Prof. Dr. Matthias Kriesell
Fakultät für Mathematik und Naturwissenschaften

TECHNISCHE UNIVERSITÄT
ILMENAU

1. Studienbrief zur Diskreten Mathematik

Im Sommersemester 2020 wende ich mich wegen des herrschenden Versammlungsverbotes mittels Studienbriefen an Sie, die Teilnehmer meiner Vorlesung Diskrete Mathematik. Sie erhalten wöchentlich mit jedem Brief Stoff etwa im Umfang einer zweistündigen Vorlesung. Auf diese Weise halten Sie ein durchgängiges Vorlesungsskript in Händen, daß Sie sich allerdings praktisch eigenständig erarbeiten müssen. Das wird jeder von Ihnen auf unterschiedliche Weise bewerkstelligen, dennoch möchte ich Ihnen ein paar grundsätzliche Hinweise mit auf den Weg geben.

Lassen Sie sich von der Kürze des Pensums nicht täuschen. Dieser erste Studienbrief enthält knapp drei Seiten Stoff — die Aufarbeitung einer Seite kann jedoch eine Stunde oder länger dauern. Auch wenn es zu vielen Definitionen Beispiele gibt, sind Sie angehalten, eine eigene Vorstellung beziehungsweise ein Bild des jeweiligen Konzeptes zu entwickeln, und das kann durch Konstruktion weiterer Beispiele geschehen. Zum Verständnis der Sätze und Folgerungen kann man ihre Bedeutung für den Beispielschatz untersuchen. Beweise sind vollständig durchformuliert, meist ein wenig detaillierter als ich es in der Vorlesung halte; vollziehen Sie die Argumente nach, hinterfragen Sie sie kritisch (an einigen Stellen habe ich versucht, Ihren Ehrgeiz durch ein geklammertes „Warum?" anzustacheln); rekapitulieren Sie den Beweisfahrplan, wenn Sie auf das „quod erat demonstrandum" stoßen (symbolisch: $\square$). Illustrieren Sie komplexe Sachverhalte. Lesen Sie gründlich.

Die Übungen dienen der Vertiefung und Verinnerlichung des Stoffs, ganz wie im „Präsenzbetrieb". Alle zwei Wochen erhalten Sie Übungsaufgaben, die Sie bitte selbständig bearbeiten und mir als .pdf zum Abgabetag zukommen lassen wollen. Eine Einzelkorrektur wird wahrscheinlich nicht möglich sein, doch werde ich Ihre „Hauptschwierigkeiten" entdecken und darauf gegebenenfalls im nächsten Brief eingehen.

Jederzeit können Sie mir schreiben, sollten Sie Fragen haben oder auf Fehler oder Unstimmigkeiten in meiner Darstellung stoßen.

Ilmenau, den 14. April 2020 · Matthias Kriesell

Kapitel 1
Mengensysteme mit Symmetrieeigenschaften

Gegenstand des ersten Teils sind zunächst, ganz allgemein, endliche Mengenfamilien, die jedoch rasch mit immer stärkeren Symmetriebedingungen versehen werden und schließlich ins Studium endlicher projektiver Ebenen münden. Wir beginnen mit einem fundamentalen Satz der Ordnungstheorie, dem Satz von DILWORTH und leiten daraus den berühmten Heiratssatz von HALL her, der zu den meistverwendeten Werkzeugen der Kombinatorik gehört.

Wir verwenden folgende Bezeichnungen:

– $\mathbb{N}_n := \{1, \ldots, n\}$ für die ersten n positiven ganzen Zahlen,
– $\mathbb{Z}_n := \{0, \ldots, n-1\}$ für die zyklische Gruppe der Ordnung n mit $+$,
– $\mathfrak{P}(M) := \{A : A \subseteq M\}$ für die Potenzmenge der Menge M,
– $\mathfrak{P}_n(M) := \{A : A \subseteq M \text{ und } |A| = n\}$ für die Menge aller n-elementigen Teilmengen von M und
– $\mathfrak{P}_{\leq n}(M) := \{A : A \subseteq M \text{ und } |A| \leq n\}$ für die Menge aller höchstens n-elementigen Teilmengen von M.

