LINEARE ALGEBRA I
(VORLESUNG SS 2024, FU BERLIN)

KLAUS ALTMANN

1. Einführende Beispiele, mathematische Sprache

16.4.24 (1)

1.1. Gemischte Beispiele: Schnitte von Ebenen und Geraden, Quadriken, affine Abbildungen $\mathbb{R}^3 \to \mathbb{R}^3$, Fibonacci-Folge, lineare (Differential-) gleichungssysteme.

1.2. Zahlen. $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ (Vorteile: Jedes Polynom hat Nullstelle; Gleichungen wie $x^2 + y^2 = 0$ liefern etwas 1-Dimensionales); $\mathbb{K}^n$; $\mathbb{C} = [\mathbb{R}^2$ mit Multiplikation$]$. $\mathbb{Z}/n\mathbb{Z}$, Eigenschaften des gcd in $\mathbb{Z}$, $\gcd(0,0) = 0$, Euklidischer Algorithmus (insbesondere $\gcd(a,b) \in a\mathbb{Z} + b\mathbb{Z}$) $\rightsquigarrow \mathbb{F}_p$. Eindeutige Primzerlegung in $\mathbb{Z}$:

19.4.24 (2)

Satz 1. *$p \in \mathbb{N}$ Primzahl $\Rightarrow$ Für $a, b \in \mathbb{Z}$ gilt: $[p|ab \Leftrightarrow p|a$ oder $p|b]$.*

($p \not| a \Rightarrow \gcd(a,p) = 1 \Rightarrow \exists x, y \in \mathbb{Z} : ax + py = 1 \Rightarrow p|b$ wegen $b = abx + pyb$.)

1.3. Mengen. Mengen und Elemente (naiv); Schreibweise von Mengen (Bsp. $2\mathbb{Z}$ oder S^1); $\emptyset$; Teilmengen; Mengenoperationen $\cup, \cap, \times, \setminus$; Gesetze wie $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$, $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$; Beziehungen zur Aussagenlogik; Mengensysteme, $\bigcup_{i \in I} A_i$, $\bigcap_{i \in I} A_i$ (auch für $I = \emptyset$).

23.4.24 (3)

1.4. Abbildungen zwischen Mengen. Naives Kategoriekonzept: Objekte und Morphismen. Schreibweise $f : A \to B$, $a \mapsto b$; Abbildungen als spezielle $f \subseteq A \times B$; $\mathrm{id}_A : A \to A$; Verknüpfung $g \circ f$; $f(a) \in B$ für $a \in A$, $f^{-1}(B') \subseteq A$ für $B' \subseteq B$, speziell: $f^{-1}(b) := f^{-1}(\{b\}) \subseteq A$ für $b \in B$ heißen *Fasern*; $f(f^{-1}(B')) \subseteq B'$, $f^{-1}(f(A')) \supseteq A'$; $f^{-1}(B_1) \cup f^{-1}(B_2) = f^{-1}(B_1 \cup B_2)$, $f^{-1}(B_1) \cap f^{-1}(B_2) = f^{-1}(B_1 \cap B_2)$ (für $B_i \subseteq B$); $f(A_1) \cup f(A_2) = f(A_1 \cup A_2)$, $f(A_1) \cap f(A_2) \supseteq f(A_1 \cap A_2)$ (für $A_i \subseteq A$); injektiv, surjektiv, bijektiv; Begriff des Isomorphismus (Invertierbarkeit), inverse Abbildung f^{-1} ("f^{-1}" ist also doppeldeutig); $(f^{-1})^{-1} = f$.

26.4.24 (4, Willem)

Satz 2. *Abbildungen zwischen Mengen sind Isomorphismen $\Leftrightarrow$ sie sind bijektiv.*

(Richtung ($\Leftarrow$) folgt aus $f^{-1}(b) = a :\Leftrightarrow f(a) = b$.)

