17.2.2025

Mathematik Entdecken 1 - Klausur 1

(Lösungsskizze. Kein Korrekturschema!)

Aufgabe 1. a) Die Potenzmenge der Menge M ist die Menge

$$2^M = \{A : A \subseteq M\}.$$

b) $2^{\{\emptyset, \{1\}\}} = \{\emptyset, \{\emptyset\}, \{\{1\}\}, \{\emptyset, \{1\}\}\}.$

c) (Allgemein gilt: $\neg(A \Rightarrow B) \Longleftrightarrow A$ und $\neg B$, also:)

$M \subseteq N$ und ($\forall x \in M$ gilt $x \notin N$).

Die Aussage ist nicht für alle Mengen M und N wahr. Zum Beispiel, für $M = \emptyset$ und $N = \{1\}$ gilt "$\emptyset \subseteq \{1\}$", aber "$\exists x \in \emptyset$ mit $x \in \{1\}$" gilt nicht.

d) Weil A und B gleichmächtig sind, existiert $f: A \longrightarrow B$ bijektiv, also auch invertierbar. Wir definieren $F: 2^A \longrightarrow 2^B$ durch $F(M) := f(M) = \{f(x) : x \in M\} \in 2^B$, $\forall M \in 2^A$.

Wir zeigen, dass F bijektiv ist, indem wir zeigen, dass F eine Inverse besitzt: $F^{-1}: 2^B \longrightarrow 2^A$, $F^{-1}(N) = f^{-1}(N)$, $\forall N \in 2^B$.

Sei $M \in 2^A$ beliebig. Es gilt:

$$(F^{-1} \circ F)(M) = F^{-1}(F(M)) = f^{-1}(f(M)) = (f^{-1} \circ f)(M) =$$
$$= id_A(M) = M.$$

Also $F^{-1} \circ F = id_{2^A}$. Analog verwenden wir $f \circ f^{-1} = id_B$ um zu zeigen, dass $F \circ F^{-1} = id_{2^B}$. $\square$

e) • f ist <u>nicht injektiv</u> weil $f(\{1\}) = f(\{1,2,3\}) = 1$, aber $\{1\} \neq \{1,2,3\}$.

• f ist <u>surjektiv</u> weil $\forall n \in \mathbb{N}$, $\exists \{n\} \in 2^{\mathbb{N}} \setminus \{\emptyset\}$, sodass

$$f(\{n\}) = \min\{n\} = n.$$

f) Wir zeigen, dass $f^{-1}(a)$ und $2^{\mathbb{N}_{>a}}$ gleichmächtig sind.

Weil $\mathbb{N}$ und $\mathbb{N}_{>a}$ gleichmächtig sind, folgt es, dan auch $2^{\mathbb{N}_{>a}}$ und $2^{\mathbb{N}}$ gleichmächtig sind.

Es gilt $f^{-1}(a) = \{A \subseteq \mathbb{N} \mid \min A = a\}$.

Wir bezeichnen diese Menge mit M_a, und definieren $\varphi: M_a \longrightarrow 2^{\mathbb{N}_{>a}}$ durch

$$\varphi(A) := A \setminus \{a\}.$$

Weil $\min A = a$, folgt es, dan $x > a$ für alle $x \in A \setminus \{a\}$. Also $\varphi(A) \in 2^{\mathbb{N}_{>a}}$.

Für die Bijektivität bestimmen wir eine Inverse:
$\varphi^{-1}: 2^{\mathbb{N}_{>a}} \longrightarrow M_a$ mit $\varphi^{-1}(B) := B \cup \{a\}$.
Weil $B \subseteq \mathbb{N}_{>a}$, folgt $b > a \;\forall b \in B$, also $\min(B \cup \{a\}) = a$. Also $\varphi^{-1}(B) \in M_a$ und φ^{-1} ist eine Abbildung.
Es gilt dann für alle $A \in M_a$, dass
$(\varphi^{-1} \circ \varphi)(A) = \varphi^{-1}(A \setminus \{a\}) = (A \setminus \{a\}) \cup \{a\} = A$ (weil $a \in A$)

Weiterhin, für alle $B \in 2^{\mathbb{N}_{>a}}$ gilt

$$(\varphi \circ \varphi^{-1})(B) = \varphi(B \cup \{a\}) = (B \cup \{a\}) \setminus \{a\} = B$$

(weil $a \notin B$).

