Prof. Dr. Benjamin Klopsch
Dr. Philip Möller
Wintersemester 2024–25

Heinrich Heine Universität Düsseldorf

Zahlentheorie I – Blatt 5

Vorstellung/Abgabe der Lösungen in der Übungsstunde am 11.11.2024, ab 14.30 Uhr

Bitte reichen Sie Lösungen zu den Aufgaben 5.1 und 5.3 ein; weitere Informationen auf

`http://reh.math.uni-duesseldorf.de/~internet/ZahlenI_WS2425/`.

Aufgabe 5.1 (4 Punkte)

Sei p eine ungerade Primzahl. Seien $F = \mathbb{F}_p$ der Körper mit p Elementen, und $E = \mathbb{F}_{p^2}$ ein quadratischer Erweiterungskörper von F.[1]

(a) Bekanntlich ist die multiplikative Gruppe $F^\times$ zyklisch. Verwenden Sie diese Tatsache, um zu zeigen:

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2},$$

d. h., -1 ist ein quadratischer Rest modulo p genau dann, wenn $p \equiv_4 1$ ist.

(b) Bekanntlich ist auch die multiplikative Gruppe $E^\times$ zyklisch. Erläutern Sie: E enthält eine primitive 8te Einheitswurzel ζ und diese erfüllt:

$$(\zeta + \zeta^7)^2 = 2 \qquad \text{sowie} \qquad \zeta + \zeta^3 + \zeta^5 + \zeta^7 = 0.$$

(c) Bekanntlich erzeugt der Frobeniusautomorphismus $E \to E$, $x \to x^p$ die Galoisgruppe $\mathrm{Gal}(E \mid F)$. Verwenden Sie diese Tatsache sowie die Ergebnisse aus (b), um zu zeigen:

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8},$$

d. h., 2 ist ein quadratischer Rest modulo p genau dann, wenn $p \equiv_8 1, 7$ ist.

Bemerkung. Die Aussagen zu den Legendre-Symbolen in (a) und (c) werden für gewöhnlich als „Ergänzungen zum Quadratischen Reziprozitätsgesetz“ bezeichnet.

Aufgabe 5.2

Die Schlacht von Hastings (14.10.1066):[2]

> Harolds Mannen standen nach alter Gewohnheit dichtgedrängt in 13 gleichgroßen Quadraten aufgestellt, und wehe dem Normannen, der es wagte, in eine solche Phalanx einbrechen zu wollen. ... Als aber Harold selbst auf dem Schlachtfeld erschien, formten die Sachsen ein einziges gewaltiges Quadrat mit ihrem König an der Spitze und stürmten mit den Schlachtrufen „Ut!“, „Olicrosse!“, „Godemite!“ vorwärts. ...
>
> (vgl. „Carmen de Hastingae Proelio“ von Guy, Bischof von Amiens)

Frage: Wie groß soll die Armee Harolds II. gewesen sein?

Bitte wenden!

[1] Daß solch ein quadratischer Erweiterungskörper stets existiert und bis auf Isomorphie eindeutig ist, läßt sich elementar einsehen – wie?

[2] Aufgabe entnommen aus: J. Neukirch, Algebraische Zahlentheorie, 1992; dort unter dem Verweis „Mitgeteilt von W.-D. Geyer“.

Aufgabe 5.3 (4 Punkte)

Sei p eine ungerade Primzahl, und sei $K \leq \overline{\mathbb{Q}}$ der Zerfällungskörper für $X^p - 2$ über $\mathbb{Q}$, also der kleinste Teilkörper von $\overline{\mathbb{Q}}$, über dem $X^p - 2$ in Linearfaktoren zerfällt.

(a) Erläutern bzw. zeigen Sie: $K\,|\,\mathbb{Q}$ ist galoissch vom Grad $[K : \mathbb{Q}] = p(p-1)$, und die Galoisgruppe $\mathrm{Gal}(K\,|\,\mathbb{Q})$ ist isomorph zu der affinen Gruppe[3]

$$\mathrm{Aff}(1,p) = \left\{ \left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right) \mid a, b \in \mathbb{F}_p \text{ mit } a \neq 0 \right\},$$

bestehend aus den (umkehrbaren) affinen Transformationen eines eindimensionalen Vektorraums über $\mathbb{F}_p$.

