Induktiv definieren wir das  $n$ -te Kreisteilungspolynom  $\Phi_n(X)$  durch die Gleichung

$$\prod_{d|n} \Phi_d(X) = X^n - 1,$$

also

$$\Phi_n(X) = \prod_{1 \leq s \leq n, (s,n)=1} (X - \omega^s).$$

Beachte:  $\Phi_n$  ist normiertes Polynom vom Grad  $\phi(n)$ .

**Satz.** Das Polynom  $\Phi_n$  ist irreduzibel.

Üblicher Beweis, siehe Algebra-Vorlesung. Wir werden weiter unten aber ebenfalls einen Beweis liefern.

#### 8.1. Der Kreisteilungskörper zu einer Primzahlpotenz $n = p^t$ .

**Lemma 1.** Sei  $p$  Primzahl und  $K = \mathbb{Q}[\omega_{p^t}]$ . Es gibt  $\epsilon \in U(\mathcal{O}_K)$  mit

$$(1 - \omega)^{\phi(p^t)} = \epsilon \cdot p.$$

Beweis: Sei  $n = p^t$ . Als erstes notieren wir:

$$\Phi_n(X) = (X^{p^t} - 1)/(X^{p^{t-1}} - 1) = X^{p^{t-1}(p-1)} + \dots + X^{p^{t-1}} + 1.$$

Rechts stehen  $p$  Summanden, also ist  $\Phi_n(1) = p$ .

Für jedes  $a \in \mathbb{N}_1$  gilt

$$1 - \omega^a = (1 - \omega)(1 + \omega + \dots + \omega^{a-1}),$$

also ist  $(1 - \omega^a)(1 - \omega)^{-1} \in \mathcal{O}_K$ . Ist nun  $(a, n) = 1$ , so gibt es  $b \in \mathbb{N}$  mit  $ab \equiv 1 \pmod{n}$  (Bézout'sche Gleichung), also ist  $(\omega^a)^b = \omega$  und wir sehen entsprechend:  $(1 - \omega)(1 - \omega^a) \in \mathcal{O}_K$ ; setzen wir also  $\epsilon_a = (1 - \omega^a)(1 - \omega)^{-1}$ , so ist dies eine Einheit in  $\mathcal{O}_K$  mit  $1 - \omega^a = \epsilon_a(1 - \omega)$ .

Wir erhalten alle primitiven  $n$ -ten Einheitswurzeln, wenn wir  $\omega^a$  mit  $1 \leq a \leq n$ ,  $(a, n) = 1$  bilden. Wir setzen 1 in  $\Phi_n = \prod_{1 \leq a \leq n, (a,n)=1} (X - \omega^a)$  ein:

$$p = \Phi_n(1) = \prod_{1 \leq a \leq n, (a,n)=1} (1 - \omega^a) = (1 - \omega)^{\phi(n)} \prod \epsilon_a.$$

Damit ist das Lemma gezeigt.

Diese einfache Rechnung liefert ganz wichtige Folgerungen:

**Folgerungen.**

- (1)  $\langle 1 - \omega \rangle$  ist ein maximales Ideal mit Norm  $p$ .
- (2) Das Ideal  $\langle p \rangle$  in  $\mathcal{O}_K$  ist total verzweigt.
- (3) Das Kreisteilungspolynom  $\Phi_{p^t}$  ist irreduzibel.

Beweis: Schreibe in  $\mathcal{O}_K$  das von  $1 - \omega$  erzeugte Hauptideal als Produkt von Primidealen, etwa

$$\langle 1 - \omega \rangle = P_1^{m_1} \cdots P_r^{m_r}.$$

Das Lemma zeigt:

$$\langle p \rangle = \langle 1 - \omega \rangle^{\phi(n)} = (P_1^{m_1} \cdots P_r^{m_r})^{\phi(n)}.$$

Bezeichnen wir mit  $e_i$  den Trägheitsindex von  $P_i$ , so besagt die Fundamentalgleichung

$$\sum e_i m_i \phi(n) = [\mathbb{Q}[\omega] : \mathbb{Q}].$$

Wir erhalten die folgende Ungleichungskette

$$\phi(n) \leq \phi(n) \left( \sum e_i m_i \right) = \sum e_i m_i \phi(n) = [\mathbb{Q}[\omega] : \mathbb{Q}] \leq \phi(n),$$

dabei gilt die rechte Ungleichung, weil das Minimalpolynom von  $\omega$  über  $\mathbb{Q}$  ein Teiler von  $\Phi_n$  sein muss, und  $\Phi_n$  den Grad  $\phi(n)$  hat. Es folgt, dass in unserer Ungleichungskette links wie rechts die Kleiner-gleich-Zeichen durch Gleichheitszeichen ersetzt werden können.

Das rechte Gleichheitszeichen  $[\mathbb{Q}[\omega] : \mathbb{Q}] = \phi(n)$  zeigt, dass  $\Phi_n$  das Minimalpolynom von  $\omega$ , und demnach irreduzibel ist (dies ist die Behauptung (3)).

Das linke Gleichheitszeichen besagt  $\sum e_i m_i = 1$ , also gilt  $r = 1$ ,  $e_1 = 1$ ,  $m_1 = 1$ . Wegen  $r = 1$  und  $m_1 = 1$  ist  $\langle 1 - \omega \rangle$  ein maximales Ideal, wegen  $e_1 = 1$  hat es Norm  $p$ . Dies ist die Behauptung (1). Wegen  $t = 1$  und  $e_1 = 1$  erhalten wir auch die Behauptung (2).