1.5. Relationen. Relationen: mögliche Eigenschaften Reflexiv, AntiSymmetrisch, Symmetrisch, Transitiv;
Halbordnungen = "Posets", Poset-Homomorphismen, minimale/maximale Elemente, Minima und Maxima in Posets (Beispiele: $\leq$, $\subseteq$, $|$ in $\mathbb{N}$); totale Ordnungen, Wohlordnungen;
Äquivalenzrelationen; Einteilung in Äquivalenzklassen, $\sim$ vs. surjektive Abbildungen $M \twoheadrightarrow M/\!\sim$; Auswahlaxiom. Beispiele: Mächtigkeit, Translationsklassen, Reste mod n, also $\mathbb{Z} \twoheadrightarrow \mathbb{Z}/n\mathbb{Z}$. 30.4.24 (5)

2. Grundkurs: Gruppen, Ringe, Körper

3.5.24 (6)

2.1. Gruppen. Beispiel $S_n \rightsquigarrow$ *Gruppe* G: Nur *eine* Operation mit Assoziativität, neutralem Element und Inversem ($\forall g \in G\ \exists g^{-1} \in G : gg^{-1} = g^{-1}g = e$; ist eindeutig); es folgt $(gh)^{-1} = h^{-1}g^{-1}$.
Bijektive Gruppenhomomorphismen sind Gruppenisomorphismen. Weitere Beispiele für Gruppen: $\mathbb{Z}$; $\mathbb{Z}/n\mathbb{Z}$; $V := \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$; $\mathrm{GL}(2, \mathbb{K})$; $S^1 = \mathbb{R}/\mathbb{Z}$; $\mathbb{C}^* = S^1 \times \mathbb{R}_{>0}$; Einheitengruppe $R^* \subseteq R$ für Ringe R, $\mathbb{Z}^*$, $\mathbb{K}^* = \mathbb{K} \setminus \{0\}$. 7.5.24 (7)
$(\mathbb{Z}/n\mathbb{Z})^*$ mit $\varphi(n) := |(\mathbb{Z}/n\mathbb{Z})^*|$; $\varphi(p^k) = (p-1)p^{k-1}$ und $\varphi(mn) = \varphi(m)\varphi(n)$ für $\gcd(m,n) = 1$ (folgt aus "Chinesischem Restsatz", d.h. der Bijektivität von $\mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$).
$g^{\#G} = 1_G$ in abelschen Gruppen $\Rightarrow$ kleiner Fermat: $\gcd(a,n) = 1 \Rightarrow a^{\varphi(n)} \equiv 1\,(n)$; public key Kryptographie: $n = pq$ mit $p \neq q$ Primzahlen, $k \equiv 1\,(\varphi(n)) \Rightarrow a^k \equiv a\,(n)$.

2.2. Untergruppen. $U \subseteq G$ (Beispiel $n\mathbb{Z} \subseteq \mathbb{Z}$), Gruppenhomomorphismen $\varphi : G \to H$ (Isomorphismen $\Leftrightarrow$ bijektiv); $\ker\varphi$ (Spezialfall von $\varphi^{-1}(V)$), $\operatorname{im}\varphi$ (Spezialfall von $\varphi(U)$); φ ist injektiv $\Leftrightarrow \ker\varphi = \{1_G\}$; *Linksnebenklassen* gU, *Index* $(G : U) := \#(\mathrm{LNK})$.

Satz 3 (Lagrange)**.** *$\#(G) = \#(U) \cdot (G : U)$. Insbesondere gilt $\#(U)|\#(G)$.*

Proof. G ist disjunkte Vereinigung der LNK, und diese sind alle gleichmächtig. □

Folgerung 4. (1) *$g \in G \Rightarrow |g|\big|\#(G)$; insbesondere gilt $g^{\#(G)} = 1_G$.*
(2) *$\#(G) =$ Primzahl p $\Rightarrow G \cong \mathbb{Z}/p\mathbb{Z}$ ("zyklisch").*

Normalteiler (oder "normale Untergruppen") $N \triangleleft G$ ($\forall g \in G : gNg^{-1} \subseteq N$, d.h. Links- und Rechtsnebenklassen stimmen überein) und *Faktorgruppen* $\pi : G \to \to G/N$. Beispiel: Kerne sind Normalteiler, $\{(1), (12)\} \subseteq S_3$ ist eine *nicht* normale Untergruppe.

