Übungen zur "Algebraische Zahlentheorie"
SS20 Blatt 8

Ausgabe: 6.7.2020, **Abgabe:** 13.7.2020

Informationen zur Vorlesung finden Sie unter:

http://home.mathematik.uni-freiburg.de/arithgeom/lehre/ss20/algzt/index.html

Alle Lösungen sind vollständig zu begründen. Bei Aufgaben, die als *mit SAGE* deklariert sind, erklären Sie, wie Sie vorgegangen sind, d.h. dokumentieren Sie, was Sie SAGE haben rechnen lassen.
Bonusaufgaben gehen nicht in die Pflichtwertung ein, sondern können benutzt werden, um zusätzliche Punkte zu erhalten.

Aufgabe 8.1: (ohne SAGE; 10 Punkte) Wir wollen nochmal neu aufgreifen, dass sich jede Primzahl der Form $p = 4k+1$ mit $k \in \mathbb{N}$ als Summe von zwei Quadraten, also in der Form $p = x^2 + y^2$ mit $x, y \in \mathbb{Z}$, schreiben lässt.
Wir folgen den Schritten:

1. Zeigen Sie, dass $\mathbb{F}_p^\times$ ein Element u von genauer Ordnung 4 enthält. Folgern Sie, dass $u^2 \equiv -1 \bmod p$.

2. Sei $L \subseteq \mathbb{Z}^2$ die Teilmenge aller Paare (a, b) mit

$$b \equiv ua \pmod{p}.$$

   Zeigen Sie, dass L ein Gitter im $\mathbb{R}^2$ ist.

3. Zeigen Sie, dass $[\mathbb{Z}^2 : L] = p$.

4. Bestimmen Sie das Kovolumen von L bezüglich des Lebesgue-Maßes auf $\mathbb{R}^2$.

5. Zeigen Sie, dass ein Punkt $(a, b) \in L$ existiert mit

$$0 \neq a^2 + b^2 \leq \frac{3}{2}p.$$

6. Zeigen Sie, dass $a^2 + b^2$ ein Vielfaches von p sein muss, was strikt zwischen 0 und $2p$ liegt. Nutzen Sie Aufgabenteil (2).

Natürlich bleibt dieser Ansatz schwächer als das präzisere Resultat in Aufgabe 5.3.7 (wie genau folgt das obige Resultat nämlich daraus?).

Aufgabe 8.2: (ohne SAGE; 15 Punkte) Wir wollen mit einer ähnlichen Idee zeigen: Jede positive ganze Zahl x ist die Summe von vier Quadraten,

$$x = a^2 + b^2 + c^2 + d^2$$

mit $a, b, c, d \in \mathbb{Z}$.

1. Beweisen Sie die Aussage direkt für $x = 2$.

2. Wir beweisen die Aussage in den folgenden Schritten nun für den Spezialfall, dass x eine ungerade Primzahl p ist:

   (a) Zeigen Sie, dass es $u, v \in \mathbb{Z}$ gibt mit $u^2 + v^2 + 1 \equiv 0 (\mathrm{mod}\, p)$. Zählen Sie dazu, wie viele verschiedene Werte u^2 und $v^2 + 1$ in $\mathbb{F}_p$ annehmen (Idee: "Der Körper ist doch recht beengt.").

   (b) Betrachten Sie die Teilmenge

   $$L := \left\{ (a, b, c, d) \in \mathbb{Z}^4 \;\middle|\; \begin{array}{ll} c \equiv ua + vb & (\mathrm{mod}\, p) \\ d \equiv ub - va & (\mathrm{mod}\, p) \end{array} \right\}.$$

   (c) Berechnen Sie den Index $[\mathbb{Z}^4 : L]$.

   (d) Beweisen Sie, dass es ein $(a, b, c, d) \neq 0$ in L gibt, welches $a^2 + b^2 + c^2 + d^2 < 2p$ erfüllt.

   (e) Folgern Sie, dass $a^2 + b^2 + c^2 + d^2 = p$.