**Folgerung (4).** Der Betrag der Diskriminante  $\Delta(1, \omega, \dots, \omega^{\phi(n)-1})$  ist eine Potenz von  $p$ .

Beweis: Seien  $\omega_1, \dots, \omega_{\phi(n)}$  die primitiven  $n$ -ten Einheitswurzeln. Dann ist

$$\Delta := \Delta(1, \omega, \dots, \omega^{\phi(n)-1}) = \prod_{i < j} (\omega_i - \omega_j)^2$$

und jeder dieser Faktoren ist in  $\mathcal{O}_K$  ein Teiler von  $p$ , denn

$$\omega_i - \omega_j = \omega_i (1 - \omega_i^{-1} \omega_j)$$

und  $\omega' = \omega_i^{-1} \omega_j \neq 1$  ist eine  $n$ -te Einheitswurzel. Lemma 1 zeigt, dass  $1 - \omega'$  in  $\mathcal{O}_{\mathbb{Q}[\omega']}$ , und damit auch in  $\mathcal{O}_K$  ein Teiler von  $p$  ist.

Insgesamt sehen wir: Es gibt eine natürliche Zahl  $a$  mit  $\Delta \mid p^a$  in  $\mathcal{O}_K$ , also schon in  $\mathbb{Z}$ . (Zur Erinnerung: Ist  $R \subseteq S$  eine ganze Ring-Erweiterung und ist  $R$  ein normaler Bereich [also ganz abgeschlossen in seinem Quotientenkörper], so gilt: sind  $r_1, r_2$  von Null verschiedene Elemente und ist  $r_1$  ein Teiler von  $r_2$  in  $S$ , so auch in  $R$ . Denn ist  $s \in S$  mit  $r_1 s = r_2$ , so ist  $s$  ganz über  $R$  [alle Elemente von  $S$  sind ganz über  $R$ ], und  $s = r_2/r_1$  gehört zum Quotientenkörper von  $R$ . Die Normalität von  $R$  zeigt:  $s \in R$ .) Alle Teiler in  $\mathbb{Z}$  von  $p^a$  sind aber Zahlen, deren Betrag eine Potenz von  $p$  sind.

**Hinweis:** Mit etwas Geduld kann man  $\Delta(1, \omega, \dots, \omega^{\phi(n)-1})$  explizit berechnen.

**Satz.** Sei  $p$  Primzahl, sei  $\omega = \omega_{p^t}$  und  $K = \mathbb{Q}[\omega]$ . Es ist  $\mathcal{O}_K = \mathbb{Z}[\omega]$  und der Betrag von  $\Delta_K$  ist eine  $p$ -Potenz.

Beweis: Sei  $\Delta_K = p^a$  für ein  $a \in \mathbb{N}_0$ . Dann gilt (siehe Aufgabe 7.2):

$$\langle p^a \rangle = p^a \mathcal{O}_K \subseteq \mathbb{Z}[\omega].$$

Sei  $\beta = 1 - \omega$ . Wegen  $|\mathcal{O}_K / \langle \beta \rangle| = p$  sieht man:

$$(*) \quad \mathcal{O}_K = \mathbb{Z} + \langle \beta \rangle,$$

(denn ist  $\alpha \in \mathcal{O}_K$ , so gibt es  $z \in \mathbb{Z}$  mit  $\bar{\alpha} = \bar{z}$  in  $\mathcal{O}_K / \langle \beta \rangle$ , also ist  $\alpha - z \in \langle \beta \rangle$ ). Wir behaupten, dass für alle  $s \in \mathbb{N}_1$  gilt:

$$\mathcal{O}_K \subseteq \mathbb{Z}[\omega] + \langle \beta^s \rangle.$$

Für  $s = 1$  folgt dies unmittelbar aus (\*). Kennt man die Inklusion für ein  $s$  und mutipiziert man dies mit  $\beta$ , so erhält man

$$\begin{aligned} \langle \beta \rangle &= \beta \mathcal{O}_K \subseteq \beta \mathbb{Z}[\omega] + \langle \beta^{s+1} \rangle \\ &\subseteq \mathbb{Z}[\omega] + \langle \beta^{s+1} \rangle \end{aligned}$$

(dabei hat man verwendet, dass  $\beta$  zu  $\mathbb{Z}[\omega]$  gehört). Wir setzen dies in (\*) ein und sehen:

$$\mathcal{O}_K = \mathbb{Z} + \langle \beta \rangle \subseteq \mathbb{Z} + \mathbb{Z}[\omega] + \langle \beta^{s+1} \rangle = \mathbb{Z}[\omega] + \langle \beta^{s+1} \rangle.$$

Für  $s = \phi(n)a$  erhalten wir

$$\mathcal{O}_K \subseteq \mathbb{Z}[\omega] + \langle \beta^{\phi(n)a} \rangle \subseteq \mathbb{Z}[\omega] + \langle p^a \rangle \subseteq \mathbb{Z}[\omega],$$

die umgekehrte Inklusion  $\mathbb{Z}[\omega] \subseteq \mathcal{O}_K$  ist trivialerweise erfüllt. Damit haben wir also  $\mathcal{O}_K = \mathbb{Z}[\omega]$  gezeigt.

Da  $\mathcal{O}_K = \mathbb{Z}[\omega]$ , ist  $\Delta_K = \Delta(1, \omega, \dots, \omega^{\phi(n)-1})$ , und dies ist nach Folgerung (4) betragsmäßig eine  $p$ -Potenz.

**Folgerung.** Die einzige Primzahl, die in  $\mathbb{Q}[\omega]$  verzweigt ist, ist  $p$ .

Beweis: 6.6.