Also $\varphi^{-1} \circ \varphi = \mathrm{id}_{M_a}$ und $\varphi \circ \varphi^{-1} = \mathrm{id}_{2^{\mathbb{N}_{>a}}}$, also φ ist eine bijektive Abbildung.

Aufgabe 2 a) <u>Lemma von Bézout</u>

Für alle $a, b \in \mathbb{Z}$ existieren $\lambda, \mu \in \mathbb{Z}$, sodass

$$ggT(a,b) = \lambda \cdot a + \mu \cdot b.$$

b) $d \mid a \implies \exists\, k \in \mathbb{Z} : a = k \cdot d$

$d \mid b \implies \exists\, l \in \mathbb{Z} : b = l \cdot d$

Seien $\lambda, \mu \in \mathbb{Z}$ beliebig. Es gilt:

$$\lambda \cdot a + \mu \cdot b = \lambda (k \cdot d) + \mu \cdot (l \cdot d) = (\lambda k + \mu l) \cdot d,$$

also $d \mid \lambda a + \mu b$.

c) Wir wenden den erweiterten Euklidischen Algorithmus:

$$\left.\begin{array}{lll} 117 = 23 \cdot 5 + 2 & \implies & 2 = 1 \cdot 117 + (-5) \cdot 23 \\ 23 = 11 \cdot 2 + 1 & \implies & 1 = 1 \cdot 23 + (-11) \cdot 2 \end{array}\right] \implies$$

$$\implies 1 = 1 \cdot 23 + (-11) \cdot [117 + (-5) \cdot 23] =$$

$$= 56 \cdot 23 + (-11) \cdot 117 = 1288 - 1287$$

Also $(\lambda, \mu) = (56, -11)$ ist ein solches Paar.

Um ein weiteres Paar zu finden verwenden wir: $117 \cdot 23 + (-23) \cdot 117 = 0$. Es gilt also:

$$1 = 1 + 0 = (56 \cdot 23 + (-11) \cdot 117) + (117 \cdot 23 + (-23) \cdot 117) =$$

$$= 173 \cdot 23 + (-34) \cdot 117.$$

Ein zweites Paar ist also $(\lambda, \mu) = (173, -34)$.

d) Wir verwenden Induktion nach n für die Familie von

Aussagen $\mathcal{A}(n)$: $\quad 9 \mid n^3 + (n+1)^3 + (n+2)^3$.

I.A: $\mathcal{A}(0)$: $\quad 9 \mid 0 + 1 + 2^3$ ist wahr.

I.S.: $\mathcal{A}(n) \Rightarrow \mathcal{A}(n+1)$

Die inductive Voraussetzung ist also

(I.V.) $\quad 9 \mid n^3 + (n+1)^3 + (n+2)^3$.

Zu zeigen ist: $9 \mid (n+1)^3 + (n+2)^3 + (n+3)^3$.

Es gilt:

$$(n+1)^3 + (n+2)^3 + (n+3)^3 = (n+1)^3 + (n+2)^3 + n^3 + 3 \cdot n^2 \cdot 3 + 3 \cdot n \cdot 3^2 + 3^3 =$$

$$= \underbrace{\left[n^3 + (n+1)^3 + (n+2)^3\right]}_{a} + \underbrace{9(n^2 + 3n + 9)}_{b}$$

Aus der (I.V.) gilt $9 \mid a$, und b ist ein Vielfaches von 9. Also $9 \mid a+b$.

e) Es gilt $2025 = 45^2$ und $45 \equiv 4 \mod 41$.