Satz 5 (Homomorphie-Satz)**.** *Sei $f : G \to H$ ein Gruppenhomomorphismus, sei $N \subseteq \ker f$ Normalteiler in G. Dann gibt genau ein $F : G/N \to H$ mit $f = F \circ \pi$.*

Darüberhinaus ist $\ker F = (\ker f)/N$. *Falls* $N = \ker f$, *dann ist* F *also injektiv, d.h.* $G/\ker f \cong \operatorname{im} f$.

Umformulierung: Für gegebene Normalteiler $N \lhd G \Rightarrow$ erhalten wir eine Bijektion $\{\text{Homomorphismen } G/N \xrightarrow{F} H\} \xrightarrow{\sim} \{\text{Homomorphismen } G \xrightarrow{f} H \text{ mit } N \subseteq \ker f\}$.

$N \lhd G \Rightarrow$ Bijektion $\{\text{Untergruppen } N \subseteq U \subseteq G\} \xrightarrow{\sim} \{\text{Untergruppen } U/N \subseteq G/N\}$; dabei gilt $[U \lhd G \Leftrightarrow U/N \lhd G/N]$ und (falls $U \lhd G$): $(G/N)/(U/N) \cong G/U$.

2.3. S_n **als Beispiel für** $\operatorname{Aut}(X)$**.** $X =$ Objekt in einer Kategorie $\Rightarrow \operatorname{Aut}(X)$ ist "*Automorphismengruppe*"; $S_n := \operatorname{Aut}(\{1, \dots, n\})$. Zyklenschreibweise: $(k_1, \dots, k_\ell) := \begin{pmatrix} k_1 & k_2 & \dots & k_\ell & \text{Rest} \\ k_2 & k_3 & \dots & k_1 & \text{Rest} \end{pmatrix}$; *elementfremde* Zyklen kommutieren (aber: $(i, i+1)(i-1, i) = (i, i-1, i+1)$ und $(i-1, i)(i, i+1) = (i, i+1, i-1)$); jede Permutation läßt sich bis auf Reihenfolge eindeutig als $\boxed{\text{Produkt elementfremder Zyklen}}$ schreiben $\rightsquigarrow$ "Typ einer Permutation" – dieser charakterisiert die Konjugationsklassen in der S_n. $\operatorname{sgn} : S_n \to \{\pm 1\}$ mittels $\operatorname{sgn}(\pi) := \prod_{\#\{i,j\}=2} (\pi(j) - \pi(i))/(j - i)$; man erhält $\operatorname{sgn}(\sigma\pi) = \prod (\sigma\pi(j) - \sigma\pi(i))/(\pi(j) - \pi(i)) \cdot (\pi(j) - \pi(i))/(j - i) = \operatorname{sgn}(\sigma) \operatorname{sgn}(\pi)$ und $[k\text{-Zyklus}] \mapsto (-1)^{k-1}$ (Induktion mit $(a_1 \dots a_{k-1})(a_{k-1} a_k) = (a_1 \dots a_k)$).

2.4. Ringe. *Ring* R *mit* 1: Operationen "+" und "$\cdot$" mit Axiomen (Assoziativität und neutrales Element für beide, Kommutativität und Existenz von Inversen für "+", Distributivgesetze). Es folgt z.B. $0_R \cdot a = a \cdot 0_R = 0_R$. Ring-Homomorphismen. Beispiele: $\mathbb{Z}$; $\mathbb{Z}/n\mathbb{Z}$; $R[x_1, \dots, x_n]$; *Körper* $\mathbb{K} = \mathbb{Q}, \mathbb{R}, \mathbb{C}$; $\mathbb{M}(n, R)$.

Nullteiler; $\boxed{\operatorname{char} R}$ (ist 0 oder Primzahl bei *Integritätsbereichen*, d.h. bei kommutativen Ringen ohne Nullteiler).

Ringhomomorphismen; $\mathbb{Z}/a\mathbb{Z} \to \mathbb{Z}/b\mathbb{Z} \Leftrightarrow b|a$, Ringhomomorphismen sind Isomorphismen $\Leftrightarrow$ bijektiv, Chinesischer Restsatz, $\mathbb{Z}/4\mathbb{Z} \ncong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
Beispiele: $\mathbb{K}[x, y] \to \mathbb{K}$, $f \mapsto f(3, 7)$, aber $\det : \mathbb{M}(2, \mathbb{R}) \to \mathbb{R}$ und $(\cdot 2) : \mathbb{Z} \to \mathbb{Z}$ sind keine Ringhomomorphismen.

