LEHRSTUHL A FÜR MATHEMATIK
Prof. Dr. A. Krieg, A. Marschner

Aachen, den 21. Mai 2003

3. Übung zur Algebraischen Zahlentheorie

Abgabe: Montag, 02.06.2003, 12.00 Uhr

Aufgabe 1 (10 Punkte): Sei $K = \mathbb{Q}(\sqrt[3]{n})$ mit $n \in \mathbb{N}$, $n \geq 2$ quadratfrei.

a) $\alpha = a + b\sqrt[3]{n} + c\sqrt[3]{n^2}$ erfüllt $\alpha \in o_K$ genau dann, wenn

$$S(\alpha) = 3a \in \mathbb{Z}, \quad N(\alpha) = a^3 + nb^3 + n^2c^3 - 3nabc \in \mathbb{Z} \quad \text{und} \quad T(\alpha) = 3a^2 - 3nbc \in \mathbb{Z}.$$

b) Für $\mathcal{M} = \mathbb{Z} + \mathbb{Z}\sqrt[3]{n} + \mathbb{Z}\sqrt[3]{n^2}$ gilt

$$\mathcal{M} \subset o_K \subset \frac{1}{3}\mathcal{M}.$$

c) Für $n \not\equiv \pm 1 \mod 9$ gilt

$$o_K = \mathcal{M} \quad \text{und} \quad d_K = -27n^2.$$

d) Für $n \equiv \pm 1 \mod 9$ gilt

$$o_K = \mathbb{Z}\omega + \mathbb{Z}\sqrt[3]{n} + \mathbb{Z}\sqrt[3]{n^2} \quad \text{mit} \quad \omega = \frac{1}{3}(1 + n\sqrt[3]{n} + \sqrt[3]{n^2}) \quad \text{und} \quad d_K = -3n^2.$$

Aufgabe 2 (10 Punkte):
Es sei $\mathcal{R}$ ein Integritätsbereich mit Quotientenkörper K. Die Polynome $f, g \in \mathcal{R}[X]$ seien durch $f(X) = \sum_{i=0}^{m} f_i X^i$ und $g(X) = \sum_{i=0}^{n} g_i X^i$ gegeben. Wir definieren die Resultante von f und g wie folgt:
$\mathrm{Res}(f,g) = \det S$ mit

$$S := \begin{pmatrix}
f_m & f_{m-1} & f_{m-2} & \cdots & f_1 & f_0 & 0 & 0 & \cdots & 0 \\
0 & f_m & f_{m-1} & f_{m-2} & \cdots & f_1 & f_0 & 0 & \cdots & 0 \\
0 & 0 & f_m & f_{m-1} & f_{m-2} & \cdots & f_1 & f_0 & \cdots & 0 \\
\vdots & \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\
0 & 0 & \cdots & 0 & f_m & f_{m-1} & f_{m-2} & \cdots & f_1 & f_0 \\
g_n & g_{n-1} & g_{n-2} & \cdots & g_1 & g_0 & 0 & 0 & \cdots & 0 \\
0 & g_n & g_{n-1} & g_{n-2} & \cdots & g_1 & g_0 & 0 & \cdots & 0 \\
0 & 0 & g_n & g_{n-1} & g_{n-2} & \cdots & g_1 & g_0 & \cdots & 0 \\
\vdots & \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\
0 & 0 & \cdots & 0 & g_n & g_{n-1} & g_{n-2} & \cdots & g_1 & g_0
\end{pmatrix},$$

wobei die Koeffizienten von f über $n = \deg g$ und die Koeffizienten von g über $m = \deg f$ Reihen wiederholt werden. Ist $\mathcal{R}$ selber ein Polynomring, so schreiben wir $\mathrm{Res}_X(f,g)$, um anzudeuten bezüglich welcher Variablen die Resultante gebildet wird. Zeigen Sie:

a) $\mathrm{Res}(f,g) \in \mathcal{R}$ und es gilt $\mathrm{Res}(f,g) = 0$ genau dann, wenn $\mathrm{ggT}(f,g) \neq 1$ gilt.
Hinweis: Stelle das kgV als Vielfaches von f und g dar und betrachte das sich ergebende Gleichungssystem für die Koeffizienten.

