Wie werden die Vorlesungen/Übungen organiziert?

- Einzige Änderung: die Hausaufgaben können zuzweit abgegeben werden.
- Sonsts wie im Wintersemester:
  - Sie müssen an den Übungen regelmäßig und aktiv teilnehmen
  - Mind. 60% der Punkte von der Hausaufgaben sammeln
    1. Am fast jeden Montag wird ein Übungsblatt mit in der regel vier Aufgaben in Netz gestellt (CAJ, bitte unter http://caj.informatik.uni-jena.de/ sich anmelden).
    2. Heute kommen die erste Hausaufgaben.
    3. Sie müssen die Aufgaben lösen und vor der darauffolgenden Montagsvorlesung abgeben
    4. Dieses Mal ist die Regel „vor der Vorlesung“ streng.
  - in der Woche 16.06–22.06 Schreiben wir eine Probe-Klausur (Freiwillig, bis zum 20 % der Hausaufgabenpunkten)
  - Sie bekommen 2 Bonusblättern.
- Sie müssen die Modul–Anmeldungen ausdrücken, ausfüllen, und im Prüfungsamt (Physik-Studenten: mir) abgeben

Es gibt 2 oder 3 Übungsgruppen:

1. Mi 8–10. (Dr. Uta Freiberg)
2. Do 8–10. (Dr. Konrad Schöbel)

- Nach Bedarf gibt es noch eine Übungsgruppe.

Verteilung in die Übungsgruppen findet morgen statt (weil die Anzahl von Übungsgruppen von Anzahl von Teilnehmern abhängt).

Was werden wir zuerst lehrnen?

- Grunglagen der Algebra und mathematischen Logik (Körpererweiterungen, kardinalitäten, Paradoxen).
- Jordan-Normalformen (verallgemeinerung von Diagonalizierung).

Körper – Wiederholung

Körper (Def. 13 und 16, LAAG I) ist die Menge mit zwei innerverknüpfungen $(\mathbb{K}, +, \cdot)$ mit der folgenden Eigenschaften:

(R1) $(\mathbb{K}, +)$ ist eine abel'sche Gruppe, deren neutrales Element werden wir 0 bezeichen;

(R2) die Multiplikation „$\cdot$“ ist assoziativ und kommutativ.

(R3) es gilt das Distributivgesetz, d. h. für alle $a, b, c \in \mathbb{K}$ ist $a \cdot (b + c) = a \cdot b + a \cdot c$.

(K4) $(\mathbb{K} \setminus \{0\}, \cdot)$ eine (abelsche) Gruppe ist.

Unterkörper ist eine nichtleere Teilmenge $\mathbb{K}'$ der Körper, die eine Untergruppe bzgl. „$+$“ ist, und sodass $\mathbb{K}' \setminus \{0\}$ eine Untergruppe bzgl. „$\cdot$“ ist.

Bemerkung $0 \in \mathbb{K}'$, weil $\mathbb{K}'$ eine Untergruppe bzgl. $+$ ist, und deswegen das neutrale Element enthalten muß.

Bemerkung. Aus Def. 4/ Satz 5 LAAG I folgt, dass die Verknüpfungen „$+$“ und „$\cdot$“ auf $\mathbb{K}'$ wohldefiniert sind, und dass die Teilmengen $\mathbb{K}'$ und $\mathbb{K}' \setminus \{0\}$ Gruppen bzgl. „$+$“ bzw. „$\cdot$“ sind. Deswegen ist ein Unterkörper auch ein Körper.

Körpererweiterung

Zwei Körper $(\mathbb{K}_1, +_1, \cdot_1)$ und $(\mathbb{K}_2, +_2, \cdot_2)$ sind isomorph, falls es eine Bijektion $\phi : \mathbb{K}_1 \to \mathbb{K}_2$ gibt, die die Verknüpfungen erhält: $\phi(x \cdot_1 y) = \phi(x) \cdot_2 \phi(y)$, $\phi(x +_1 y) = \phi(x) +_2 \phi(y)$.