Ideale als die Objekte, nach denen faktorisiert werden darf (treten als Kerne von Ringhomomorphismen auf); triviale Ideale $(0) = \{0\}$, $(1) = R$; Homomorphiesatz; Ideale in R/I. *Körper* haben nur die trivialen Ideale (0) und (1); Beispiel $\mathbb{F}_4 := \mathbb{F}_2[x]/(x^2 + x + 1)$.

Literatur

[Art] Artin, M.: Algebra.

[Bri] Brieskorn, E.: Lineare Algebra und analytische Geometrie.

[Ch] Cheng, Eugenia: Cakes, Custard and Category Theory. Profile Books, 2015.

[Ebb] Ebbinghaus et al.: Zahlen. Springer-Verlag 1992.

[Fis] Fischer, G.: Lineare Algebra.

[Giv] Givental, Alexander: Linear Algebra and Differential Equations. American Mathematical Society, Berkeley Center for Pure and Applied Mathematics, 2001. `http://math.berkeley.edu/~giventh/papers/ode.pdf`

[Kli] Klingenberg, W.: Lineare Algebra und Geometrie.
[Kd] Kochendörffer, R.: Einführung in die Algebra.
[Kow] Kowalsky, H.J.: Lineare Algebra.
[La2] Lang, S.: Linear algebra.
[La3] Lang, S.: Algebra.

Klaus Altmann
Mathematisches Institut
Freie Universität Berlin
Tel.: (030) 838 - 75428
altmann@math.fu-berlin.de

Willem van Zuijlen
WIAS
vanzuijlen@wias-berlin.de

"Lineare Algebra I "
FUB, Sommer 2024
Tutoren: Laura Weyers,
Christopher Huggle

1. Aufgabenblatt zum 26.4.24

Aufgabe 1. Zeigen Sie, daß es für natürliche Zahlen $a \in \mathbb{N}$ und $b \in \mathbb{Z}_{\geq 1}$ stets ein $r \in \mathbb{N}$ mit $0 \leq r < b$ und ein $q \in \mathbb{N}$ gibt, so daß $a = q \cdot b + r$ gilt. Benutzen Sie dabei, daß jede nichtleere Teilmenge $S \subseteq \mathbb{N}$ immer ein kleinstes Element besitzt (genannt $\min(S)$).

Tip: Nehmen Sie b als gegeben an und betrachten Sie die Menge aller Zahlen a, die *nicht* solch eine Division mit Rest erlauben.

Solution: Sei $b \in \mathbb{Z}_{\geq 1}$ gegeben. Wir definieren

$$S = S(b) := \{a \in \mathbb{N} \,|\, \text{es gibt } \textit{keine } q \in \mathbb{N} \text{ und } r \in \mathbb{N} \cap [0, b) \text{ mit } a = q \cdot b + r\}.$$

Falls $S \neq \emptyset$, so sei $a_0 := \min(S)$. Da $0 = 0 \cdot b + 0$ gilt, folgt $0 \notin S$, d.h. $a_0 \neq 0$. Wir können somit

$$a := a_0 - 1 \in \mathbb{N}$$

betrachten. Damit folgt sofort, daß $a \notin S$ gelten muß. Insbesondere gibt es eine Darstellung

$$a_0 - 1 = a = q \cdot b + r$$

mit $q \in \mathbb{N}$ und $r \in \{0, \ldots, b-1\}$. Daraus folgt aber

$$a_0 = q \cdot b + (r + 1),$$

und wir unterscheiden zwei Fälle: (1) Falls $r \leq b - 2$, dann ist $r + 1 \leq b - 1$, und der Beweis ist beendet. Fall $r = b - 1$, so folgt $a_0 = q \cdot b + b = (q + 1) \cdot b + 0$, und wir sind ebenfalls fertig.

