Algebraische Zahlentheorie
4. Übungsblatt

TECHNISCHE UNIVERSITÄT DARMSTADT

Fachbereich Mathematik
Prof. Dr. J. H. Bruinier
Dipl.-Math. E. Hofmann

SS 2010
19. Mai 2010

Gruppenübung

Dieses Blatt befasst sich mit den Eigenschaften von Kreisteilungskörpern $\mathbb{Q}[\omega]$, mit $\omega = e^{2\pi i/m}$. Dabei soll folgender Satz bewiesen werden:

Satz 1. *Ist m Potenz einer ungeraden Primzahl p, so ist der Ring der ganzen Zahlen im m-ten Kreisteilungskörper $\mathbb{Q}[\omega]$, also $\Omega \cap \mathbb{Q}[\omega]$, durch $\mathbb{Z}[\omega]$ gegeben.*

Die Aufgaben G1, G2 und G3 stellen hierfür Hilfaussagen bereit.

Aufgabe G1
In dieser Aufgabe sei m eine ganze Zahl, $m \geq 3$, und ω die m-te Einheitswurzel $\omega = e^{2\pi i/m}$. Weisen Sie nach, dass

$$\mathbb{Z}[1-\omega] = \mathbb{Z}[\omega] \qquad \text{und} \quad \mathrm{d}(1-\omega) = \mathrm{d}(\omega),$$

wobei d die Diskriminante bezeichnet.

Aufgabe G2
Sei ω primitive m-te Einheitswurzel, mit m einer ganzen Zahl ≥ 3. Zeigen Sie, dass die Diskriminante $d(\omega) = d(1, \cdots, \omega^{\varphi(m)})$ ein Teiler von $m^{\varphi(m)}$ ist. Hierbei bezeichnet $\varphi(m)$ die Eulersche-Phi-Funktion, d.h. $\varphi(m) = \sharp\{1 \leq k \leq m\,;\ \mathrm{ggT}(k,m) = 1\}$.
Hinweis: Ist $f(X)$ normiertes Minimalpolynom von ω, so gilt $f(X) \mid X^m - 1$. Gehen Sie ansonsten ähnlich vor, wie in Aufgabe G3 des dritten Übungsblatts.

Aufgabe G3
Sei nun p eine ungerade Primzahl, $m = p^r$ und $\omega = e^{2\pi i/m}$ eine primitive m-te Einheitswurzel. Beweisen Sie folgende Identität

$$\prod_{\substack{1 \leq k \leq m \\ p \nmid k}} \left(1 - \omega^k\right) = p.$$

Das Produkt wird dabei über alle zu p teilerfremden Zahlen zwischen 1 und $m = p^r$ gebildet.
Hinweis: Da ω primitive Einheitswurzel, gilt $\omega^{p^r} = 1$ aber $\omega^{p^{r-1}} \neq 1$.

Aufgabe G4

Wie in der vorherigen Aufgabe sei $\omega = e^{2\pi i/m}$, mit $m = p^r$ Potenz einer ungeraden Primzahl. Beweisen Sie nun Satz 1.

Vorgehensweise:

- Man setze $B = \Omega \cap \mathbb{Q}[\omega]$. Jedes $\alpha \in B$ lässt sich in der Form
$$\alpha = \frac{1}{\mathrm{d}} \left(a_0 + a_1(1-\omega) + \cdots + a_{n-1}(1-\omega)^{n-1} \right),$$
mit $a_0, \ldots .a_{n-1} \in \mathbb{Z}$ und $n = \varphi(m)$ darstellen. (Warum?)
Nehmen Sie zunächst an, $B \neq \mathbb{Z}[1-\omega]$.
- Folgern Sie aus dieser Annahme, dass es ein $\beta \in B$ gibt, mit
$$\beta = \frac{1}{p} \left(b_i(1-\omega)^i + \cdots + b_{n-1}(1-\omega)^{n-1} \right),$$
mit einem $i \leq n-1$ und b_j ganzen Zahlen, wobei $p \nmid b_i$. (Hinweis: Aufgabe G2)
- Weisen Sie nun mittels Aufgabe G3 nach:
$$\frac{\beta p}{(1-\omega)^{i+1}} \in B.$$
- Leiten Sie einen Widerpruch her und zeigen Sie $B = \mathbb{Z}[\omega]$.