Def. 1 Körper $\mathbb{H}$ heißt eine Körpererweiterung von einem Körper $\mathbb{K}$, falls es einen Unterkörper $\mathbb{H}' \subseteq \mathbb{H}$ gibt, der zu $\mathbb{K}$ isomorph ist.

(In der Regel wird $\mathbb{K}$ bereits ein Unterkörper von $\mathbb{H}$ sein; in dem Fall wird Isomorphismus die Identitetsabbildung.)

Bsp. $\mathbb{C}$ ist eine Körpererweiterung von $\mathbb{R}$.
Bsp. $\mathbb{R}$ ist eine Körpererweiterung von $\mathbb{Q}$.

Wicht. Bsp. Quadratrische Körpererweiterung von $\mathbb{Q}$.
Sei $s \in \mathbb{Q}_{\geq 0}$ sodass $\sqrt{s} \notin \mathbb{Q}$ (Z.B. $s = 2$).
Setze $\mathbb{Q}(\sqrt{s}) := \{x + y\sqrt{s} \mid x, y \in \mathbb{Q}\} \subseteq \mathbb{R}$.
Lemma 1 $\mathbb{Q}(\sqrt{s})$ ist eine Körpererweiterung von $\mathbb{Q}$.
Beweis. Offensichtlich ist $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{s})$. Nach Def. 1 müssen wir zeigen, dass $\mathbb{Q}(\sqrt{s})$ ein Körper ist.

Es genugend z.z. (s. Bemerkung oben), dass $\mathbb{Q}(\sqrt{s})$ ein Unterkörper von $\mathbb{R}$. Wir müssen zeigen, dass $\mathbb{Q}(\sqrt{s})$ und $\mathbb{Q}(\sqrt{s}) \setminus \{0\}$ Untegruppen von $\mathbb{Q}$ ist, d.h., $\mathbb{Q}(\sqrt{s})$ abgeschlossen bzgl. „+“ , „·“, und invertieren ist.

Addition: $x_1 + y_1\sqrt{s} + x_2 + y_2\sqrt{s} = \underbrace{x_1 + x_2}_{x \in \mathbb{Q}} + \underbrace{(y_1 + y_2)}_{y \in \mathbb{Q}}\sqrt{s}$.

Invertieren bzgl. „+“: $x + y\sqrt{s} + (-x - y\sqrt{s}) = 0$.

Multiplikation: $(x_1 + y_1\sqrt{s}) \cdot (x_2 + y_2\sqrt{s}) = \underbrace{x_1x_2 + y_1y_2s}_{x \in \mathbb{Q}} + \underbrace{(x_1y_2 + x_2y_1)}_{y \in \mathbb{Q}}\sqrt{s}$

Invertieren bzgl. „·“:

$$(x + y\sqrt{s}) \cdot \left(\underbrace{\frac{x}{x^2 - y^2s}}_{\in \mathbb{Q}} - \underbrace{\frac{y}{x^2 - y^2s}}_{\in \mathbb{Q}}\sqrt{s} \right) = \frac{(x+y\sqrt{s})(x-y\sqrt{s})}{x^2-y^2s} = 1. \qquad \square$$

Bemerkung: Für $x + y\sqrt{s} \neq 0$ ist der Nenner $x^2 - y^2s \neq 0$, weil sonst $\frac{x^2}{y^2} = s$ ist, also $\sqrt{s} = \frac{|x|}{|y|} \in \mathbb{Q}$, was Voraussetzungen widerspricht.

In Beweis von Lemma 1 kann man $\mathbb{Q}$ mit jedem Unterkörper $\mathbb{K} \subseteq \mathbb{R}$ (oder sogar $\mathbb{K} \subseteq \mathbb{C}$) ersetzen (die Zahl s erfüllt dann die Bedienung $\sqrt{s} \notin \mathbb{K}$). Beweis wird buchstäblich wiederholt. Also gilt:

Lemma 1' Sei $\mathbb{K}$ eine Unterkörper von $\mathbb{R}$ (bzw. $\mathbb{C}$), und $s \in \mathbb{K}$ mit $\sqrt{s} \notin \mathbb{K}$. Dann ist die Menge $\mathbb{K}(\sqrt{s}) := \{x + y\sqrt{s} \mid x, y \in \mathbb{K}\} \subseteq \mathbb{R}$ (bzw. $\subseteq \mathbb{C}$) auch eine Unterkörper von $\mathbb{R}$ (bzw. $\mathbb{C}$).