Aufgabe 2. a) Bestimmen Sie den $\mathrm{ggT}(723, 612)$ und stellen Sie ihn als Linearkombination der beiden Zahlen 723 und 612 dar, d.h., bestimmen Sie ganze Zahlen $x, y \in \mathbb{Z}$ mit $723\,x + 612\,y = \mathrm{ggT}(723, 612)$.

b) Sind die Zahlen $x, y \in \mathbb{Z}$ eindeutig bestimmt? Wenn nicht, können Sie sogar *alle* Lösungen $(x, y) \in \mathbb{Z}^2$ der Gleichung $723\,x + 612\,y = \mathrm{ggT}(723, 612)$ bestimmen?

Solution: (a) Eine Variante des Euklidischen Algorithmus' erlaubt die Benutzung der etwas entspannteren Version der Division mit Rest $a = q \cdot b \pm r$ mit $r \in \{0, 1, \ldots, b-1\}$. Damit verkürzen sich manchmal die Rechnungen. Hier bekommen wir

$$\begin{aligned} 723 &= 1 \cdot 612 + 111 \\ 612 &= 5 \cdot 111 + 57 \\ 111 &= 2 \cdot 57 - 3, \end{aligned}$$

und die nächste Zeile liefert 0 in der rechten unteren Ecke. Damit ist $\mathrm{ggT}(723, 612) = 3$, und wir erhalten $3 = 2 \cdot \underline{57} - \underline{111} = 2 \cdot (\underline{612} - 5 \cdot \underline{111}) - \underline{111} = 2 \cdot \underline{612} - 11 \cdot \underline{111} = 2 \cdot \underline{612} - 11 \cdot (\underline{723} - \underline{612}) = 13 \cdot \underline{612} - 11 \cdot \underline{723}$.

b) Mit $ax + by = d$ gilt auch $ax' + by' = d$, wenn $x' = x - b$ und $y' = y + a$ ist. Die Koeffizienten $x, y \in \mathbb{Z}$ sind also *nicht* eindeutig bestimmt. Falls, o.B.d.A. $d = 1$ gilt (sonst dividiere man die gesamte Gleichung durch d), dann erhält man folgende Gesamtlösung:

Ist $ax + by = 1 = ax' + by'$, so folgt $a(x - x') = b(y' - y)$ und somit $a|(y' - y)$ und $b|(x - x')$ (denn a und b sind wegen $d = 1$ teilerfremd). Damit ergeben sich *alle* Lösungen (x, y) aus *einer* Lösung (x_0, y_0) mittels $x = x_0 + kb$, $y = y_0 - ka$ für beliebige $k \in \mathbb{Z}$.

Aufgabe 3. Man programmiere in einer beliebigen Programmiersprache den Euklidischen Algorithmus: Die Eingabe ist $a, b \in \mathbb{Z}$ (oder $a, b \in \mathbb{Z}_{\geq 1}$), die Ausgabe sind drei Zahlen $d = \gcd(a, b) \in \mathbb{N}$ ($\gcd = $ ggT bezeichne den größten gemeinsamen Teiler) und $x, y \in \mathbb{Z}$ mit $ax + by = d$.

Solution: Wir erstellen eine rekursive Prozedur für $d(a, b)$, $x(a, b)$ und $y(a, b)$. Zuerst dividiere man mit Rest: $a = q \cdot b + r$ (die Zahlen q und r sind oft schon als $div(a, b)$ und $mod(b, a)$ implementiert).

Falls $r = 0$, so geben wir aus: $d(a, b) := b$ und $x(a, b) := 0$ und $y(a, b) := 1$.

Sonst ist $d(a, b) := d(b, r)$ und $x(a, b) := y(b, r)$ und $y(a, b) := x(b, r) - q \cdot y(b, r)$.

Aufgabe 4. Seien B, C Teilmengen einer Menge A. Gilt dann $A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$? Falls nicht, ist wenigstens eine der beiden Seiten in der anderen enthalten? (Geben Sie jeweils einen Beweis oder ein Gegenbeispiel.)

Solution: Die Gleichheit ist richtig. Beweis: Sei $a \in A \setminus (B \cap C)$. Dann ist $a \notin B \cap C$, d.h. o.B.d.A. können wir annehmen, daß $a \notin B$. Daraus folgt $a \in A \setminus B$, d.h. a ist ein Element der rechten Seite.
Für die andere Richtung sei o.B.d.A. $a \in A \setminus B$. Wegen $B \cap C \subseteq B$ folgt dann aber direkt $a \in A \setminus (B \cap C)$.

