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

Zahlentheorie I – Blatt 10

Vorstellung/Abgabe der Lösungen in der Übungsstunde am 16.12.2024, ab 14.30 Uhr

Bitte reichen Sie Lösungen zu den Aufgaben 10.1 und 10.2 ein; weitere Informationen auf

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

Aufgabe 10.1 (4 Punkte)

In Abschnitt 4 der Vorlesung wird für $m, n \in \mathbb{N}$ die Anzahl $S(m,n)$ aller Untergruppen der abelschen Gruppe $\mathbb{Z}^n/m\mathbb{Z}^n$ nach oben "großzügig" mit m^{n^2} abgeschätzt.

(a) Erläutern Sie, wie sich die Abschätzung $S(m,n) \leq m^{n^2}$ ergibt.

(b) Sei $m = \prod_{i=1}^{r} p_i^{e_i}$ die Primfaktorzerlegung von m, wobei $p_1, \ldots, p_r$ die verschiedenen Primteiler von m bezeichnen. Erklären Sie, wieso $S(m,n) = \prod_{i=1}^{r} S(p_i^{e_i}, n)$ gilt.

(c) Zeigen Sie: Für $n \in \mathbb{N}_0$ gilt im Polynomring $\mathbb{Z}[X,Y]$ die Identität

$$\prod_{d=0}^{n-1}(1+X^dY) = \sum_{d=0}^{n} X^{d(d-1)/2} \binom{n}{d}_X Y^d,$$

wobei die auftretenden *Gaußschen Binomialkoeffizienten*[1] direkt wie folgt beschrieben werden können:

$$\binom{n}{d}_X = \frac{(1-X^n)(1-X^{n-1})\cdots(1-X^{n-d+1})}{(1-X^d)(1-X^{d-1})\cdots(1-X)} \in \mathbb{Z}[X] \qquad (0 \leq d \leq n).$$

Insbesondere ist $\binom{n}{d}_X$ stets normiert, besitzt ausschließlich nicht-negative Koeffizienten und hat den Grad $(n-d)d$.

Erläutern sie weiter: Für jede Primzahlpotenz q und $n \geq d \geq 0$ liefert $\binom{n}{d}_q$ die Anzahl der d-dimensionalen Teilvektorräume eines n-dimensionalen Vektorraums über $\mathbb{F}_q$.

(d) Zeigen Sie: In dem Spezialfall, daß $m = p^e$ eine Primzahlpotenz und $n = 3$ ist, gilt die explizite kombinatorische Formel

$$S(p^e,3) = S(p^e,3,0) + S(p^e,3,1) + S(p^e,3,2)$$

mit

$$S(p^e,3,0) = \sum_{0\leq e_1\leq e} p^0 = e+1,$$

$$S(p^e,3,1) = \sum_{\substack{0<d_1<3\\ 0\leq e_1<e_2\leq e}} \binom{3}{d_1}_{p^{-1}} p^{d_1(3-d_1)(e_2-e_1)} = 2\cdot\binom{3}{1}_{p^{-1}} p^{2e_2-2e_1},$$

$$S(p^e,3,2) = \sum_{\substack{0<d_1<d_2<3\\ 0\leq e_1<e_2<e_3\leq e}} \binom{3}{d_2}_{p^{-1}}\binom{d_2}{d_1}_{p^{-1}} p^{d_1(d_2-d_1)(e_2-e_1)+d_1(3-d_2)(e_3-e_1)+(d_2-d_1)(3-d_2)(e_3-e_2)}$$

$$= \sum_{0\leq e_1<e_2<e_3\leq e} \binom{3}{2}_{p^{-1}}\binom{2}{1}_{p^{-1}} p^{2e_3-2e_1}.$$

Hinweis. Bestimmen Sie die Anzahl der Untergruppen mit Faktorgruppe isomorph zu $(\mathbb{Z}/p^{e_1}\mathbb{Z}) \oplus (\mathbb{Z}/p^{e_2}\mathbb{Z}) \oplus (\mathbb{Z}/p^{e_3}\mathbb{Z})$ und sortieren Sie nach $|\{e_1,e_2,e_3\}|$.

Bitte wenden!

[1] Der gewöhnliche Binomialkoeffizient $\binom{n}{d}$ ergibt sich, indem $\binom{n}{d}_X$ an der Stelle $X = 1$ ausgewertet wird. In diesem Sinne handelt es sich um eine Verallgemeinerung des klassischen Begriffsapparats.

Aufgabe 10.2 (4 Punkte)

Sei $k = \mathbb{Q}(\vartheta)$ für $\vartheta \in \mathbb{C}$ mit $\vartheta^3 - \vartheta^2 - 2\vartheta - 8 = 0$, und sei $\tilde{\vartheta} = 4\vartheta^{-1}$.
Verifizieren Sie schrittweise die nachfolgenden Behauptungen.

(a) Das Minimalpolynom von ϑ über $\mathbb{Q}$ ist $X^3 - X^2 - 2X - 8$. Folglich ist k ein kubischer Zahlkörper, und es gilt $\vartheta \in \mathfrak{o}_k$.

(b) Es gilt $\tilde{\vartheta}^3 + \tilde{\vartheta}^2 + 2\tilde{\vartheta} - 8 = 0$ und folglich $\tilde{\vartheta} \in \mathfrak{o}_k$.

(c) Es gelten $\vartheta\tilde{\vartheta} = 4$, $\vartheta^2 = 2 + \vartheta + 2\tilde{\vartheta}$ und $\tilde{\vartheta}^2 = -2 + 2\vartheta - \tilde{\vartheta}$. Folglich ist $\mathbb{Z} + \mathbb{Z}\vartheta + \mathbb{Z}\tilde{\vartheta}$ ein Teilring von $\mathfrak{o}_k$.

(d) Die Elemente $1, \vartheta, \tilde{\vartheta}$ bilden eine Ganzheitsbasis für k. Also ist $\mathfrak{o}_k = \mathbb{Z} + \mathbb{Z}\vartheta + \mathbb{Z}\tilde{\vartheta}$.

Hinweis. Berechnen Sie die Diskriminante $d_{k|\mathbb{Q}}(1, \vartheta, \tilde{\vartheta})$.

(e) Für jedes $\alpha \in \mathfrak{o}_k$ ist $\mathbb{Z}[\alpha] \subsetneq \mathfrak{o}_k$.

Hinweis. Schreiben Sie $\alpha = a + b\vartheta + c\tilde{\vartheta}$ mit $a, b, c \in \mathbb{Z}$, und reduzieren Sie das zu lösende Problem auf den Fall $a = 0$, aber $(b, c) \neq (0, 0)$. Bestimmen Sie die ganzzahlige Matrix $A \in \mathrm{Mat}_3(\mathbb{Z})$ mit $(1, \alpha, \alpha^2) = (1, \vartheta, \tilde{\vartheta})A^{\mathrm{tr}}$, um anschließend einzusehen, daß $|\mathfrak{o}_k : \mathbb{Z}[\alpha]|$ stets gerade (und damit ungleich 1) ist.

Bemerkung. Das Beispiel geht auf Dedekind (1871) zurück. Es gibt zahlreiche Zahlkörper, die keine Ganzheitsbasis der Form $1, \alpha, \ldots, \alpha^{n-1}$ besitzen.