Dieser Unterkörper heißt eine quadratische Erweiterung von $\mathbb{K}$.

Bsp. $\mathbb{C} = \mathbb{R}(\sqrt{-1})$. Tatsächlich, jede Zahl $z \in \mathbb{C}$ kann man in der Form $\underbrace{x}_{\in\mathbb{R}} + \underbrace{y}_{\in\mathbb{R}} \cdot i$ darstellen.

Endliche Körpererweiterungen

Lemma 2 Sei $\mathbb{K}'$ eine Unterkörper der Körper $(\mathbb{K}, +, \cdot)$. Dann ist $(\mathbb{K}, +, \cdot)$ ein $\mathbb{K}'$-Vektorraum.

(Diese Aussage war in Blatt 8 LAAG I).

Beweis. $(\mathbb{K}', +, \cdot)$ ist ein Körper; $(\mathbb{K}, +)$ ist eine abelsche Gruppe. Wir müssen die Axiomen (V1 – V4) nachweisen: für $\lambda, \mu \in \mathbb{K}'$ und $v, u \in \mathbb{K}$ soll

(V1) $\lambda(\mu v) = (\lambda\mu)v \quad (=: \lambda\mu v) \Longleftarrow$ Assoziativität von $\mathbb{K}$ bzgl. „$\cdot$“.

(V2) $(\lambda + \mu)v = (\lambda v) + (\mu v) \Longleftarrow$ (R3) (das Distributivgesetz)

(V3) $\lambda(v + w) = (\lambda v) + (\lambda w) \Longleftarrow$ (R3) (das Distributivgesetz)

(V4) $1v = v$ weil Einselement der Untergruppe auch Einselement der Gruppe ist. □

Eine Körpererweiterung $\mathbb{K}' \subseteq K$ heißt endlich, falls die Dimension von $(\mathbb{K}, +, \cdot)$ ein endlichdimensionaler $\mathbb{K}'$-Vektorraumist.

Bsp. $\mathbb{Q}(\sqrt{s})$ ist eine endliche Erweiterung von $\mathbb{Q}$ (weil jedes Element die Form $x + y \cdot \sqrt{s}$ hat, also die Menge $\{1, \sqrt{s}\}$ ist erzeugend.)

Bsp. $\mathbb{C}$ ist eine endliche Erweiterung von $\mathbb{R}$, weil die Menge $\{1, i\}$ erzeugend ist.z 1

Satz 1. $\mathbb{R}$ ist keine endliche Erweiterung von $\mathbb{Q}$.

Exkurs: Mächtigkeit (Ordnung) einer Menge

Def. 2 Seien A, B Mengen. Wir sagen, dass A höchstens gleichmächtig als B ist, falls es eine injektive Abbildung $f : A \to B$ gibt. Screibweise: $|A| \leq |B|$. Wir sagen, dass A und B gleichmächtig sind, falls $|A| \geq |B|$ und $|B| \geq |A|$ ist. Schreibweise: $|A| = |B|$.

Bsp. Die Mengen A, B seien endlich, $|A| := a$, $|B| := b$. Dann gilt: $|A| \geq |B| \iff a \geq b$, folglich $|A| = |B| \iff a = b$.

Bemerkung. Gibt es eine Bijektion $f : A \to B$, so gilt: $|A| = |B|$.
Beweis. f ist bijektiv, deswegen injektiv, deswegen $|A| \leq |B|$. Da f bijektiv ist, gibt es eine inverse Abbldung $g : B \to A$, die auch bijektiv (folglich injektiv) ist; also $|A| \geq |B|$. □

Bsp. $I_1 := \{x \in \mathbb{R} \mid 0 < x < 1\}$ ist gleichmächtig mit $I_2 := \{x \in \mathbb{R} \mid 0 < x < 2\}$.