Also: $\quad 2025^{2025} - 1 \equiv (45^2)^{45 \cdot 45} - 1 \equiv 4^{2 \cdot 45 \cdot 45} - 1 \equiv$

$$\equiv \left[(4^{45})^{45}\right]^2 - 1 \equiv \left[(4^{45})^{45} - 1\right]\left[(4^{45})^{45} + 1\right] \mod 41$$

Weil 41 prim ist folgt aus dem (Korollar von dem) kleinen Satz von Fermat:

$$a^{40} \equiv 1 \mod 41, \quad \forall a \text{ mit } a \not\equiv 0 \mod 41.$$

Es folgt also: $\quad a^{45} \equiv a^{40+5} \equiv a^{40} \cdot a^5 \equiv a^5 \mod 41$.

Weil $2^k \not\equiv 0 \mod 41$, $\forall k \in \mathbb{N}$ haben wir

$$(4^{45})^{45} \equiv (4^{45})^5 \equiv (4^5)^5 \equiv 4^{25} \equiv 2^{50} \equiv 2^{10} \mod 41.$$

Aus und folgt also

$$2025^{2025} - 1 \equiv (2^{10} - 1) \cdot (2^{10} + 1) \mod 41.$$

Wir bemerken, dass $2^7 \equiv 128 \equiv 3 \cdot 41 + 5 \equiv 5 \mod 41$.

Also $2^{10} \equiv 2^3 \cdot 2^7 \equiv 8 \cdot 5 \equiv 40 \equiv -1 \mod 41$.

Wenn wir in einsetzen, bekommen wir

$$2025^{2025} - 1 \equiv (-1-1) \cdot (-1+1) \equiv 0 \mod 41.$$

Also $41 \mid 2025^{2025} - 1$.

Aufgabe 3. a) Eine Inzidenzgeometrie ist eine Inzidenzstruktur $(\mathfrak{X}, \mathcal{G})$, die folgende drei Axiome erfüllt:

(I1.) $\forall A, B \in \mathfrak{X}$ mit $A \neq B$, $\exists!\, g \in \mathcal{G}$ mit $A \in g$ und $B \in g$.

(I2.) $\forall g \in \mathcal{G}$ gilt $\# g \geq 2$.

(I3.) $\exists\, A, B, C \in \mathfrak{X}$, sodass A, B, C nicht kollinear sind.

b) Seien $g, h \in \mathcal{G}$ mit $g \neq h$.

Wir führen einen Widerspruchsbeweis um $\#(g \cap h) \leq 1$ z.z.

Nehmen wir an, dass $\#(g \cap h) \geq 2$. Es folgt also, dass es $A \neq B$ gibt mit $A, B \in g \cap h$. Weil $A \neq B$ gibt es laut (I1) genau eine Gerade die A und B enthält. Also, weil $A, B \in g$ und $A, B \in h$ folgt $g = h$ - $\lightning$ zu $g \neq h$.

Also $\#(g \cap h) \leq 1$.

c) <u>Beispiel</u>: $\mathfrak{X} = \{1, 2, 3\}$, $\mathcal{G} = \{\{1,2\}, \{1,3\}, \{2,3\}\}$

ist eine Inzidenzgeometrie mit

$1 \in \{1, 2\}$, $1 \in \{1, 3\}$, $1 \notin \{2, 3\}$.

Also 1 liegt auf genau zwei Geraden, somit ist es eine V-Geometrie

<u>Nichtbeispiel</u>: In der euklidischen Ebene liegt jeder Punkt auf unendlich-viele Geraden. Es ist also nicht eine V-Geometrie

<u>Alternativ</u>: Die affine Ebene mit 4 Punkten. Dort liegt jeder Punkt auf genau drei Geraden.

d) Sei $n \in \mathbb{N}$, $n \geq 3$ und $\mathcal{X} = \{1, 2, .., n\}$

Wir setzen $\mathcal{G} = \{\{1, .., n-1\}\} \cup \{\{i, n\} : i = 1, .., n-1\}$

Diese ist eine Inzidenzgeometrie (aus der VL) und der Punkt 1 liegt auf genau zwei Geraden:
$1 \in \{1, .., n-1\}$ und $\{1, n\}$.

e) Sei $(\mathcal{X}, \mathcal{G})$ eine V-Geometrie, mit $P \in \mathcal{X}$ auf genau zwei geraden: g_1, g_2. Wenn $g_1 \cup g_2 \subsetneq \mathcal{X}$, dann muss ein $Q \in \mathcal{X} \setminus (g_1 \cup g_2)$ existieren. Nach (I1) existiert auch eine Gerade PQ mit $PQ \neq g_1$ und $PQ \neq g_2$ $\lightning$.
Also $g_1 \cup g_2 = \mathcal{X}$.

