

ÜBUNG 4

Ein etwas anderes Übungsblatt

Dieses Übungsblatt unterscheidet sich von den bisherigen. Es enthält keine klassischen Aufgaben im engeren Sinne, sondern lädt Sie ein, einen zusammenhängenden mathematischen Text zu lesen – und zwar so, wie man mathematische Texte lesen sollte: langsam, aufmerksam und mit Stift und Papier in der Hand.

Der Text entwickelt eine kleine, in sich geschlossene Theorie: die Theorie der endlichen affinen Ebenen. Sie entsteht Schritt für Schritt innerhalb unseres axiomatischen Aufbaus, und Sie werden sehen, wie aus wenigen Grundbegriffen und Axiomen ein überraschend reichhaltiges Gebäude wächst. Vieles davon wird Ihnen bekannt vorkommen, manches erscheint im neuen Gewand, und einiges ist tatsächlich neu.

Mathematische Texte zu lesen ist eine Kunst, die man lernen muss – und die anfangs anstrengend sein kann. Es ist völlig normal, nach einer einzigen Zeile innezuhalten, das Blatt zur Seite zu legen und sich zu fragen: Was will mir der Autor hier eigentlich sagen? Was bedeutet dieses Symbol? Warum steht hier *sei* und nicht *ist*? Geben Sie sich die Zeit dafür. Nehmen Sie sich Bleistift und Papier, zeichnen Sie Skizzen, probieren Sie Beispiele aus, identifizieren Sie jeden noch so unscheinbaren Buchstaben und versuchen Sie, einen Zusammenhang zwischen all diesen herzustellen. Genau so arbeiten Mathematikerinnen und Mathematiker, wenn sie einen neuen Text erschließen.

Zwischendurch werden Ihnen im Text kleine Lücken begegnen: Auslassungspunkte „...“, Fragezeichen (?) und kurze Arbeitsaufträge. Diese sind bewusst gesetzt und laden Sie ein, selbst aktiv zu werden – eine Begründung zu vervollständigen, ein Argument nachzuvollziehen oder ein kleines Beispiel zu finden. Bearbeiten Sie diese Stellen, denn gerade in diesen Momenten findet das eigentliche Lernen statt.

Wir werden am Montag in der Vorlesung um 9 Uhr ausführlich über dieses Blatt sprechen, Fragen klären und die Ergebnisse gemeinsam besprechen. Bis dahin wünschen wir Ihnen viel Freude – und vielleicht auch die eine oder andere Überraschung – beim Lesen des Textes.

Wir beginnen - wie könnte es anders sein - mit einer

Definition 0.1. Sei $(\mathcal{P}, \mathcal{G})$ eine Inzidenzstruktur, $A \in \mathcal{P}$ und $a \in \mathcal{G}$. Dann heißt $G_A := \{g \mid g \in \mathcal{G}, A \in g\}$ das Sternbüschel von A , und $G_a := \{g \mid g \in \mathcal{G}, g \parallel a\}$ das Parallelbüschel von a .

Man überprüfe die Aussage des folgenden Satzes im Minimal-Modell und analysiere ihn anschließend.

Satz 0.1. Sei $(\mathcal{P}, \mathcal{G})$ eine endliche Inzidenzstruktur. Dann gilt

$$\sum_{A \in \mathcal{P}} |G_A| = \sum_{g \in \mathcal{G}} |g|.$$

Beweis 0.1. Die Inzidenzrelation I der Inzidenzstruktur $(\mathcal{P}, \mathcal{G})$ besteht aus allen Paaren (A, g) mit $A \in \mathcal{P}, g \in \mathcal{G}, A \in g$. Zählt man diese Menge I nach der linken Kompetente ab, so erhält man $|I| = \sum_{A \in \mathcal{P}} |G_A|$. Zählt man entsprechend nach der rechten Kompetente ab, so erhält man $|I| = \sum_{g \in \mathcal{G}} |g|$. Damit folgt die Behauptung.

Die Aussagen des folgenden Satzes über die Anzahlen einer endlichen affinen Ebene sind tw. bereits für den Fall $n = 2$ bewiesen (oder werden es in der nächsten Vorlesung), man analysiere den nun folgenden Beweis und vervollständige ihn.