Klaus Altmann
Mathematisches Institut
Freie Universität Berlin
Tel.: (030) 838 - 75428
altmann@math.fu-berlin.de

Willem van Zuijlen
WIAS
vanzuijlen@wias-berlin.de

"Lineare Algebra I "
FUB, Sommer 2024
Tutoren: Laura Weyers,
Christopher Huggle

2. Aufgabenblatt zum 3.5.24

Aufgabe 5. Sei $f : M \to N$ eine Abbildung, und seien $A \subseteq M$ und $B \subseteq N$ Teilmengen.

a) Zeigen Sie die Inklusionen $f(f^{-1}(B)) \subseteq B$, $f^{-1}(f(A)) \supseteq A$.

b) Geben Sie für beide Inklusionen Beispiele (konkrete Abbildungen f), die belegen, daß die Gleichheit i.a. nicht gilt.

Aufgabe 6. Sei $f : M \to N$ eine Abbildung, und seien $A, A' \subseteq M$ und $B, B' \subseteq N$ Teilmengen. Zeigen Sie dann die Gleichungen $f^{-1}(B) \cup f^{-1}(B') = f^{-1}(B \cup B')$, und $f(A) \cup f(A') = f(A \cup A')$.

Aufgabe 7. Seien $f : L \to M$ und $g : M \to N$ Abbildungen.

a) Zeigen Sie, daß aus der Surjektivität von f und g die Surjektivität von $g \circ f$ folgt.

b) Zeigen Sie, daß aus der Surjektivität von $g \circ f$ die Surjektivität von g folgt.

c) Sei $f : L \to M$ eine surjektive Abbildung. Man zeige, daß dann ein sogenannter Schnitt existiert, d.h. eine (injektive) Abbildung $s : M \hookrightarrow L$ mit $g \circ s = \mathrm{id}_M$.

Aufgabe 8. Sei $(M, \leq)$ eine "poset", d.h. eine Menge mit einer Halbordnung, d.h. Halbordnungsrelation "$\leq$". Wir sagen, daß ein Element $a \in M$ "*minimal*" ist, falls es kein von a verschiedenes Element $b \in M$ gibt mit $b \leq a$. Wir sagen, daß ein Element $x \in M$ das (!) "*Minimum*" von M ist (und nennen es $x = \min(M) = \min(M, \leq)$), falls für alle $y \in M$ die Relation $x \leq y$ gilt.

a) Was ist die genaue Beziehung zwischen diesen beiden Begriffen? Sind sie gleich – oder impliziert wenigstens einer den anderen? (Beweis/Gegenbeispiel). Was bedeutet das Wort "das" im obigen Text?

b) Sei $M := \mathbb{N}$ mit der Teilbarkeitsrelation, d.h. wir *definieren* $a \leq b :\Leftrightarrow a|b$. ($a \leq b$ bedeutet in dieser Aufgabe also *nicht* die übliche kleinerGleich-Relation.) Bestimmen Sie alle minimalen Elemente und alle Minima in $(\mathbb{N}, |)$ (also in $\mathbb{N}$ bzgl. der Teilbarkeitsrelation).

c) Analog zu den Begriffen "*minimal*" und "*Minimum*" kann man die Begriffe "*maximal*" und "*Maximum*" definieren. Bestimmen Sie alle maximalen Elemente und alle Maxima in $(\mathbb{N}, |)$.

d) Lösen Sie die Teilaufgaben (b) und (c) für $(\mathbb{N}_{\geq 2}, |)$ statt $(\mathbb{N}, |)$.

Klaus Altmann
Mathematisches Institut
Freie Universität Berlin
Tel.: (030) 838 - 75428
altmann@math.fu-berlin.de

Willem van Zuijlen
WIAS
vanzuijlen@wias-berlin.de

"Lineare Algebra I "
FUB, Sommer 2024
Tutoren: Laura Weyers,
Christopher Huggle

3. Aufgabenblatt zum 10.5.24

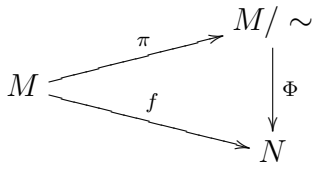
Aufgabe 9. Benutzen Sie die Idee der Russellschen Antinomie, um zu zeigen, daß eine Menge M *nie* gleichmächtig zu ihrer Potenzmenge 2^M sein kann. D.h. führen Sie die Existenz einer bijektiven (oder sogar nur *surjektiven*) Abbildung $\varphi : M \twoheadrightarrow 2^M$ zum Widerspruch. (Gibt es *injektive* Abbildungen $M \hookrightarrow 2^M$?)

