# Algebraische Zahlentheorie

## Blatt 6 — 02.02.2016

**Aufgabe 24.**

Sei $m \in \mathbb{N}$ und $m > 0$. Zeigen Sie, daß $\cos(2\pi/m)$ über $\mathbb{Q}$ algebraisch ist und bestimmen Sie den Ganzzahlring von $\mathbb{Q}(\cos(2\pi/m))$.

**Aufgabe 25.**

Sei $E/F$ eine endliche Erweiterung von Zahlkörpern. Zeigen Sie unter der Annahme einer der beiden folgenden Bedingungen, daß höchstens endlich viele Primideale $\mathfrak{p}$ von $\mathfrak{o}_F$ in $\mathfrak{o}_E$ unzerlegt sind.

(a) $E/F$ sei galoissch und die Galoisgruppe $\mathrm{Gal}(E/F)$ nicht zyklisch.

(b) $E/F$ besitze Zwischenkörper $E_1 \neq E_2$ mit gleichem Grad $[E_1 : F] = [E_2 : F]$.

*Erinnerung:* Ein Primideal $\mathfrak{p}$ von $\mathfrak{o}_F$ heißt in $\mathfrak{o}_E$ **unzerlegt**, wenn nur ein Primideal $\mathfrak{q}$ von $\mathfrak{o}_E$ ein Teiler von $\mathfrak{p}\mathfrak{o}_E$ ist.

**Aufgabe 26.**

Sei $\alpha$ eine Nullstelle von $X^3 - 13X + 7$ und $E$ eine normale Hülle von $F = \mathbb{Q}(\alpha)$. Zeigen Sie die folgenden Aussagen:

(a) Es gilt $\mathfrak{o}_F = \mathbb{Z}[\alpha]$.

(b) Die Primidealzerlegung von $(5)$ in $\mathfrak{o}_F$ hat die Form $\mathfrak{p}_1\mathfrak{p}_2^2$. Die Primidealzerlegungen von $\mathfrak{p}_1$ und $\mathfrak{p}_2$ in $\mathfrak{o}_E$ haben die Form $\mathfrak{p}_1\mathfrak{o}_E = \mathfrak{P}_1^2$ und $\mathfrak{p}_2\mathfrak{o}_E = \mathfrak{P}_2\mathfrak{P}_3$ für geeignete Primideale $\mathfrak{P}_1, \mathfrak{P}_2, \mathfrak{P}_3$ von $\mathfrak{o}_E$.

(c) $F$ ist der Fixkörper von $E$ unter der Zerlegungsgruppe von $\mathfrak{P}_1$.

**Aufgabe 27.** (Fermat im Fall 1)

Im Folgenden sei $p > 2$ eine Primzahl, $\zeta = \zeta_p$ eine primitive $p$te Einheitswurzel und $F = \mathbb{Q}(\zeta_p)$ der Kreisteilungskörper der $p$ten Einheitswurzeln mit Ganzheitsring $\mathfrak{o}_F = \mathbb{Z}[\zeta_p]$. Wir wollen entlang einer Anleitung den Satz von Fermat im 'ersten Fall', d.h. $p \nmid xyz$, für reguläre[1] Primzahlen beweisen, wie dies schon Ernst Eduard Kummer 1847 konnte.

[1] Eine reguläre Primzahl ist eine Primzahl $p$, die nicht die Klassenzahl von $\mathbb{Q}(\zeta_p)$ teilt. Eine Liste der irregulären Primzahlen findet man unter http://www.research.att.com/~njas/sequences/A000928

**Satz.** *Für eine reguläre Primzahl $p > 2$ hat die Gleichung $X^p + Y^p = Z^p$ keine ganzzahlige Lösung $x, y, z \in \mathbb{Z}$ mit $p \not| xyz$.*

(a) Jede $(p-1)$-elementige Teilmenge von $\{1, \zeta_p, \zeta_p^2, \ldots, \zeta_p^{p-1}\}$ ist eine $\mathbb{Z}$-Basis von $\mathbb{Z}[\zeta_p]$.