Hinweis. Beschreiben Sie K als $K = \mathbb{Q}(\alpha, \zeta)$ für geeignete Elemente α, ζ und erfassen Sie Automorphismen von K durch ihre Wirkung auf den zu α bzw. ζ konjugierten Elementen.

(b) Bestimmen Sie konkret ein primitives Element für die Erweiterung $K\,|\,\mathbb{Q}$, also $\beta \in K$ mit $K = \mathbb{Q}(\beta)$.

(c) Sei nun konkret $p = 5$. Geben Sie explizit alle Untergruppen von $\mathrm{Gal}(K\,|\,\mathbb{Q}) \cong \mathrm{Aff}(1,5)$ und die zughörigen Zwischenkörper k von $K\,|\,\mathbb{Q}$ an, wobei Sie jeweils ein primitives Element für $k\,|\,\mathbb{Q}$ bestimmen. Stellen Sie beide Verbände durch geeignet beschriftete Hassediagramme dar, aus denen dann auch die jeweiligen Gruppenindizes bzw. Erweiterungsgrade erkennbar sind. Finden Sie weiter heraus, welche der Zwischenkörper k galoissch über $\mathbb{Q}$ sind.

Hinweis. Schreiben Sie die affine Gruppe als $\mathrm{Aff}(1,5) = \langle s, t \mid s^4 = t^5 = 1,\ sts^{-1} = t^2 \rangle$, wobei $s = \left(\begin{smallmatrix} 2 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ und $t = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ gesetzt sind. Jedes Element von $\mathrm{Aff}(1,5)$ läßt sich dann eindeutig schreiben als $t^i s^j$ mit $0 \leq i \leq 4$ und $0 \leq j \leq 3$; überlegen Sie sich, welche Ordnung die Elemente jeweils haben. Die Untergruppen lassen sich jeweils durch Angabe eines oder zweier erzeugender Elemente beschreiben – wieso? (Zur Kontrolle: Es gibt insgesamt 14 Untergruppen.) Wenden Sie alsdann den Hauptsatz der galoisschen Theorie an.

Aufgabe 5.4

Der Abstand zweier ganzer Zahlen $x, y \in \mathbb{Z}$ sei definiert als

$$d(x,y) = \begin{cases} m^{-1} & \text{mit } m = \min\{n \in \mathbb{N} \mid x \not\equiv_n y\}, \text{ falls } x \neq y, \\ 0 & \text{falls } x = y. \end{cases}$$

(a) Überprüfen Sie, daß $\mathbb{Z}$ mittels dieser Abstandsfunktion einen metrischen Raum bildet, und beachten Sie, daß der Abstand translationsinvariant (unter Addition mit einer Konstanten) ist. Die zugehörige Topologie heißt *pro-endliche Topologie* auf $\mathbb{Z}$.

(b) Zeigen Sie: Die offenen Teilmengen von $\mathbb{Z}$ bzgl. der pro-endlichen Topologie sind gerade die Vereinigungen von Nebenklassen der Form $a + b\mathbb{Z}$ für $a, b \in \mathbb{Z}$ mit $b \neq 0$. Insbesondere ist in dieser Topologie jede nicht-leere offene Teilmenge von $\mathbb{Z}$ unendlich.

(c) Folgern Sie aus der Gleichung $\mathbb{Z} \smallsetminus \{1, -1\} = \bigcup\{p\mathbb{Z} \mid p \text{ prim}\}$, daß es unendlich viele Primzahlen gibt.

Bemerkung. Die Addition auf $\mathbb{Z}$ und die zugehörige Inversenabbildung sind stetig bzgl. der pro-endlichen Topologie. Durch die (eindeutige) Fortsetzung dieser stetigen Abbildungen erhält die Vervollständigung $\widehat{\mathbb{Z}}$ von $\mathbb{Z}$ die Struktur einer abelschen kompakten topologischen Gruppe. Für jeden endlichen Körper $\mathbb{F}_q$ ist die absolute Galoisgruppe von $\mathbb{F}_q$, ausgestattet mit der Krulltopologie, isomorph zu der Gruppe $\widehat{\mathbb{Z}}$.

[3] In Hinblick auf die bereits behandelten Möbiustransformationen paßt es hier gut, obere Dreiecksmatrizen zu wählen. Für die Bearbeitung der Aufgabe ist es dann günstig und pragmatisch, Körperautomorphismen ausnahmsweise von links wirken zu lassen.