Satz 0.2 (Anzahlen in affinen Ebenen). Sei $(\mathcal{P}, \mathcal{G})$ eine endliche affine Ebene der Ordnung $n \in \mathbb{N}$. Dann gilt

- a) $|G_a| = n$ für alle Geraden a .
- b) $|G_A| = n + 1$ für alle Punkte A .
- c) $|\mathcal{P}| = n^2$.
- d) $|\mathcal{G}| = n \cdot (n + 1) = n^2 + n$.
- e) Es gibt genau $n + 1$ -viele Parallelbüschel.

Wir beweisen nun obigen Anzahl-Satz:

Beweis 0.2. a) Sei a eine Gerade. Man wählt eine Gerade s mit $s \not\parallel a$. Die Abbildung $G_a \rightarrow s$ mit $g \mapsto X \in g \cap s$ ist offenbar eine Bijektion. Also gilt $|G_a| = |\dots| = n$.

b) Sei A ein Punkt. Man wählt eine Gerade s mit $A \notin s$. Sei a die Parallele zu s durch den Punkt A . Die Abbildung $s \rightarrow G_A \setminus \{a\}$ mit $X \mapsto \overline{XA}$ ist offenbar eine Bijektion. Also gilt $n = |s| = |\dots| = |G_A| - 1$, also $|G_A| = n + 1$.

c) Man wählt eine Gerade a . Offenbar ist G_a eine Klasseneinteilung von \mathcal{P} . Also gilt

$$|\mathcal{P}| = \sum_{g \in G_a} |g| = \sum_{g \in G_a} n = |G_a| \cdot n \stackrel{\text{Teil a)}}{=} \dots \cdot n = n^2.$$

d) Es gilt:

$$|\mathcal{G}| \cdot n = \sum_{g \in \mathcal{G}} |g| \stackrel{\text{Satz 0.1)}}{=} \sum_{A \in \mathcal{P}} |\dots| \stackrel{\text{Teil b)}}{=} \sum_{A \in \mathcal{P}} \dots = |\dots| \cdot (n+1) \stackrel{\text{Teil c)}}{=} \dots \cdot (n+1).$$

Es folgt $|\mathcal{G}| = n \cdot (n+1) = n^2 + n$.

e) Offenbar ist die Menge der Parallelenbüschel eine Klasseneinteilung von \mathcal{G} . Mit den Teilen a) und d) folgt die Behauptung, also es gibt genau $n+1$ -viele Parallelenbüschel.

Mit den obigen zum Teil kombinatorischen Überlegungen kann man nun das folgende Kriterium für endliche affine Ebene beweisen, das sollen Sie nun auch tun, wobei eine Reihe von Hilfestellungen gegeben werden, schauen Sie selbst ...

Satz 0.3 (Kriterium für endliche affine Ebenen). Sei $n \in \mathbb{N}_{\geq 2}$ und $(\mathcal{P}, \mathcal{G})$ eine endliche Inzidenzstruktur mit folgenden Eigenschaften:

- i) $|\mathcal{P}| = n^2$.
- ii) $|\mathcal{G}| = n \cdot (n+1) = n^2 + n$.
- iii) $|g| = n$ für alle Geraden g .
- iv) In $(\mathcal{P}, \mathcal{G})$ gilt die Eindeutigkeit der Verbindungsgeraden. Dann ist $(\mathcal{P}, \mathcal{G})$ eine affine Ebene der Ordnung n .

Beweis 0.3. Den Beweis strukturieren wir in 7 Schritten.

1. Wir zeigen: In $(\mathcal{P}, \mathcal{G})$ gilt das Axiom (D).

Beweis. Wegen der Voraussetzung ... findet man eine Gerade g . Wegen Voraussetzung ... liegen auf g (mindestens) zwei verschiedene Punkte A, B . Wegen ... und ... gilt die Ungleichung $|g| = n < n^2 = |\mathcal{P}|$, also gilt, dass g eine echte Teilmenge von \mathcal{P} ist, also $g \subset \mathcal{P}$. Also findet man einen Punkt $C \in \mathcal{P}$ mit $C \notin g$. Wegen ... ist ABC ein echtes Dreieck.