3. Die allgemeine Aussage folgt aus der Identität

   $$\begin{aligned} (a^2 + b^2 + c^2 + d^2)(A^2 + B^2 + C^2 + D^2) \\ = (aA - bB - cC - dD)^2 + (aB + bA + cD - dC)^2 \\ + (aC - bD + cA + dB)^2 + (aD + bC - cB + dA)^2, \end{aligned}$$

   die Sie nicht nachrechnen müssen.[1]

4. Zeigen Sie, dass drei Quadrate nicht genügen, um jede positive ganze Zahl darzustellen.

Aufgabe 8.3: (ohne SAGE; 15 Punkte) Wir betrachten den Zahlkörper $F = \mathbb{Q}(\alpha)$, wobei α das Minimalpolynom

$$T^3 + T^2 - 2T + 8$$

habe. Wir wollen einige Schritte, die wir bisher nur mittels SAGE bestimmen konnten, solide beweisen:

1. Berechnen Sie die Diskriminante des Minimalpolynoms.

2. Folgern Sie, dass entweder $\mathcal{O}_F = \mathbb{Z}[\alpha]$ gilt, oder aber $[\mathcal{O}_F : \mathbb{Z}[\alpha]] = 2$ und $\Delta_F = -503$.

[1] Diese Identität erinnert sicher an die Norm-Identität $N(xy) = N(x)N(y)$, die wir im Zahlkörper $\mathbb{Q}(\sqrt{-1})$ mit $N(x + \sqrt{-1}y) = x^2 + y^2$ haben. In der Algebraische Zahlentheorie Vorlesung arbeiten wir nur mit kommutativen Ringen, aber die gesamte Theorie lässt sich in einem nichtkommutativen Setting verallgemeinern und hinter der Identität in (3) steckt dann in der Tat die Gleichung $N(xy) = N(x)N(y)$, wobei man statt mit dem Zahlkörper $\mathbb{Q}(\sqrt{-1})$ mit den nichtkommutativen Quaternionen arbeitet. Es existiert auch eine Zählformel wie in Aufgabe 5.3.7. Dies nur als Ausblick, was man noch alles tun kann...

3. Berechnen Sie das Minimalpolynom von

$$\frac{\alpha^2+\alpha}{2}$$

und folgern Sie, dass $\mathcal{O}_F \neq \mathbb{Z}[\alpha]$. Folgern Sie, dass

$$\mathcal{O}_F = \mathbb{Z}\left[\alpha, \frac{\alpha^2+\alpha}{2}\right].$$

4. Geben Sie die Norm $N(\alpha)$ an. Folgern Sie, dass die Primidealfaktorisierung von $\alpha\mathcal{O}_F$ nur Primideale $\mathfrak{p}$ über 2 enthalten kann (also mit $\mathfrak{p} \cap \mathbb{Z} = 2\mathbb{Z}$).

5. Bestimmen Sie das Minimalpolynom von $\alpha + 1$. Geben Sie die Norm von $\alpha + 1$ an.

6. Zeigen Sie, dass es ein Primideal $\mathfrak{p}_1$ mit $\mathcal{N}(\mathfrak{p}_1) = 2$ in $\mathcal{O}_F$ geben muss, was $(\alpha+1)\mathcal{O}_F$ teilt. Folgern Sie, dass dieses Primideal in der Faktorisierung von $2\mathcal{O}_F$ mit $e_i \geq 1$ auftreten muss. Berechnen Sie dieses e_i.

7. Folgern Sie, dass die Primidealfaktorisierung von $2\mathcal{O}_F$ entweder die Form $\mathfrak{p}_1\mathfrak{p}_2$ mit Idealnormen $2, 4$ haben muss, oder aber $\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$, alle mit Idealnorm 2.

8. Wir betrachten nur den hypothetischen Fall $2\mathcal{O}_F = \mathfrak{p}_1\mathfrak{p}_2$ mit $\mathcal{N}(\mathfrak{p}_2) = 4$: Zeigen Sie, dass

$$\alpha\mathcal{O}_F = \mathfrak{p}_1^{n_1}\mathfrak{p}_2^{n_2}$$

für irgendwelche $n_1, n_2 \in \mathbb{Z}_{\geq 0}$. Folgern Sie aus $\alpha + 1 \in \mathfrak{p}_1$, dass $\alpha \notin \mathfrak{p}_1$. Folgern Sie einen Widerspruch.

9. Folgern Sie, dass für jedes $\gamma \in \mathcal{O}_F$, wir die Teilbarkeit $2 \mid [\mathcal{O}_F : \mathbb{Z}[\gamma]]$ haben müssen.