Aufgabe 10. Sei M eine Menge, $\sim$ eine Äquivalenzrelation auf M und $\pi : M \to \to M/\sim$ die zugehörige Surjektion auf den Quotienten, d.h. auf die Menge aller Äquivalenzklassen.

a) Sei $f : M \to N$ eine Abbildung mit der Eigenschaft, daß $f(a) = f(b)$ für alle $a, b \in M$ mit $a \sim b$ gilt. Zeigen Sie, daß es dann genau eine (!) Abbildung

$$\Phi : M/\sim \longrightarrow N$$

gibt mit $\Phi \circ \pi = f$. Für diese Gleichheit sagen wir, daß das Diagramm



kommutiert.

b) Zeigen Sie, daß Φ genau dann injektiv ist, wenn für alle $a, b \in M$ gilt:

$$a \sim b \iff f(a) = f(b).$$

c) Zeigen Sie, daß Φ genau dann surjektiv ist, wenn f surjektiv ist.

d) Für Mengen A, B bezeichne $\mathrm{Abb}(A, B)$ die Menge aller Abbildungen von A nach B. Wir erhalten damit für jede Menge N eine "natürliche"/"kanonische" Abbildung

$$\begin{array}{ccc} \mathrm{Abb}(M/\sim, N) & \longrightarrow & \{f \in \mathrm{Abb}(M,N) \mid f(a) = f(b) \text{ für } a \sim b\} \\ \Phi & \mapsto & \Phi \circ \pi. \end{array}$$

Zeigen Sie, daß diese Abbildung bijektiv ist.

Aufgabe 11. a) Definieren Sie auf $\mathbb{Z}/n\mathbb{Z}$ ein Produkt (und überprüfen Sie insbesondere die Korrektheit Ihrer Definition), so daß für die kanonische Abbildung $\pi : \mathbb{Z} \twoheadrightarrow \mathbb{Z}/n\mathbb{Z}$ die Gleichung

$$\pi(a) \cdot \pi(b) = \pi(ab)$$

gilt.

b) Gibt es für diese Produktdefinition mehrere Möglichkeiten, oder ist sie eindeutig? Ist Ihr Produkt auf $\mathbb{Z}/n\mathbb{Z}$ assoziativ, kommutativ? Erfüllt es das Distributivgesetz mit der Addition?

Aufgabe 12. a) Bezeichne $\overline{a}$ (oder $[a]$) die Restklasse von a in $\mathbb{Z}/n\mathbb{Z}$. Welche der Gleichungen $\overline{6} \cdot x = \overline{5}$ oder $\overline{6} \cdot y = \overline{4}$ oder $\overline{5} \cdot z = \overline{1}$ sind in $\mathbb{Z}/8\mathbb{Z}$ lösbar? Und falls eine der Gleichungen lösbar ist – sind die Lösungen in $\mathbb{Z}/8\mathbb{Z}$ eindeutig?

b) Seien $n \in \mathbb{N}_{\geq 1}$ und $a \in \mathbb{Z}$ mit $\mathrm{ggT}(a, n) = 1$. Nutzen Sie Aufgabe 2, um die Kongruenz $ax \equiv 1 \pmod{n}$ in $\mathbb{Z}$, bzw. die Gleichung $\overline{a} \cdot x = \overline{1}$ in $\mathbb{Z}/n\mathbb{Z}$ zu lösen.

Gemeint ist: Zeigen Sie, daß diese Gleichung eine eindeutige Lösung hat. Wir bezeichnen die eindeutige Lösung x dann als $1/\overline{a} \in \mathbb{Z}/n\mathbb{Z}$.

c) Berechnen Sie $1/\overline{9}$ in $\mathbb{Z}/22\mathbb{Z}$.