Wir definieren für jeden Punkt $P(A) := \bigcup_{g \in G_A} g$.

2. Wie zeigen: Für alle Punkte A gilt: $|P(A)| - 1 = |G_A| \cdot (n-1)$.

Beweis. Sei A ein Punkt. Offenbar ist die Menge $\{g \setminus \{A\} \mid g \in G_A\}$ eine Klasseneinteilung von $P(A) \setminus \{A\}$, das gilt wegen Voraussetzung Also gilt die Gleichung

$$|P(A)| - 1 = |P(A) \setminus \{A\}| = \sum_{g \in G_A} |g \setminus \{A\}| = |G_A| \cdot (n-1).$$

3. Für alle Punkte A gilt: $|G_A| \leq n + 1$.

Beweis. Sei A ein Punkt, dann gilt

$$|G_A| \cdot (n - 1) \stackrel{2.}{=} \dots \leq |\mathcal{P}| - 1 \stackrel{i)}{=} \dots$$

Also folgt mit Division der Ungleichung mit $(n - 1)$ die Behauptung $|G_A| \leq n + 1$.

4. Es gilt $\sum_{A \in \mathcal{P}} |G_A| = \sum_{A \in \mathcal{P}} (n + 1)$.

Beweis.

$$n^2 \cdot (n + 1) \stackrel{?)}{=} |\mathcal{G}| \cdot n \stackrel{?)}{=} \sum_{g \in \mathcal{G}} |g| \stackrel{\text{Satz } ?}{=} \sum_{A \in \mathcal{P}} |G_A| \stackrel{?)}{\leq} \sum_{A \in \mathcal{P}} (n + 1) \stackrel{?)}{=} n^2 \cdot (n + 1),$$

also gilt die Behauptung (warum?).

Aus ?. und ?. folgt nun unmittelbar

5. Für alle Punkte A gilt: $|G_A| = n + 1$.

6. In $(\mathcal{P}, \mathcal{G})$ gilt das Axiom (V).

Beweis. Wegen ?) ist nur die ... zu beweisen.

Dazu reicht es zu zeigen, dass für jeden Punkt A gilt: $P(A) = \mathcal{P}$, warum?

Sei also A ein Punkt. Dann gilt:

$$|P(A)| - 1 \stackrel{?)}{=} |G_A| \cdot (n - 1) \stackrel{?)}{=} (n + 1) \cdot (n - 1) = n^2 - 1 \stackrel{?)}{=} |\mathcal{P}| - 1.$$

7. Es bleibt der Nachweis für das Parallelenaxiom (P).

Beweis. Sei g eine Gerade und A ein Punkt mit $A \notin g$. Wegen 6. ist die Abbildung $g \rightarrow G_A$ mit $X \mapsto \overline{XA}$ injektiv. Also wird wegen iii) und 5. genau ein Element aus G_A bei dieser Abbildung nicht getroffen, d.h. es gibt genau eine Gerade durch A , die g nicht schneidet.

Aus 1., 6. und 7. folgt die Behauptung.

Für die Konstruktion endlicher affiner Ebenen geben wir ein etwas Eigentümliches kombinatorisches Verfahren an, das nur einen geringfügigen Aufwand benötigt, die wir schon in einer vorherigen Übung kennengelernt haben. Vorweg eine kleine Definition und Bemerkung, die Sie beweisen sollen, also

Definition 0.2. Sei R eine endliche abelsche Gruppe (additiv geschrieben, vgl. Vorlesung aus dem zweiten Semester oder aber auch hier¹) und \mathcal{D} eine Teilmenge von R . \mathcal{D} heißt eine Differenzenmenge von R , wenn die Abbildung δ mit

$$\delta : \mathcal{D} \times \mathcal{D} \setminus id_{\mathcal{D}} \rightarrow R \setminus \{0\}, (x, y) \mapsto \delta((x, y)) := x - y$$

eine Bijektion ist.

