Algebraische Zahlentheorie
9. Übungsblatt

TECHNISCHE UNIVERSITÄT DARMSTADT

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

SS 2010
30. Juni 2010

Gruppenübung

Aufgabe G1
Seien K, L Zahlkörper mit $K \subset L$ und $\mathcal{O}_K \subset \mathcal{O}_L$ deren Ganzheitsringe. Sei A eine additive Untergruppe von L und A^{-1} das Inverse, gegeben durch $A^{-1} = \{\alpha \in L\,;\ \alpha A \subset \mathcal{O}_L\}$. Ferner sei A^* das Dual von A bezüglicher der Spur,

$$A^* = \left\{\alpha \in L\,;\ \mathrm{tr}_{L/K}(\alpha A) \subset \mathcal{O}_K\ \right\}.$$

(a) Man kann L sowohl als $\mathcal{O}_L$- als auch als $\mathcal{O}_K$-Modul betrachten. Zeigen Sie, dass A^{-1} ein $\mathcal{O}_L$-Untermodul, A^* hingegen ein $\mathcal{O}_K$-Untermodul ist.

(b) Die *Differente* ist für eine additive Untergruppe A als $\mathrm{diff}\,A = (A^*)^{-1}$ definiert. Zeigen Sie folgende Aussagen, dabei seien A und B additive Untergruppen von L und $\mathfrak{I}$ ein gebrochenes Ideal.
- $\mathrm{diff}\,A \subset \left(A^{-1}\right)^{-1}$. Für Ideale gilt sogar $\mathrm{diff}\,\mathfrak{I} \subset \mathfrak{I}$.
- $\mathfrak{I} \cdot \mathfrak{I}^* \subset \mathcal{O}_L^*$ und $\mathfrak{I}^{-1}\mathcal{O}_L^* \subset \mathfrak{I}^*$.
- $\mathfrak{I} \cdot \mathfrak{I}^* = \mathcal{O}_L^*$.
- $\mathfrak{I}^{**} = \mathfrak{I}$
- $\mathrm{diff}\,\mathfrak{I} = \mathfrak{I}\,\mathrm{diff}\,\mathcal{O}_L$.

Aufgabe G2
Seien m, n quadratfreie ganze Zahlen, mit $m, n \neq 1$ und $m \neq n$. Der biquadratische Zahlkörper $K = \mathbb{Q}(\sqrt{m}, \sqrt{n})$ ist eine normale Erweiterung von $\mathbb{Q}$; Seine Galois-Gruppe ist isomorph zu $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Im Folgenden bezeichne p eine Primzahl.

(a) K hat drei quadratische Teilkörper. Geben Sie diese an!

(b) Es sei p in jedem der quadratischen Teilkörper verzweigt. Was geschieht dann in K? Geben Sie ein Beispiel für diese Situation an!

(c) Es sei p in jedem der quadratischen Teilkörper vollständig zerlegt. Was geschieht dann in K? Geben Sie ein Beispiel für diese Situation an!

(d) Es sei p träge in jedem der quadratischen Teilkörper. Was geschieht dann in K? Kann dieser Fall überhaupt eintreten?

(e) Finden sie je ein Beispiel, in welchem p folgendes Zerlegungsverhalten in K aufweist: $p = \mathfrak{p}\mathfrak{q}$, $p = \mathfrak{p}^2\mathfrak{q}^2$ und $p = \mathfrak{p}^2$.

Aufgabe G3 (Legendre-Symbol)
Zu einer Primzahl p und einer ganzen Zahl a ist das *Legendresymbol* $\left(\frac{a}{p}\right)$ wie folgt definiert:

$$\left(\frac{a}{p}\right) = \begin{cases} +1 & \text{falls } \operatorname{ggT}(a,p) = 1 \text{ und } x^2 \equiv a \mod p \text{ lösbar ist} \\ -1 & \text{falls } \operatorname{ggT}(a,p) = 1 \text{ und } x^2 \equiv a \mod p \text{ nicht lösbar ist} \\ 0 & \text{falls } a \equiv 0 \mod p. \end{cases}$$

Weisen Sie nun folgende Eigenschaften des Legendresymbols nach:

(a) Es ist $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$ wenn $a \equiv b \mod p$.

(b) Es gilt $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

(c) Es gilt
$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \mod p, \quad \text{insbesondere} \quad \left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \mod p.$$

(d) Es gilt $\left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right)$ falls $p \nmid b$.

Aufgabe G4 (Dirichletscher Primzahlsatz)
Beweisen Sie folgenden Satz: Zu jeder natürlichen Zahl n gibt es unendlich viele Primzahlen, für welche $p \equiv 1 \mod n$ gilt.
Hinweise: Nehmen Sie an, es gäbe nur endlich viele solche Primzahlen. Sei P deren Produkt. Betrachtet man die Zahlen $\Phi_n(nPx)$, $x \in \mathbb{Z}$, wobei Φ_n das n-te Kreisteilungspolynom ist, so können diese nicht alle gleich 1 sein. Also gibt es eine Primzahl p mit $p \mid \Phi_n(nxP)$ für ein geeignetes x. Leiten Sie hieraus einen Widerspruch her.