Mathematisches Institut der Universität Heidelberg

Prof. Dr. R. Weissauer/Dr. U. Weselmann

Übungen zur Algebraischen Zahlentheorie SS 2007

Blatt 9 Abgabe bis Donnerstag 21.06.2007 um 14:00 Uhr

Aufgabe 31) Zeige, dass für eine Körpererweiterung $F/\mathbb{Q}_p$ und eine natürliche Zahl $f \geq 2$ die folgenden Aussagen äquivalent sind:

(a) $F/\mathbb{Q}_p$ ist eine unverzweigte Erweiterung vom Grad f.

(b) F ist Zerfällungskörper des Polynoms $X^{p^f} - X$ über $\mathbb{Q}_p$.

(c) $[F : \mathbb{Q}_p] = f$ und F enthält einen Zerfällungskörper des Polynoms $X^{p^f} - X$ über $\mathbb{Q}_p$.

(3 Punkte)

Aufgabe 32) Sei $L/\mathbb{Q}$ ein Zerfällungskörper des Polynoms

$$P(X) = X^3 - X + 1;$$

es seien $\alpha_1, \alpha_2, \alpha_3$ die Nullstellen von $P(X)$ in L.

Sei $K = \mathbb{Q}(\sqrt{-23}) \subset L$ der quadratische Unterkörper.

(a) Zeige: Bei geeigneter Wahl des Vorzeichens von $\sqrt{-23}$ gilt:

$$\sqrt{-23} \cdot (\alpha_2 - \alpha_3) = 6\alpha_1^2 + 9\alpha_1 - 4.$$

(b) Zeige: $\mathcal{O}_L$ wird als $\mathcal{O}_K$-Modul von $1, \alpha_1, \alpha_1^2$ und $\alpha_2 - \alpha_3$ erzeugt. Folgere daraus, dass $\mathcal{O}_L$ als Ring von α_1, α_2 und α_3 erzeugt wird.

(c) Zeige: die Erweiterung L/K ist unverzweigt.

(d) Zeige: jedes Ideal $\mathfrak{a}$ in $\mathcal{O}_K$ wird in $\mathcal{O}_L$ zu einem Hauptideal.

(6=1+2+2+1 Punkte)

Aufgabe 33) Wir behalten die Bezeichnungen der Aufgabe 32) bei. Für eine Primzahl $p \neq 23$ gebe man das Zerlegungsverhalten in $L/\mathbb{Q}$ an, wenn die Gleichung $x^3 - x + 1 = 0$

(a) genau drei Lösungen in $\mathbb{F}_p$ hat;

(b) keine Lösung in $\mathbb{F}_p$ hat;

(c) genau eine Lösung in $\mathbb{F}_p$ hat.

Welche Ordnung hat dann jeweils die Konjugationsklasse des Frobenius F_p? Was lässt sich in den Fällen (a), (b) bzw. (c) jeweils über die Lösbarkeit der Kongruenz $y^2 \equiv -23 \; mod \; p$ sagen?

(3 Punkte)

Aufgabe 34) Sei $K = \mathbb{Q}(\sqrt{-23})$ und $p \neq 23, p \neq 2$ eine Primzahl, für welche die Kongruenz $y^2 \equiv -23 \; mod \; p$ eine Lösung hat. Zeige, dass genau einer der beiden folgenden Fälle eintritt:

(a) Es gibt $a, b \in \mathbb{Z}$ mit $\qquad p = a^2 + 23 \cdot b^2$;

(b) Es gibt $a, b \in \mathbb{Z}$ mit $\quad 8 \cdot p = a^2 + 23 \cdot b^2$.

Nach Aufgabe 25)b) existiert in $\mathcal{O}_K$ eine Zerlegung $p = \mathfrak{p}_1 \cdot \mathfrak{p}_2$. Wie kann man die auftretenden Primideale $\mathfrak{p}_1, \mathfrak{p}_2$ mit Hilfe der a, b beschreiben?

Hinweis: Benutze Aufgabe 20)b) und die Ideale $(1), \mathfrak{a}$ und $\bar{\mathfrak{a}}$ aus Aufgabe 4) sowie die Normabbildung.

(4 Punkte)

Zusatzaufgabe: Man untersuche mit Hilfe eines Computeralgebraprogramms für alle in Frage kommenden Primzahlen $p \leq 130$, ob es einen Zusammenhang zwischen dem Eintreten der Fälle (a) bzw. (b) in Aufgabe 34) und dem Eintreten der Fälle in Aufgabe 33) gibt.

(3 Punkte)