Binäre Relationen auf einer Menge M fassen wir wie üblich als Teilmengen von $M \times M$ auf. Eine Menge M heißt *durch* $\leq\, \subseteq M \times M$ *geordnet*, falls gilt:

(i) $a \leq a$ für alle $a \in M$ ($\leq$ reflexiv);
(ii) $a \leq b$ und $b \leq a$ impliziert $a = b$ für alle a, b aus M ($\leq$ antisymmetrisch);
(iii) $a \leq b$ und $b \leq c$ impliziert $a \leq c$ für alle a, b, c aus M ($\leq$ transitiv).

$a \in M$ heißt *maximal* in M, falls $a \leq b$ impliziert $a = b$ für alle $b \in M$; $a \in M$ heißt *größtes Element* in M, falls $b \leq a$ für alle $b \in M$ gilt; $a \in M$ heißt *minimal* in M, falls $b \leq a$ impliziert $b = a$ für alle $b \in M$; $a \in M$ heißt *kleinstes Element* in M, falls $a \leq b$ für alle $b \in M$ gilt. a, b heißen *vergleichbar*, falls $a \leq b$ oder $b \leq a$ gilt und *unvergleichbar* sonst. $A \subseteq M$ heißt *Kette*, falls a, b vergleichbar sind für alle $a, b \in M$, $A \subseteq M$ heißt *Antikette*, falls a, b unvergleichbar sind für alle $a \neq b$ aus M. Eine Kette und eine Antikette haben daher höchstens ein gemeinsames Element. Ist M durch $\leq$ geordnet und $L \subseteq M$, so ist L durch $\leq \cap (L \times L)$ geordnet; anstelle $\leq \cap (L \times L)$ schreiben wir dann schlicht $\leq$.

Zum Beispiel ist $\mathfrak{P}(M)$ durch $\subseteq$ geordnet, die Menge T_n aller positiven Teiler der Zahl n ist durch die Teilbarkeitsrelation $|$ geordnet usw.

Geordnete Mengen veranschaulicht man durch ihr HASSE-Diagramm: Die Elemente der Menge werden durch Punkte in der Ebene dargestellt; gilt $a \leq b$ und $a \neq b$, so wird a „unter" b gezeichnet, und a, b werden durch eine Linie verbunden, wenn es kein $z \in M \setminus \{a, b\}$ mit $a \leq z \leq b$ gibt (also kein Element

„zwischen“ a und b). $\mathfrak{P}(M)$ kann so *schichtweise* dargestellt werden: Zuunterst kommt die leere Menge, dann die 1-elementigen, dann die 2-elementigen Mengen usf. Entsprechend heißt $\mathfrak{P}_\ell(M)$ auch die ℓ-te Schicht von $\mathfrak{P}(M)$. Für $x \in \mathbb{R}$ seien $\lfloor x \rfloor := \max\{y \in \mathbb{Z} : y \leq x\}$ und $\lceil x \rceil := \min\{y \in \mathbb{Z} : x \leq y\}$. Für $n \in \mathbb{N}$ ist $n! = n \cdot (n-1) \cdot \ldots \cdot 3 \cdot 2 \cdot 1$, und für $n, k \in \mathbb{N}$ ist $\binom{n}{k} := |\mathfrak{P}_k(\mathbb{N}_n)|$ die Anzahl der k-elementigen Teilmengen einer n-elementigen Menge, also bekanntlich gleich $\frac{n!}{k! \cdot (n-k)!}$.