Tatsächlich, die Abbildung $f : x \mapsto 2 \cdot x$ ist eine Bijektion zwischen I_1 und I_2.

Bsp. $|\mathbb{Z}| = |\mathbb{N}|$. **Beweis.** Die Abildung $f : \mathbb{N} \to \mathbb{Z}$,

$$f(n) = \begin{cases} (n-1)/2 & \text{falls } n \text{ ungerade ist} \\ -n/2 & \text{falls } n \text{ gerade ist} \end{cases}$$

ist eine Bijektion

Ein kurioses Beispiel

Hilberts Hotel (Hilbert:  1862 –1943) besteht aus unendlich viel Zimmer (mit natürlichen Zahlen nummeriert), die leider alle belegt sind. Es kommen aber noch unendlich viele Gäste (auch mit natürlichen Zahlen durchnummeriert). Kann man Sie unterbringen, ohne die Zimmern doppelt belegt sind?

Antwort: Ja!

Den Gast aus Zimmer k geht in das Zimmer $2k$

Der Neugekommene mit Nummer k geht in das Zimmer $2k - 1$.

Keine Doppelbelegung: die alte Gueste sind jetzt in Zimmern mit geraden Nummern, die neue in in Zimmern mit ungeraden Nummern. Alle sind untergebracht.

Wicht. Bsp. $|\mathbb{N}| = |\mathbb{N} \times \mathbb{N}|$.

Beweis: Die injektive Abbildung $\mathbb{N} \to \mathbb{N} \times \mathbb{N}$ ist einfach zu finden: $n \mapsto (1, n)$.

Wir konstruieren eine injektive Abbildung $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$.

Sei p_n die $n-$te Primzahl. Z.B., $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_4 = 7$.

Wir definieren $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, $f(n, m) = p_n^m$.

Die Abbildung ist injektiv: ist $f(n, m) = f(n', m')$, so ist $p_{n'}^{m'} = p_n^m$

folglich $p_{n'}^{m'} \equiv p_n^m \pmod{p_n}$

folglich $p_{n'}^{m'} \equiv 0 \pmod{p_n}$,

was unmöglich ist, weil $\mathbb{Z}_{p_n}$ ein Körper ist und $p_{n'} \not\equiv 0 \pmod{p_n}$ ist

. □

Daraus folgt insbesonderem, dass $|\mathbb{N}| = |\mathbb{Q}|$.
In der Tat, $|\mathbb{Q}| \geq |\mathbb{N}|$, weil die Abbildung $I : \mathbb{N} \to \mathbb{Q}$, $I(n) = n$ eine Injektion ist.

Um zu zeigen, dass $|\mathbb{Q}| \leq |\mathbb{N}|$, benutzen wir die Abbildung
$f \circ g : \mathbb{Q} \to \mathbb{N}$, wobei
f die injektive Abbildung : $\mathbb{N} \to \mathbb{N} \times \mathbb{N}$ aus dem Wicht. Bsp. ist,
und $g : \mathbb{Q} \to \mathbb{N} \times \mathbb{N}$ ist die folgende injektive Abbildung:

$$g(p/q) = \begin{cases} (|p|, |q|) & \text{falls } p/q \geq 0 \\ (2 \cdot |p|, 2 \cdot |q|) & \text{falls } p/q < 0 \end{cases} \in \mathbb{N} \times \mathbb{N}.$$

(Wir nehmen an, dass p und q Teilfremd sind.)
Da die Verkettung von injektiven Abbildungen injektiv ist, ist
$f \circ g : \mathbb{Q} \to \mathbb{N}$ auch injektiv, folglich $\mathbb{Q} \leq \mathbb{N}$. Dann $|\mathbb{Q}| = |\mathbb{N}|$. $\square$

Satz 2. Zwei Mengen A, B sind genau dann gleichmächtig, wenn es eine Bijektion $h\colon A \to B$ gibt.

Beweis. $\Longleftarrow$ ist trivial (und ist bereits oben bewiesen; wir wiederholen den Beweis): h ist injektiv; deswegen $|A| \leq |B|$. Die inverse Abbildung h^{-1} ist auch eine Bijektion, folglich injektiv, folglich $|A| \geq |B|$.

