Leibniz Universität Hannover
Fakultät für Mathematik und Physik
Prof. Dr. M. Schütt
MSc. S. Brandhorst

26. Mai 2016

Einführung in die Algebraische Zahlentheorie
Sommersemester 2016
Blatt 7

Material für die KW 21,22 & 23

Zyklische kubische Zahlkörper

Hintergrund: Ziel dieses kleinen Projekts soll sein, ähnlich wie bei den quadratischen Zahlkörpern aus der Vorlesung, eine vollständige Klassifikation der sogenannten *zyklischen kubischen Zahlkörper* herzuleiten, die als nächst einfachere Klasse angesehen werden kann. Die Klassifikation ist bei weitem nicht so übersichtlich wie bei den quadratischen Zahlkörpern, bei denen im wesentlichen ein Parameter zur Beschreibung ausreicht. Wie Sie sehen werden, spielt die jeweilige Bestimmung einer Ganzheitsbasis und der Diskriminante eine tragende Rolle im Klassifikationsbeweis, was als hauptsächliches unmittelbares Übungsziel (neben konkreten Berechnungen von Normen, Spuren usw.) angesehen werden sollte.

Ein zyklischer kubischer Zahlkörper K ist eine *galoische* Erweiterung von $\mathbb{Q}$ vom Grad 3. Diese werden durch den folgenden Satz vollständig klassifiziert.

Satz Jede Isomorphieklasse eines zyklischen kubischen Zahlkörpers wird im Folgenden genau ein Mal aufgezählt:

1. Falls die Primzahl 3 in K verzweigt, dann ist $K = \mathbb{Q}(\theta)$, wobei
$$\mathrm{minpol}_{\mathbb{Q}}(\theta) = x^3 - \tfrac{e}{3}x - \tfrac{eu}{27} \in \mathbb{Z}[x].$$
Hierbei gilt $e = \frac{u^2+27v^2}{4}$, $u \equiv 6 \bmod 9$, $3 \nmid v$, $u \equiv v \bmod 2$, $v > 0$ und $\frac{e}{9}$ ist ein Produkt von paarweise verschiedenen rationalen Primzahlen, die kongruent zu 1 modulo 3 sind.

2. Falls die Primzahl 3 in K unverzweigt ist, dann ist $K = \mathbb{Q}(\theta)$, wobei
$$\mathrm{minpol}_{\mathbb{Q}}(\theta) = x^3 - x^2 + \tfrac{1-e}{3}x - \tfrac{1-3e+eu}{27} \in \mathbb{Z}[x].$$
Hierbei gilt $e = \frac{u^2+27v^2}{4}$, $u \equiv 2 \bmod 3$, $u \equiv v \bmod 2$, $v > 0$ und e ist ein Produkt von paarweise verschiedenen rationalen Primzahlen, die kongruent zu 1 modulo 3 sind.

   In *beiden* Fällen hat das angegebene Minimalpolynom die Diskriminante e^2v^2 und die Diskriminante des Zahlkörpers K ist e^2.

3. Umgekehrt: Seien $p_1, \dots, p_t$ paarweise verschiedene Primzahlen mit $p_i \equiv 1 \bmod 3$, sowie $e = 9\prod_{i=1}^{t-1} p_i$ (bzw. $e = \prod_{i=1}^{t} p_i$). Dann gibt es bis auf Isomorphie genau 2^{t-1} zyklische kubische Zahlkörper mit Diskriminante e^2; diese werden durch die Polynome in (1) – bzw. (2) – spezifiziert.

Literatur: Sie sollen sich den Beweis in einer Folge von Schritten erarbeiten, die im Folgenden kurz skizziert werden. Als Grundlage zum gesamten Beweis dient §6.4.2 (mit Rückgriffen auf §6.1.1 und §6.1.2) des Buches *A Course in Computational Algebraic Number Theory* von H. Cohen. Alle Angaben beziehen sich auf diesen Text.

Sei K ein zyklischer kubischer Zahlkörper.

1. **Aussage** Machen Sie sich die Aussage des Satzes überhaupt klar, und bestimmen Sie zum Beispiel alle zyklischen kubischen Zahlkörper mit Diskriminante 1729^2, indem Sie die zugehörigen Polynome (laut Satz) explizit auflisten.

2. **Vorüberlegungen** Frischen Sie aus der Algebra auf (vgl. Prop 6.4.3): Sei K der Zerfällungskörper eines irreduziblen Polynoms $f \in \mathbb{Q}[x]$ vom Grad n. Wann ist die Galoisgruppe $\mathrm{Gal}(f)$ (als Permutationen der Nullstellen von f aufgefaßt) eine Untergruppe der alternierenden Gruppe A_n?
Warum ist der Körper K total-reell? Sei $\omega := \zeta_3 = \exp(\frac{2\pi i}{3})$. Beschreiben Sie die Galoisgruppe $\mathrm{Gal}(K(\omega)) = \langle \sigma, \tau \rangle$, wobei $\mathrm{Gal}(K) = \langle \sigma \rangle$ und τ durch komplexe Konjugation induziert wird.