Satz 1.1. (Satz von DILWORTH 1950)

Sei M eine endliche, durch $\leq$ geordnete Menge. Dann ist

$$\begin{aligned} & \min\{k : \text{es gibt disjunkte Ketten } C_1, \ldots, C_k \text{ in } M \text{ mit } C_1 \cup \cdots \cup C_k = M\} \\ = \quad & \max\{|A| : A \text{ Antikette in } M\}. \end{aligned}$$

Beweis. Da jede Antikette höchstens ein Element einer Kette enthält, folgt $\geq$. Zum Nachweis von $\leq$ sei $\ell := \max\{|A| : A \text{ Antikette in } M\}$; wir haben zu zeigen, daß eine Überdeckung von M durch höchstens ℓ Ketten existiert. Diese Behauptung zeigen wir induktiv über $|M|$; sie gilt offenbar für $|M| = 0$. Für $|M| > 0$ sei C eine längste Kette (insbesondere ist $C \neq \emptyset$).

Wenn alle Antiketten von $M \setminus C$ weniger als ℓ Elemente haben, dann gibt es eine Überdeckung von $M \setminus C$ durch weniger als ℓ Ketten, und diese leistet zusammen mit C das Gewünschte.

Andernfalls gibt es eine Antikette A in $M \setminus C$ mit $|A| = \ell$. Jedes Element aus $M \setminus A$ ist vergleichbar mit wenigstens einem Element aus A. Wir zerlegen M in

$$\begin{aligned} M^+ &:= \{x \in M : a \leq x \text{ für ein } a \in A\} \text{ und} \\ M^- &:= \{x \in M : x \leq a \text{ für ein } a \in A\}. \end{aligned}$$

Weil A eine Antikette ist, folgt $M^+ \cap M^- = A$. Das größte Element von C liegt nicht in A und daher nach Wahl von C nicht in M^-, das kleinste Element von C liegt analog nicht in M^+. Somit gilt $|M^+|, |M^-| < |M|$, und wir können Induktion auf M^+, M^- anwenden. Da $|A|$ längste Antikette in M^+ und auch M^- ist, existiert eine Überdeckung von M^+ durch Ketten $C_1^+, \ldots, C_\ell^+$, jeweils mit kleinstem Element a_i^+ aus A (warum?) und eine Überdeckung von M^- durch Ketten $C_1^-, \ldots, C_\ell^-$, jeweils mit größtem Element a_i^- aus A. Durch Umbenennung kann man $a_i^+ = a_i^-$ für alle i erreichen, so daß $C_1^+ \cup C_1^-, \ldots, C_\ell^+ \cup C_\ell^-$ eine Überdeckung von M durch Ketten ist. $\square$

Aus dem Satz von DILWORTH kann man den Heiratssatz von HALL gewinnen, der zu den wichtigsten Werkzeuge in der Kombinatorik gehört.

Folgerung 1.2. (Satz von HALL)

Eine endliche Familie $(A_i)_{i\in I}$ endlicher Teilmengen einer Menge M erfüllt genau dann die HALL-*Bedingung*

$$|\bigcup_{j\in J} A_j| \quad \geq \quad |J| \text{ für alle } J \subseteq I, \tag{1}$$

wenn sie ein *Repräsentantensystem* besitzt, das heißt eine Famile $(a_i)_{i\in I}$ mit $a_i \neq a_j$ für $i \neq j$ aus I und $a_i \in A_i$ für alle $i \in I$. (Auch: *Injektive Auswahlfunktion*.)

Beweis. Die HALL-Bedingung erweist sich leicht als notwendig für die Existenz eines Repräsentantensystems. Sie ist aber auch hinreichend: Ohne Beschränkung der Allgemeinheit sei $M \cap I = \emptyset$. Durch

$$x \leq j :\longleftrightarrow (x \in A_j \text{ und } j \in I) \text{ oder } (x = j \text{ und } x, j \in M \cup I)$$

wird eine Ordnung auf $M \cup I$ definiert, deren Ketten die Länge höchstens 2 haben. Sei A eine größte Antikette. Dann gilt