Nach eventueller Umbenennung können wir OBdA annehmen, dass: $\mathcal{X} = \{1, 2, .., 7\}$, $P = 1$,

$$g_1 = g_{1k} = \{1, .., k\} \text{ und } g_2 = g_{2k} = \{1, k+1, .., 7\}.$$

Nach Axiom I2 gilt $\#g_{1k}, \#g_{2k} \geq 2$, also $k \in \{2, .., 6\}$.

Weil $g_{1k} \cup g_{2k} = \mathcal{X}$ gilt für alle $g \in \mathcal{G} \setminus \{g_{1k}, g_{2k}\}$:

$$g = g \cap \mathcal{X} = g \cap (g_{1k} \cup g_{2k}) = (g \cap g_{1k}) \cup (g \cap g_{2k}).$$

Also $\#g \leq \#(g \cap g_{1k}) + \#(g \cap g_{2k}) = 1 + 1 = 2$.
Aus (I2) gilt $\#g \geq 2$, somit $\#g = 2$.

Sei also $g \in \mathcal{G} \setminus \{g_{1k}, g_{2k}\}$ mit $g = \{a, b\}$, $a < b$.

Weil $1 \notin g$ (V-Geometrie), folgt $1 < a$.

Weil $\#(g \cap g_{1k}) \leq 1$, folgt $b > k$.

Weil $\#(g \cap g_{2k}) \leq 1$, folgt $a \leq k$.

Also $g = \{a, b\}$, mit $a \in \{2, .., k\}$, $b \in \{k+1, .., n\}$.

Jede solche Gerade muss nach (I1) in $\mathcal{G}$ liegen.

Die V-Geometrie $(\mathcal{X}, \mathcal{G})$ ist also durch $k \in \{2, .., 6\}$ eindeutig bestimmt.

Nennen wir diese $(\mathcal{X}_k, \mathcal{G}_k)$.

Wir betrachten für jedes solches k, die Menge $\{\# g_{1k}, \# g_{2k}\}$. Wir haben:

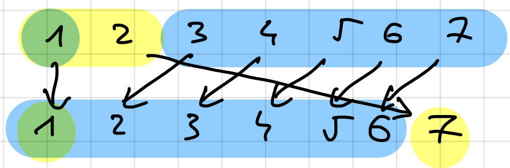
$k = 2 \rightsquigarrow \{2, 6\}$; $k = 6 \rightsquigarrow \{6, 2\}$

$k = 3 \rightsquigarrow \{3, 5\}$; $k = 5 \rightsquigarrow \{5, 3\}$

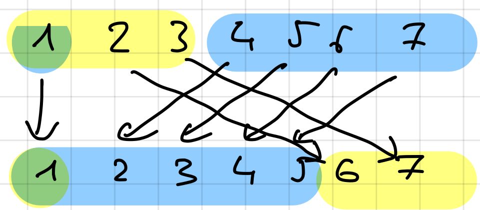
$k = 4 \rightsquigarrow \{4, 4\}$;

Also $(\mathcal{X}_2, \mathcal{G}_2)$, $(\mathcal{X}_3, \mathcal{G}_3)$, $(\mathcal{X}_4, \mathcal{G}_4)$ sind paarweise nich isomorph.

$(\mathcal{X}_2, \mathcal{G}_2) \simeq (\mathcal{X}_6, \mathcal{G}_6)$ durch



und $(\mathcal{X}_3, \mathcal{G}_3) \simeq (\mathcal{X}_5, \mathcal{G}_5)$ durch



Es gibt also, bis auf Isomorphie, genau 3 V-Geom. mit $\#\mathcal{X} = 7$.

ENDE DER LÖSUNGSSKIZZE.