Man - also Sie - überlege sich nun: In dieser Situation gilt offenbar für $n := |\mathcal{D}| - 1$ die Gleichung $|R| = n^2 + n + 1$.

Es folgt eine weitere Definition, nämlich

Definition 0.3. Sei R eine endliche abelsche Gruppe mit $|R| \geq 4$ und \mathcal{D} eine Differenzenmenge von R . Für jedes $A \in R \setminus \{0\}$ sei $g(A) := (\mathcal{D} + A) \setminus \mathcal{D}$, wobei wieder $\mathcal{D} + A := \{X + A | X \in \mathcal{D}\}$ gilt. Es sei weiterhin $G := \{g(A) | A \in R \setminus \{0\}\}$.

Man beweise nun den folgenden Satz mit dem Satz 0.3, dem Kriterium für endliche affine Ebenen, er gestattet und liefert die Konstruktion endlicher affiner Ebenen, zurecht trägt er auch den Namen. Der Beweis ist wieder gut strukturiert, Sie müssen lediglich die Lücken und Fragezeichen klären.

Satz 0.4 (Konstruktion endlicher affiner Ebenen). *Gemäß obiger Definition der Mengen R , \mathcal{D} und G ist $(R \setminus \mathcal{D}, G)$ eine affine Ebene der Ordnung $n := |\mathcal{D}| - 1$.*

Beweis 0.4. *Um zu beweisen, dass $(R \setminus \mathcal{D}, G)$ eine affine Ebene der gegebenen Ordnung ist, wollen wir (ehrlicher: sollen Sie) die vier Bedingungen des Satzes 0.3 beweisen. Legen Sie los. Wir beginnen*

Wegen $n^2 + n + 1 = |R| \geq 4$ gilt $n \geq 2$, das haben wir schon mal.

Offenbar (wirklich ?) gilt:

$$(1) |R \setminus \mathcal{D}| = n^2$$

Direkt aus der Definition der ... folgt:

$$(2) \text{ Für alle } A \in R \setminus \{0\} \text{ gilt: } |(\mathcal{D} + A) \cap \mathcal{D}| = 1.$$

Direkt daraus folgt:

¹Sei G eine Menge. Jedem Paar $(a, b) \in G \times G$ sei genau ein Element $a + b \in G$ zugeordnet. Das Paar $(G, +)$ heißt "abelsche Gruppe", wenn die Verknüpfung $+$ die folgenden Gesetze erfüllt:

- a) Assoziativgesetz: Für alle $a, b, c \in G$ gilt: $a + (b + c) = (a + b) + c$.
- b) Kommutativgesetz: Für alle $a, b \in G$ gilt: $a + b = b + a$.
- c) Neutrales Element: Es gibt ein Element $0 \in G$, so dass für alle $a \in G$ gilt: $a + 0 = a$.
- d) Inverses Element: Zu jedem $a \in G$ gibt es ein $a^{-1} \in G$ mit $a + a^{-1} = 0$.

(3) Für alle $A, B \in R$ mit $A \neq B$ gilt: $|(\mathcal{D} + A) \cap (\mathcal{D} + B)| = 1$.

(4) Für alle $A \in R \setminus \{0\}$ gilt: $|g(A)| = n$.

Beweis: Nach Definition gilt $g(A) = \dots$. Daraus folgt mit Teil (2) $|g(A)| = \dots = n$.

(5) Für alle $A, B \in R \setminus \{0\}$ mit $A \neq B$ gilt: $|g(A) \cap g(B)| \leq 1$.

Beweis: ... bitte selbst mit Teil (3).

(6) Es gilt $|G| = n \cdot (n + 1)$.

Beweis: Es genügt zu zeigen, dass die surjektive Abbildung

$$R \setminus \{0\} \rightarrow G, A \mapsto g(A)$$

injektiv in G ist. ... bitte selbst mit Teil (4) und Teil (5)!

Nun sind tatsächlich alle Voraussetzungen des Kriteriums 0.3 erfüllt, man glaubt es kaum, aber es stimmt, denn

Teil i) gilt wegen ?,

Teil ii) gilt wegen ?,

Teil iii) gilt wegen ? und

Teil iv) gilt wegen ?.

wobei die $?$ $\in \{(1), (2), (3), (4), (5), (6)\}$.