Es gelte jetzt $|A| = |B|$, und zwar seien $f\colon A \to B$ und $g\colon B \to A$ injektiv. Wir definieren jetzt eine Abbildung $h\colon A \to B$ wie folgt:Sei $A_1 = A \setminus Bild_g(B)$ und dann rekursiv $A_{n+1} = Bild_{g\circ f}(A_n)$. Sei $C = \bigcup_{n\geq 1} A_n$.

* Ist $a \in C$, so setze $h(a) = f(a)$.
* Ist $a \notin C$, so folgt insbesondere $a \in Bild_g(B)$, wir können somit $h(a) = g^{-1}(a)$ setzen.

Diese Abbildung h ist injektiv: Es gelte $h(a_1) = h(a_2)$ für zwei Elemente $a_1, a_2 \in A$.

* Ist $a_1 \in C$ und $a_2 \notin C$, so ergibt sich mit $a_2 = g(h(a_2)) = g(h(a_1)) = g(f(a_1)) \in A_{n+1}$ ein Widerspruch.
* Der Fall $a_2 \in C$ und $a_1 \notin C$ ist ebenso ausgeschlossen.
* Ist $a_1 \in C$ und $a_2 \in C$, so folgt $f(a_1) = h(a_1) = h(a_2) = f(a_2)$, also $a_1 = a_2$.
* Ist weder $a_1 \notin C$ und $a_2 \notin C$, so folgt $a_1 = g(h(a_1)) = g(h(a_2)) = a_2$.

Die Abbildung ist aber auch surjektiv: Sei $b \in B$ beliebig.

* Ist $g(b) \in A_n$ für ein $n \geq 1$ p, so folgt nach Definition von A_1, dass sogar $n > 1$ gilt.Folglich ist $g(b) = g(f(a))$ für ein $a \in A_{n-1}$ und $h(a) = f(a) = b$.
* Ansonsten gilt $h(g(b)) = g^{-1}(g(b)) = b$.

Folglich ist $h\colon A \to B$ eine Bijektion,

Folgerung. $|\underbrace{\mathbb{N} \times \cdots \times \mathbb{N}}_{k \text{ Stuck}}| = \mathbb{N}$.

Beweis für $k = 3$. Wir haben in Wicht. Bsp. gezeigt, dass $|\underbrace{\mathbb{N} \times \mathbb{N}}| = \mathbb{N}$.

Nach Satz 2 gibt es dann eine Bijektion $\phi : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$. Wir konstruieren eine Bijektion $\Phi : \mathbb{N} \times \mathbb{N} \times \mathbb{N} \to \mathbb{N}$. Wir setzen
$\Phi(n_1, n_2, n_3) := \phi(\phi(n_1, n_2), n_3) \in \mathbb{N}$.

Φ ist injektiv: gilt $\Phi(n_1, n_2, n_3) = \Phi(m_1, m_2, m_3)$, so ist $\phi(\phi(n_1, n_2), n_3) = \phi(\phi(m_1, m_2), m_3)$. Da ϕ bijektiv ist, folgt daraus, dass $\phi(n_1, n_2) = \phi(m_1, m_2)$ und $n_3 = m_3$. Da ϕ bijektiv ist, folgt aus $\phi(n_1, n_2) = \phi(m_1, m_2)$ dass $n_1 = m_1$ und $n_2 = m_2$. Also, Φ ist injektiv.

Φ ist surjektiv: Es sei $n \in \mathbb{N}$. Da ϕ surjektiv ist, gibt es n_1, n_2 mit $\phi(n_1, n_2) = n$. Da Da ϕ surjektiv ist, gibt es m_1, m_2 mit $\phi(m_1, m_2) = n_1$. Dann ist $\Phi(m_1, m_2, n_2) = \phi(\phi(m_1, m_2), n_2) = \phi(n_1, n_2) = n$. □

Bemerkung: Beweis für beliebiges k erfolgt nach Induktion (im Beweis für $k = 3$ haben wir praktisch Induktionsschritt gemacht).