LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN
MATHEMATISCHES INSTITUT

Prof. Dr. Werner Bley

Wintersemester 2019/20

Algebraische Zahlentheorie
Übungsblatt 7 Lösung

Aufgabe 1
Sei $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Finden Sie eine Untergruppe V von $\mathcal{O}_K^\times$ von endlichem Index.

Lösung: Seien $K_1 = \mathbb{Q}(\sqrt{2}), K_2 = \mathbb{Q}(\sqrt{6})$ und $K_3 = \mathbb{Q}(\sqrt{3})$ die quadratischen Teilkörper von K. Dann sind die normierten Fundamentaleinheiten gegeben durch

$$\varepsilon_1 = 1 + \sqrt{2}, \varepsilon_2 = 5 + 2\sqrt{6}, \varepsilon_3 = 2 + \sqrt{3}.$$

Wir wollen zeigen, dass $\langle \varepsilon_1, \varepsilon_2, \varepsilon_3 \rangle$ eine Untergruppe von $\mathcal{O}_K^\times$ von endlichem Index ist. Dazu reicht es zu zeigen, dass der Regulator $R(\varepsilon_1, \varepsilon_2, \varepsilon_3)$ ungleich 0 ist. Das kann man überprüfen, indem man mit reellen Approximationen arbeitet und berechnet

$$R(\varepsilon_1, \varepsilon_2, \varepsilon_3) = \det \begin{pmatrix} \log|1+\sqrt{2}| & \log|5+2\sqrt{6}| & \log|2+\sqrt{3}| \\ \log|1-\sqrt{2}| & \log|5-2\sqrt{6}| & \log|2+\sqrt{3}| \\ \log|1+\sqrt{2}| & \log|5-2\sqrt{6}| & \log|2-\sqrt{3}| \end{pmatrix} = 10.643594320761481875682734 78\ldots$$

Für den Regulator R_K erhält man übrigens $R_K = 2.660898580190370468920683 69\ldots$. Der Index ist also 4.

Aufgabe 2
Sei α die reelle Nullstelle von $x^3 - 2$ und $\zeta := \zeta_3$.

a) Zeigen Sie: $L = \mathbb{Q}(\alpha, \zeta)$ ist die galoissche Hülle von $\mathbb{Q}(\alpha)$.
Geben Sie die Galoisgruppe $G = \mathrm{Gal}(L/\mathbb{Q})$ in expliziter Form an.

b) Faktorisieren Sie $q = 2$ und $p = 3$, bestimmen Sie sämtliche Verzweigungs- und Trägheitsindizes, sowie die Zerlegung- und Trägheitsgruppen.

Lösung:

a) Sei α die reelle Nullstelle von $x^3 - 2$ und $\zeta := \zeta_3$. Zuerst stellen wir fest, dass $\mathbb{Q}(\alpha)/\mathbb{Q}$ keine galoissche Erweiterung ist, da die Erweiterung nicht normal ist. Adjungieren wir nun ζ erhalten wir den Zerfällungskörper (von $x^3 - 2$) $L := \mathbb{Q}(\alpha, \zeta)$, was natürlich auch sofort impliziert, dass wir die galoissche Hülle gefunden haben. Wir wollen nun noch die Galoisgruppe $G := \mathrm{Gal}(L/\mathbb{Q})$ explizit angeben:

$$G := \{\sigma_{ij} \mid 0 \le i \le 2, 1 \le j \le 2\}$$
$$\text{mit } \sigma_{ij}(\zeta) = \zeta^j \text{ und } \sigma_{ij|\mathbb{Q}(\alpha)}(\alpha) = \zeta^i \alpha.$$

b) Wir definieren $F := \mathbb{Q}(\alpha)$ und $K := \mathbb{Q}(\zeta)$. Wir sehen sofort ein, dass $F \cap K = \mathbb{Q}$, $FK = L$ und $K = \mathbb{Q}(\sqrt{-3})$ gilt. Wir wissen bereits aus alten Aufgaben, dass $2\mathcal{O}_F = (\alpha)^3$ und $3\mathcal{O}_F = (\alpha + 1)^3$ gilt.
Aus der Vorlesung wissen wir, dass $3\mathcal{O}_K = (\zeta - 1)^{\varphi(3)} = (\zeta - 1)^2$ und $2\mathcal{O}_K$ prim ist. Da Verzweigungsindizes und Trägheitsgrade multiplikativ in Körpertürmen sind sehen wir, dass rein aus kombinatorischen Gründen gelten muss, dass 3 in $\mathcal{O}_L$ voll verzweigt. Die Zerlegungsgruppe als auch die Verzweigungsgruppe stimmen also mit G überein.

