Prof. Dr. Peter Bürgisser
Paul Breiding
Jesko Hüttenhain

Technische Universität Berlin
Fakultät II, Institut für Mathematik
Sekretariat MA 3-2

Übungen zur Vorlesung Algebra 2

Sommersemester 2014

Aufgabenzettel 9

Aufgabe 1 (15 Punkte). Wir erweitern die Definition des Legendresymbols $\left(\frac{\cdot}{p}\right)$: Sei $a \in \mathbb{Z}$, $b \in \mathbb{N}_{>1}$ und $b = \prod_{i=1}^{r} p_i$ die Primfaktorzerlegung von b. Das *Jacobisymbol* ist dann definiert durch

$$\left(\frac{a}{b}\right) := \prod_{i=1}^{r} \left(\frac{a}{p_i}\right), \quad \left(\frac{a}{1}\right) := 1.$$

Zeige folgende Aussagen:

(1) Falls $a_1 \equiv a_2 \bmod b$, dann $\left(\frac{a_1}{b}\right) = \left(\frac{a_2}{b}\right)$.

(2) $\left(\frac{a_1 a_2}{b}\right) = \left(\frac{a_1}{b}\right)\left(\frac{a_2}{b}\right)$.

(3) $\left(\frac{a}{b_1 b_2}\right) = \left(\frac{a}{b_1}\right)\left(\frac{a}{b_2}\right)$.

(4) Für ungerade a, b: $\left(\frac{b}{a}\right) = (-1)^{\frac{(a-1)(b-1)}{4}} \left(\frac{a}{b}\right)$.

(5) $\left(\frac{-1}{b}\right) = (-1)^{\frac{b-1}{2}}$.

(6) Für ungerades b: $\left(\frac{2}{b}\right) = (-1)^{\frac{b^2-1}{8}}$. (Die Aussage von Aufgabe 3 darf verwendet werden.)

(7) Aus $\left(\frac{a}{b}\right) = -1$ folgt, dass a kein quadratischer Rest modulo b ist.

(8) Falls b zusammengesetzt ist, ist die Rückrichtung von (7) falsch.

Aufgabe 2 (5 Punkte). Die Eigenschaften (1) bis (6) können wir nutzen um das Jacobisymbol auf effziente Weise zu berechnen. Zum Bespiel ist

$$\left(\frac{1363}{65537}\right) \overset{(4)}{=} \left(\frac{65537}{1363}\right) \overset{(1)}{=} \left(\frac{113}{1363}\right) \overset{(4)}{=} \left(\frac{1363}{113}\right) \overset{(1)}{=} \left(\frac{7}{113}\right) \overset{(4)}{=} \left(\frac{113}{7}\right) \overset{(1)}{=} \left(\frac{1}{7}\right) = 1$$

Da 65537 prim ist, folgern wir, dass 1363 ein quadratischer Rest modulo 65537 ist. Berechne nun unter Verwendung von (1) bis (6) das Symbol $\left(\frac{221}{383}\right)$.

Aufgabe 3 (15 Punkte). Sei $p > 2$ eine Primzahl. Zeige, dass gilt

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

Hinweis: Arbeite in $\mathbb{Q}(\zeta_8)$ und gehe anschließend wie in der Vorlesung vor. Zeige, dass $\sqrt{2} = \zeta_8 + \zeta_8^{-1}$, $\sigma_p(\sqrt{2}) = \left(\frac{2}{p}\right)\sqrt{2}$ und $\sigma_p(\sqrt{2}) \equiv \sqrt{2}^p \bmod p\mathbb{Z}[\zeta_8]$.

Die Abgabe erfolgt bis **Dienstag**, den **24.06.2014** vor der Vorlesung. Gutes Gelingen!

Prof. Dr. Peter Bürgisser
Paul Breiding
Jesko Hüttenhain

Technische Universität Berlin
Fakultät II, Institut für Mathematik
Sekretariat MA 3-2

Aufgabe 4 (15 Punkte). Sei $n \in \mathbb{Z}$. Zeige, dass es einen Kreisteilungskörper $\mathbb{Q}(\zeta)$ gibt, der $\mathbb{Q}(\sqrt{n}) \subseteq \mathbb{Q}(\zeta)$ erfüllt. Verwende dazu folgendes Zwischenergebnis von Zettel 4, Aufgabe 3: Falls $\mathrm{ggT}(n,m) = 1$, dann ist $\mathbb{Q}(\zeta_n)\mathbb{Q}(\zeta_m) = \mathbb{Q}(\zeta_{nm})$.

Bemerkung: Die Aussage von Aufgabe 4 ist Teil des Theorems von Kronecker-Weber, welches aussagt, dass jede abelsche Erweiterung von $\mathbb{Q}$ in einem Kreisteilungskörper enthalten ist. Die Untersuchung aller abelschen Erweiterungen eines beliebigen Zahlkörpers $\mathbb{K}$ (so nennt man endliche algebraische Erweiterungen von $\mathbb{Q}$) ist Gegenstand der Klassenkörpertheorie. Über $\mathbb{K}$ wird das quadratische Reziprozitätsgesetzt, welches wir aus der Vorlesung kennen, durch das Artinsche Reziprozitätsgesetzt verallgemeinert. Mit Hilfe dieses Reziprozitätsgesetzes kann nun der Klassenkörper von $\mathbb{K}$ definiert werden. Der Klassenkörper von $\mathbb{K}$ ist die kleinste algebraische Erweiterung von $\mathbb{K}$, welche alle abelschen Erweiterungen von $\mathbb{K}$ enthält. Das Theorem von Kronecker-Weber besagt, dass der Klassenkörper von $\mathbb{Q}$ von den Polynomen $\{X^n - 1 | n \in \mathbb{N}\}$ erzeugt wird. Im Falle, dass $\mathbb{K} = \mathbb{Q}(\sqrt{d})$, wobei $d < 0$, kann mit Hilfe elliptischer Kurven eine große Klasse abelscher Erweiterungen von $\mathbb{K}$ berechnet werden. Jedoch existieren bis heute keine entsprechenden Aussagen über abelsche Erweiterungen von $\mathbb{Q}(\sqrt{d})$, wobei $d > 0$.