b) Nun sei K vollkommen, d. h. jedes Polynom in $K[X]$ ist separabel. Dabei heißt ein Polynom $f \in K[X]$ separabel, falls jeder irreduzible Faktor von f nur einfache Wurzeln hat. Ist $\overline{K}$ ein algebraischer Abschluß von K und zerfallen f und g über $\overline{K}$ als $f(X) = f_m \cdot \prod_{i=1}^{m}(X - \alpha_i)$ und $g(X) = g_n \cdot \prod_{i=1}^{n}(X - \beta_i)$, so gilt:

$$\begin{aligned}\mathrm{Res}(f,g) &= f_m^n \prod_{i=1}^{m} g(\alpha_i) \\ &= (-1)^{mn} g_n^m \prod_{i=1}^{n} f(\beta_i) \\ &= f_m^n g_n^m \prod_{\substack{1\le i\le m \\ 1\le j\le n}} (\alpha_i - \beta_j).\end{aligned}$$

Hinweis: Es sei $V = (v_{ij})_{i,j}$ die Vandermondesche Matrix mit

$$v_{ij} = \begin{cases} \beta_j^{m+n-i} & \text{für } j \le n \\ \alpha_{j-n}^{m+n-i} & \text{sonst.} \end{cases}$$

Berechne die Determinanten von V und SV.

c) $\alpha_i + \beta_j$ ist Nullstelle des Polynoms $\mathrm{Res}_Y(f(X-Y), g(Y))$ und $\alpha_i\beta_j$ ist Nullstelle von $\mathrm{Res}_Y(Y^m f(\frac{X}{Y}), g(Y))$.

d) Folgern Sie aus c) konstruktiv, dass die Menge o aller ganz-rationalen Zahlen ein Ring ist.

Aufgabe 3 (5 Punkte):
Sei K ein quadratischer Zahlkörper der Diskriminante d_K. Zeigen Sie, dass

$$\mathcal{A} := \{\alpha \in o_K; \mathrm{N}(\alpha) \equiv 0 \mod d_K\}$$

ein Ideal in o_K ist mit

$$[o_K : \mathcal{A}] = |d_K|.$$

Literatur

- T. M. Apostol, Introduction to Analytic Number Theory, UTM, Springer-Verlag, 1976, 1984.
- S. I. Borewicz and I. R. Safarevic, Zahlentheorie, Birkhäuser Verlag, 1966, MB: 3600, HB: 32 Za 5775.
- H. Cohn, A classical invitation to algebraic numbers and class fields, Universitext, Springer-Verlag, !978, 1988, MB:10056.
- H. Cohen, A course in Computational Algebraic Number Theory, GTM 138, Springer-Verlag, 1993.
- H. M. Edwards, Fermat's last theorem, GTM 50, Springer-Verlag, 1977, MB: 9404.
- K. Ireland and M. Rosen, A classical introduction to algebraic number theory, GTM 84, Springer-Verlag, 1982, 1993, MB:11471.
- S. Lang, Algebraic Number Theory, GTM 110, Springer-Verlag, 1986, 1994.
- A. Leutbecher, Zahlentheorie, Springer-Verlag, 1996.
- D. A. Marcus, Number fields, Universitext, Springer-Verlag, 1977, MB:9492.
- W. Narkiewicz, Elementary and analytic theory of algebraic numbers, PWN, Warszawa, 1974.
- J. Neukirch, Algebraische Zahlentheorie, Springer-Verlag, 1992, MB:16296, HB: Bp 1842.
- M. Pohst und H. Zassenhaus, Algorithmic Algebraic Number Theory, Cambridge Univ. Press, 1989.
- W. Scharlau and H. Opolka, Von Fermat bis Minkowski. Eine Vorlesung über Zahlentheorie und ihre Entwicklung, Springer-Verlag, 1980.
- I. N. Stewart and D. O. Tall, Algebraic number theory, Chapman and Hall, 1979, 1987, MB:10481, HB:Bf 7181.