Die 2 ist in $L/\mathbb{Q}$ ebenfalls unzerlegt, das eindeutige Primideal $\mathfrak{p}$ von $\mathcal{O}_K$ über der 2 ist in $\mathcal{O}_L$ voll verzweigt. Insgesamt ist also für die 2 der Restklassenkörpergrad gleich 2 und der Verzweigungsindex gleich 3. Die Zerlegungsgruppe ist gleich G und die Verzweigungsgruppe ist die eindeutig bestimmte Untergruppe der Ordnung $e = 3$, also gleich der Galoisgruppe von L/K.

Aufgabe 3
Es sei L/K eine Galoiserweiterung von Zahlkörpern mit Gruppe G. Sei $\mathfrak{p}$ ein Primideal in $\mathcal{O}_K$ und $\mathfrak{P} \mid \mathfrak{p}$ in L/K.

a) Für $\sigma \in G$ gelte
$$\sigma(\alpha) \equiv \alpha \mod \mathfrak{P}, \quad \forall \alpha \in \mathcal{O}_L.$$
Zeigen Sie: $\sigma \in G_{\mathfrak{P}}$. Insbesondere, ist also dann $\sigma \in I_{\mathfrak{P}}$.

Lösung: Es gilt:
$$\sigma \in G_{\mathfrak{P}} \iff \sigma\mathfrak{P} = \mathfrak{P} \iff (\forall \alpha \in \mathcal{O}_K \text{ gilt: } \sigma(\alpha) \in \mathfrak{P} \iff \alpha \in \mathfrak{P})$$
Letztere Aussage wird von $\sigma(\alpha) \equiv \alpha \mod \mathfrak{P}$ impliziert.

b) Seien $\sigma, \tau \in G$. Zeigen Sie:
$$\sigma(\alpha) \equiv \tau(\alpha) \mod \mathfrak{P}, \quad \forall \alpha \in \mathcal{O}_L \Leftrightarrow \sigma \equiv \tau \mod I_{\mathfrak{P}}.$$

Lösung: Im allgemeinen ist $I_{\mathfrak{P}}$ kein Normalteiler in G, die Aufgabe ist daher nicht wohl gestellt. Wir können zeigen:
$$\begin{aligned} & \sigma(\alpha) \equiv \tau(\alpha) \pmod{\mathfrak{P}}, \forall \alpha \\ \iff \quad & \sigma\tau^{-1}(\tau\alpha) \equiv \tau(\alpha) \pmod{\mathfrak{P}}, \forall \alpha \\ \iff \quad & \sigma\tau^{-1} \in I_{\mathfrak{P}} \\ \iff \quad & \sigma \in I_{\mathfrak{P}}\tau \end{aligned}$$

Aufgabe 4

a) Berechnen Sie die Klassenzahl von $\mathbb{Q}(\sqrt{10})$.

b) Bestimmen Sie die Gesamtheit der ganzzahligen Lösungen $(x, y) \in \mathbb{Z}^2$ von
$$x^2 - 10y^2 = p,$$
für $p = 31$ und $p = 37$.

Lösung:

a) Wir wollen zuerst die Klassenzahl von $K = \mathbb{Q}(\sqrt{10})$ berechnen. Dazu erinnern wir uns an die Formel für die Minkowski-Schranke:
$$M_K = \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n}\sqrt{|d_K|}.$$
In unserem Spezialfall haben wir $n = 2, s = 0$ und $d_K = 40$, also erhalten wir $M_K = \sqrt{10} < 4$ und somit hat jede Idealklasse einen Repräsentanten von Norm $1, 2$ oder 3. Es gilt $2\mathcal{O}_K = (2, \sqrt{10})^2$. Wenn nun $(2, \sqrt{10})$ die triviale Klasse wäre, dann müsste es ein Hauptideal (α) geben mit $\alpha = a + b\sqrt{10}, a, b \in \mathbb{Z}$. Das würde aber heißen, es gibt eine ganzzahlige Lösung der Gleichung $x^2 - 10y^2 = \pm 2$, was nicht möglich ist, da $x^2 \equiv 0, \pm 1 \bmod 5$ für $x \in \mathbb{Z}$. Also ist $[(2, \sqrt{10})]$ nicht die triviale Klasse und $2 \mid |\mathrm{Cl}_K|$.
Mit dem Polynomzerlegungsgesetz erhalten wir $3\mathcal{O}_K = \beta_1\beta_2$ mit $\beta_1 := (3, 2 + \sqrt{10})$ und $\beta_2 := (3, 4 + \sqrt{10})$. Wenn β_1 oder β_2 Hauptideale wären, dann hätte $x^2 - 10y^2 = \pm 3$ eine Lösung. Wir sehen aber, dass diese Gleichung keine Lösung hat, wenn wir beide Seiten wieder modulo 5 nehmen.
Sei nun $\gamma := \frac{4+\sqrt{10}}{2+\sqrt{10}} = \frac{1}{3}(1 + \sqrt{10})$. Wir bekommen
$$\begin{aligned} (3, 2 + \sqrt{10})(\gamma) &= (3\gamma, 4 + \sqrt{10}) \\ &= (1 + \sqrt{10}, 4 + \sqrt{10}), \\ &= (3, 4 + \sqrt{10}) \end{aligned}$$