   Ohne Einschränkung können wir voraussetzen, dass $K = \mathbb{Q}(\theta)$ mit $\theta \in \overline{\mathbb{Z}}$ und $p(x) := \mathrm{minpol}_{\mathbb{Q}}(\theta) = x^3 - Sx^2 + Tx - N \in \mathbb{Z}[X]$ (warum wurden S und N als Namen für zwei dieser Koeffizienten gewählt?). Das Minimalpolynom wird zunächst näher spezifiziert:

3. **Beweisen Sie 6.4.4** Setze $\gamma := \theta + \omega^2\sigma(\theta) + \omega\sigma^2(\theta) \in K(\omega)$ und $\beta = \frac{\gamma^2}{\tau(\gamma)}$. Dann gilt $\beta \in \mathbb{Q}(\omega)$, und mit $e = \mathrm{Norm}_{\mathbb{Q}(\omega)/\mathbb{Q}}(\beta)$ und $u = \mathrm{Spur}_{\mathbb{Q}(\omega)/\mathbb{Q}}(\beta)$ gilt:

$$p(x) = x^3 - Sx^2 + \tfrac{S^2-e}{3}x - \tfrac{S^3-3Se+eu}{27}.$$

4. **Modifikation von θ** Nun wird das primitive Element durch eine Transformation der Form $\theta \rightsquigarrow b\theta + c\sigma(\theta)$ mit $b, c \in \mathbb{Q}$ modifiziert. Überlegen Sie sich zuerst, dass die Parameter γ und β wie folgt transformieren: $\gamma \rightsquigarrow (b + c\omega)\gamma$ und $\beta \rightsquigarrow \frac{(b+c\omega)^2}{b+c\omega^2}\beta$. Versuchen Sie dann nachzuvollziehen (S.337f), warum es eine solche Transformation gibt derart, dass (erstens) $\beta \in \mathbb{Z}[\omega]$ (zweitens) Norm (als Element von $\mathbb{Z}[\omega]$ aufgefaßt) e hat, wobei e das Produkt von paarweise verschiedenen rationalen Primzahlen $\equiv 1 \bmod 3$ ist (hierzu ist die Kenntnis der Primideale in $\mathbb{Z}[\omega]$ entscheidend!).

5. **Beweisen Sie 6.4.5** Vervollständigen Sie mit dem vorherigen Schritt den Beweis dieses Lemmas und zeigen Sie, dass es zu jedem zyklischen kubischen Zahlkörper *genau ein Paar* ganzer Zahlen e, u gibt derart, dass $K = \mathbb{Q}(\theta')$ mit

$$\mathrm{minpol}_{\mathbb{Q}}(\theta') = x^3 - \tfrac{e}{3}x - \tfrac{eu}{27},$$

   e ein Produkt von paarweise verschiedenen Primzahlen $\equiv 1 \bmod 3$ ist, und $u \equiv 2 \bmod 3$ gilt. (Dies folgt im wesentlichen aus einer weiteren Modifikation des primitiven Elements θ der Form $\theta \rightsquigarrow a + \theta$ mit geeignetem $a \in \mathbb{Q}$ derart, dass das neue Element Spur Null besitzt).

6. **Interludium 1** Lernen Sie den Begriff des p-Radikals (Definition 6.1.1) kennen und charakterisieren Sie diesen, indem Sie Proposition 6.1.2 beweisen.

7. **Interludium 2** Beweisen Sie die folgende Verfeinerung der Methode aus der Vorlesung zur Konstruktion von Ganzheitsbasen: Theorem 6.1.3.

8. **Interludium 3** Beweisen Sie das (technische) Dedekindsche Kriterium 6.1.4.

   Wenn Sie wollen, können Sie diesen mittleren Einschub (6)–(8) überspringen und sich damit zufriedengeben, das Dedekindsche Kriterium im Folgenden nur anzuwenden.

9. **Beweisen Sie 6.4.7** Im Augenblick haben wir eine Reduktion auf den Fall $K = \mathbb{Q}(\theta)$ mit $p(x) = \mathrm{minpol}_{\mathbb{Q}}(\theta) = x^3 - 3ex - eu$, $e = \frac{u^2+3v^2}{4}$ und u, e wie unter Punkt (5) geführt. Zeigen Sie, dass $\mathbb{Z}[\theta]$ p-maximal ist für Primzahlen $p \in \mathbb{P}$ mit $p \mid e$.

10. **Beweisen Sie 6.4.8** Folgern Sie aus dem vorherigen Punkt, dass (erstens) das Polynom $p(x)$ Diskriminante $81e^2v^2$ besitzt und (zweitens) $e^2 \mid d_K$.

11. **Beweisen Sie 6.4.9** Falls $3 \nmid v$, so ist $\mathbb{Z}[\theta]$ 3-maximal.

12. **Beweisen Sie 6.4.10** Bestimmen Sie ganz explitit die algebraischen Konjugierten $\sigma(\theta)$ und $\sigma^2(\theta)$ des bisherigen primitiven Elements θ.

13. **Beweisen Sie 6.4.11** Mit anderen Worten: Bestimmen Sie eine Ganzheitsbasis des kubischen Zahlkörpers $K = \mathbb{Q}(\theta)$ (wie unter Punkt (9) beschrieben). Falls $3 \nmid v$, so ist $(1, \theta, \sigma(\theta))$ eine Ganzheitsbasis und $d_K = (9e)^2$. Falls $3 \mid v$, so ist $(1, \theta', \sigma(\theta'))$ eine Ganzheitsbasis, wobei $\theta' = \frac{\theta+1}{3}$, und $d_K = e^2$.

14. **Abschluss** Vervollständigen Sie den Beweis des Klassifikationssatzes für zyklische kubische Zahlkörper (S.342f).