$$A \cap M \subseteq M \setminus \bigcup_{j\in A\cap I} A_j, \text{ also}$$

$$|A \cap M| \leq |M| - |\bigcup_{j\in A\cap I} A_j| \leq |M| - |A \cap I|$$

wegen der HALL-Bedingung für $J = A \cap I$, und infolgedessen $|A| = |A \cap M| + |A \cap I| \leq |M|$. Nach Satz 1.1. existiert eine Zerlegung von $M \cup I$ in $|A|$ disjunkte Ketten, etwa: ℓ viele der Länge 2 und $|A| - \ell$ viele der Länge 1. Wegen $2\ell + |A| - \ell = |M \cup I| = |M| + |I| \geq |A| + |I|$ folgt $\ell \geq |I|$, und natürlich gilt $\ell \leq |I|$, weil jede der ℓ Ketten der Länge 2 ein Element aus I (und eines aus M) enthält. Somit gibt es genau $|I|$ Ketten der Länge 2, etwa $\{a_i, i\}$ mit $i \in I$; damit ist $(a_i)_{i\in I}$ ein Repräsentantensystem. $\square$

Übungen (1)

Abgabe bis Freitag den 1. Mai 2020.

1. Sei n eine natürliche Zahl. Man rufe sich in Erinnerung, daß die Teilbarkeitsrelation $|$ auf der Menge T_n der positiven Teiler von n eine Ordnung liefert. Man zeichne das HASSE-Diagramm für den Fall $n = 60$ und bestimme eine Zerlegung von T_{60} in möglichst wenige Ketten.

2. Man zeige, daß eine durch $\leq$ geordnete endliche Menge M genau dann eine Antikette der Länge ℓ besitzt, wenn sie sich nicht in weniger als ℓ Ketten zerlegen läßt.

3. Sei M eine endliche durch $\leq$ geordnete Menge. Man zeige: Besitzt M keine Kette mit mehr als ℓ Elementen, so ist M die Vereinigung von höchstens ℓ Antiketten. Gilt die Umkehrung? Können Sie ein min-max-Theorem ableiten?

   Hinweis. Man führe Induktion über ℓ und beachte, daß die maximalen Elemente von M eine Antikette bilden.

4. Sei σ eine Permutation von $M := \{1, \ldots, n^2+1\}$. Man zeige mit Hilfe des Satzes von DILWORTH, daß die Folge $\sigma(1), \ldots, \sigma(n^2+1)$ eine monotone Teilfolge der Länge $n+1$ besitzt.

5. Man beweise die folgende graphentheoretische[1] Version des Satzes von HALL: Genau dann besitzt der endliche bipartite Graph G mit Klassen A, B ein Matching, das A überdeckt, wenn gilt

$$|N_G(S)| \geq |S| \text{ für alle } S \subseteq A.$$

[1]Ein (ungerichteter, schlingenloser, einfacher) *Graph* ist ein Paar $G = (V, E)$ aus Mengen V, E mit $E \subseteq \mathfrak{P}_2(V) = \{e \subseteq V : |e| = 2\}$. Die Elemente aus $V =: V(G)$ und $E =: E(G)$ heißen *Ecken* bzw. *Kanten* von G. G heißt *endlich*, wenn $V(G)$ endlich ist, sonst *unendlich*. Ecken x, y heißen (zueinander) *benachbart* in G, wenn $\{x, y\} \in E(G)$ gilt. Die *Nachbarschaft* einer Menge $A \subseteq V(G)$ in G ist die Menge aller Ecken aus $V(G) \setminus A$, die zu wenigstens einer Ecke aus A benachbart sind, und wird mit $N_G(A)$ bezeichnet. Eine Menge A paarweise nicht benachbarter Ecken heißt *unabhängig* oder eine *Anticlique* in G. Ein Graph heißt *bipartit*, wenn er sich durch zwei disjunkte Anticliquen überdecken läßt. Auf diese — im allgemeinen nicht eindeutig bestimmten Mengen — wird durch das Wort *Klasse* oder *Farbklasse* Bezug genommen. Ein *Matching* ist eine Menge M paarweise disjunkter Kanten von G. Eine Menge F von Kanten *überdeckt* eine Menge A von Ecken, falls $A \subseteq \bigcup F$ gilt.