also gilt $[\beta_1] = [\beta_2]$. So ist also jedes Element in Cl_K äquivalent zu einem der folgenden Elemente

$$(1), (2, \sqrt{10}) \text{ und } (3, 2+\sqrt{10}).$$

Das heißt aber $|\mathrm{Cl}_K| \leq 3$ und wir hatten bereits gezeigt $2 \mid |\mathrm{Cl}_K|$, also kann nur $h_K = |\mathrm{Cl}_K| = 2$ gelten.

b) Sei $\alpha = a + b\sqrt{10} \in \mathcal{O}_K = \mathbb{Z}[\sqrt{10}]$. Dann gilt offensichtlich $N(\alpha) = p$, genau dann wenn $a^2 - 10b^2 = p$.
Wir wollen zuerst einsehen, dass, unter der Bedingung $p \nmid d$, $N(\alpha) = p$ genau dann lösbar ist, wenn p zerlegt, i.e., $p\mathcal{O}_K = \mathfrak{p}\bar{\mathfrak{p}}$ und $[\mathfrak{p}]$ die triviale Klasse ist. Diese Äquivalenz folgt (da wir $p \nmid d$ voraussetzen) sofort aus den Definitionen und aus $N(\alpha\mathcal{O}_K) = |N(\alpha)|$.

Sei nun $p = 31$. Mit dem Polynomzerlegungsgesetz und etwas Rechnen erhalten wir $31\mathcal{O}_K = (11 + 3\sqrt{10})(11 - 3\sqrt{10})$. Hier ist also $p = 31$ zerlegt und die Primideale über p sind Hauptideale. Es gibt also eine Lösung.

Eine Fundamentaleinheit $3 + \sqrt{10}$ (mit Norm -1). Aus dem Dirichletschen Einheitensatz erhalten wir, dass wir durch $\pm(3+\sqrt{10})^{2m}$ alle Einheiten mit Norm 1 darstellen können. Also sind alle möglichen Lösungen von der Form $\alpha = \pm(3+\sqrt{10})^{2m}(11 \pm 3\sqrt{10})$ mit $m \in \mathbb{Z}$.
Für $p = 37$ können wir schnell feststellen, dass es keine ganzzahligen Lösungen gibt, in dem wir die Gleichung modulo 5 nehmen. Damit ist die Aufgabe gelöst.

Bemerkung: Wegen $\left(\frac{10}{37}\right) = 1$ ist 37 zerelgt, d.h. $37\mathcal{O}_K = \mathfrak{p}\bar{\mathfrak{p}}$. Wir haben also gezeigt, dass die Klasse von $\mathfrak{p}$ nicht trivial ist.

Aufgabe 5
Sei $n \in \mathbb{N}$ und C eine zyklische Gruppe der Ordnung n.
Zeigen Sie, dass es eine endliche galoissche Erweiterung $L/\mathbb{Q}$ gibt mit $\mathrm{Gal}(L/\mathbb{Q}) \cong C$.
Hinweis: Benutzen Sie Kreiskörpertheorie und den Dirichletschen Primzahlsatz.

Lösung: Der Dirichletsche Primzahlsatz liefert unendlich viele Primzahlen p mit $p \equiv 1 \pmod{n}$. Man nehme solch ein p. Wir wissen, dass $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ zyklisch von der Ordnung $p-1$ ist. Wegen $n \mid (p-1)$ gibt es eine Untergruppe H von $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ vom Index n. Dann ist also $\mathbb{Q}(\zeta_p)^H/\mathbb{Q}$ zyklisch von der Ordnung n.