(b) Insbesondere ist $a_0 + a_1\zeta_p + \ldots a_{p-1}\zeta_p^{p-1}$ mit ganzen Zahlen $a_i$ für $i = 0, \ldots, p-1$, von denen wenigstens eine verschwindet, genau dann in $\mathbb{Z}[\zeta_p]$ durch $N \in \mathbb{Z}$ teilbar, wenn alle $a_i$ durch $N$ teilbar sind.

(c) Eine Einheit in $\mathbb{Z}[\zeta_p]$ ist ein Produkt aus einer $p$ten Einheitswurzel und einer total reellen Einheit.

*Anleitung*: Sei $\varepsilon = a_0 + a_1\zeta + \ldots a_{p-2}\zeta^{p-2} = f(\zeta)$ mit $f(X) \in \mathbb{Z}[X]$ eine Einheit und sei

$$\vartheta = \varepsilon/\bar{\varepsilon} = f(\zeta)/f(\zeta^{-1}).$$

Zeigen Sie, daß alle Konjugierten von $\vartheta$ den Absolutbetrag 1 haben. Schließen Sie aus multiplikativer Minkowskitheorie, daß $\vartheta$ eine Einheitswurzel ist, und sogar $\vartheta = \pm\zeta^{2n}$ für geeignetes $n$ gilt. Somit ist $\rho = \varepsilon/\zeta^n$ total reell oder $i\rho$ total reell. Letzteres führt modulo $(1-\zeta)$ zum Widerspruch.

(d) Für teilerfremde ganze Zahlen $x, y \in \mathbb{Z}$ und $a \not\equiv b$ aus $\mathbb{Z}/p\mathbb{Z}$ sind $x + \zeta^a y$ und $x + \zeta^b y$ teilerfremde Elemente von $\mathbb{Z}[\zeta_p]$.

(e) Für jedes $\alpha \in \mathbb{Z}[\zeta_p]$ liegt $\alpha^p$ in $\mathbb{Z} + p\mathbb{Z}[\zeta_p]$.

(f) Der Satz gilt für $p = 3$ und $p = 5$.

*Anleitung*: Modulo 9 bzw. 25.

(g) Man darf ohne Einschränkung im Widerspruchsbeweis des Satzes annehmen, daß $x, y, z$ paarweise teilerfremd sind und $p \not| x - y$.

(h) Sei $p > 5$ eine reguläre Primzahl und sei $x, y, z \in \mathbb{Z}$ eine Lösung die dem Satz widerspricht und gemäß (g) normiert ist. Dann gibt es $r \in \mathbb{Z}$, eine total reelle Einheit $\rho \in \mathbb{Z}[\zeta_p]^*$ und $a \in \mathbb{Z}$ mit

$$x + \zeta y \equiv \zeta^r \rho a \mod p\mathbb{Z}[\zeta_p] \tag{$*$}$$

Vergleichen Sie nun $x + \zeta y$ mit seinem Konjugierten $x + \zeta^{-1}y$ und führen Sie die Kongruenz $(*)$ zu einem Widerspruch zu $p \not| (x-y)xy$.

*Anleitung*: Verwenden Sie die Faktorisierung

$$\prod_{j=0}^{p-1}(x + \zeta^j y) = x^p + y^p = z^p.$$

Aus (d) schließen Sie, daß das Ideal $(x + \zeta^j y)$ die $p$te Potenz eines Ideals $\mathfrak{a}_j$ ist. Da $p$ eine reguläre Primzahl ist, muß notwendigerweise $\mathfrak{a}_j$ ein Hauptideal sein. Verwenden Sie dann (c) und (e). Erzwingen Sie zum Schluß den Widerspruch aus Aufgabe (b).

---

**Abgabe:** Am kommenden Dienstag, den 09.02.2016, bis zur Vorlesung in den Kasten im 3. Stock, Institut für Mathemtik, Robert–Mayer Strasse 6-8. Downloads von Übungsblättern und Informationen zur Vorlesung unter

http://www.uni-frankfurt.de/57777299/Algebraische-Zahlentheorie_WS2015_16

---

2. Februar 2016