Also folgt die Behauptung, nämlich $(R \setminus \mathcal{D}, G)$ ist eine affine Ebene der Ordnung $n := |\mathcal{D}| - 1$.

Haben Sie noch Lust? Ist schon sehr anstrengend, oder? Wir wollen nun die Früchte unserer Arbeit ernten, Sie können aber auch - bei zunächst oberflächlicher Lektüre des Vorangegangenen - gleich hier loslegen, und dann im zweiten Anlauf eine Rückschau auf die Theorieentwicklung halten.

Also: Für die Konstruktion einer affinen Ebene gibt man sich eine Ordnung n vor. Die kleinstmögliche Ordnung ist 2, dies führt bei uns zum Minimalmodell aus 4 Punkten und 6 Geraden. Welche Zahlen kommen als Ordnung in Frage? Man weiß, d.h. man kann beweisen, dass alle Primzahlpotenzen zu affinen Ebenen führen, das sind schon ganz schön viele. Bei den anderen Zahlen zeigt die bisherige Erfahrung (das sind natürlich keine Beweise), dass sie als Ordnung nicht in Frage kommen.

Die ersten Zahlen, die als Ordnungen nicht in Frage kommen sind 6 und 10. Im folgenden geben wir (und dürfen Sie) Beispiele für die Konstruktion gemäß Satz 0.4 angeben. Dabei muss zu vorgegebenen n eine endliche abelsche Gruppe R mit $|R| = m := n^2 + n + 1$ gewählt werden. Welche Gruppe würde sich hier besser anbieten als die Restklassengruppe $(\mathbb{Z}_m, +)$, Sie erinnern sich sicher an das letzte Übungsblatt. Dann muss eine Differenzenmenge \mathcal{D} von \mathbb{Z}_m gefunden werden (das ist ein wenig eine Spielerei, aber einige \mathcal{D} sind aufgeführt). Die Restklassen in \mathbb{Z}_m bezeichnen wir wie üblich mit den Repräsentanten $0, 1, 2, 3, \dots, m-1$ und rechnen mit diesen Elementen modulo m . Fangen Sie am besten bei $n = 3$ an, es folgt $|R| = 3^2 + 3 + 1 = 13$, also wähle man \mathbb{Z}_{13} . Nun kann man $\mathcal{D} = \{0, 1, 3, 9\}$ wählen. Bestätigen Sie nochmals, dass die Menge \mathcal{D} tatsächlich eine Differenzenmenge ist, also man rechnet $0 - 1 = -1 = 12$, auf diese Weise müssen alle Elemente von \mathbb{Z}_{13} entstehen, die 0 natürlich nicht. Schreiben Sie jetzt alle Geraden auf, frei nach dem Motto $g(2) := \mathcal{D} + 2 \setminus \mathcal{D} = \{2, 5, 11\}$. Füllen Sie folgende Tabelle ein wenig weiter aus, mindestens eine Zeile ...

n	R	\mathcal{D}
2	\mathbb{Z}_7	$\{1, 2, 4\}$ <small>$7-3=4$, unser Minimalmodell ist geschaffen</small>
3	\mathbb{Z}_{13}	$\{0, 1, 3, 9\}$ <small>$13-4=9$, dieses Modell wird später eine wichtige Rolle spielen.</small>
4	$\mathbb{Z}_?$	$\{0, 1, 4, 14, 16\}$ (5 Elemente) <small>das werden 16 Punkte ...</small>
5	$\mathbb{Z}_?$	$\{1, 5, 17, 22, 23, 25\}$ (6 Elemente)
6	zwecklos	
7	$\mathbb{Z}_?$	$\{0, 1, 7, 19, 23, 44, 47, 49\}$ (8 Elemente)
8	$\mathbb{Z}_?$	$\{1, 2, 4, 8, 16, 32, 37, 55, 64\}$ (9 Elemente)
9	$\mathbb{Z}_?$	$\{\}$ (? Elemente)
10	zwecklos	