ALG Ü8

16b) zz: Für die eulersche φ-Funktion und $n \in \mathbb{N}^+$ gilt $n = \sum_{t|n} \varphi(t)$

$$\varphi(n) := |\{k \in \mathbb{N} : 0 \leq k < n,\ ggT(k,n) = 1\}|$$

Für die zyklische Gruppe $C_t = \mathbb{Z}/t\mathbb{Z}$ gibt es $\varphi(t)$ Erzeuger der ganzen Gruppe. Das folgt aus Proposition 3.2.4.10 ($g \in G$ mit $ord(g) < \infty$ $\Rightarrow ord(g^k) = \frac{ord(g)}{ggT(ord(g),k)}$)

$1 \in C_t$, $ord(1) = t < \infty \Rightarrow ord(k \cdot 1) = \frac{ord(1)}{ggT(ord(1),k)} = \frac{t}{ggT(t,k)}$

Für $k \in \{0, \dots, t-1\}$ gilt

1. Fall $ggT(t,k) = 1$: $ord(k \cdot 1) = t \Rightarrow \langle k \cdot 1 \rangle = C_t$

2. Fall $ggT(t,k) \neq 1$: $ord(k \cdot 1) \neq t \Rightarrow \langle k \cdot 1 \rangle \subsetneqq C_t$

$\Rightarrow \exists\ \varphi(t)$ verschiedene Erzeuger von C_t

Aus Satz 3.2.4.8. folgt, dass jede Untergruppe $C_x \cong \langle t \cdot 1 \rangle \leq C_n$ von einem Teiler t von n erzeugt wird.

Für jeden Teiler t von n gibt es eine Untergruppe U mit $ord(U) = t$, nämlich $U = \langle \frac{n}{k} \cdot 1 \rangle$ mit $k \in \mathbb{Z} : k \cdot t = n$ (existiert da t Teiler von n).

Da $U \cong C_t$ gibt es nach oben $\varphi(t)$ Erzeuger von U.

Da für alle $t \in \{0, \dots, n-1\}$: $\langle t \cdot 1 \rangle$ eine Untergruppe erzeugt muss die Summe aller Erzeuger aller Untergruppen von C_n gleich n sein.

$\Rightarrow \sum_{t|n} \varphi(t) = n$

$\square$

ALG Ü8

198) zz: $\varphi(n) = \prod_{i=1}^{k} (p_i - 1)\, p_i^{e_i - 1}$ mit $n = \prod_{i=1}^{k} p_i^{e_i}$, $k \in \mathbb{N}$, $p_i \in \mathbb{P}$

$\forall i,j,\ i \neq j : p_i \neq p_j$, $e_i \in \mathbb{N}^+$

1) Fall $n = p^e$ $\Rightarrow k = 1,\ p_1 = p,\ e_1 = e$ zz: $\varphi(n) = (p-1)\, p^{e-1}$

$(p-1)\,p^{e-1} = p^{e} - p^{e-1} = n - p^{e-1}$

$\{k \in \mathbb{N} : 0 \leq k < n,\ ggT(k,n) \neq 1\}$ sind genau Elemente der Form $a \cdot p$ mit $a \in \{0, 1, \dots, p^{e-1} - 1\}$, da p der einzige Primfaktor von n ist.

$\Rightarrow \varphi(n) = n - |\{k \in \mathbb{N} : 0 \leq k < n,\ ggT(k,n) \neq 1\}| = n - |\{0, 1, \dots, p^{e-1} - 1\}| = n - p^{e-1}$

2) zz: k ...prim mod m $\Leftrightarrow$ $\bar{k}$ ... Einheit von $(\mathbb{Z}_m, \cdot)$

$\Rightarrow$ nach 3.2.4.2. gilt $\bar{1} = \bar{k} \cdot \bar{a}$ also $k \cdot a = 1 + m\mathbb{Z}$ $\Leftrightarrow$

$ggT(k,a) \mid 1 + m\mathbb{Z}$ also $ggT(\bar{k}, \bar{a}) \mid \bar{1}$, da k prim mod m

gilt $\forall \bar{a} \in \mathbb{Z}_m \setminus \{\mathbb{Z}\bar{k}\} : ggT(\bar{k}, \bar{a}) = \bar{1}$ für $m \geq 3$ ...

ALG Ü8

290) $\mathcal{K}$ ... Klasse von Algebren selben Typs $\quad S\mathcal{K}=\mathcal{K} \quad \mathcal{F}\in\mathcal{K}$

$X \subseteq F \qquad$ (1) $\forall \mathcal{A}\in\mathcal{K}\ \forall j: X \to A\ \exists \varphi: \mathcal{F}\to\mathcal{A}$ ... Homomorphismus, $j \subseteq \varphi$

(2) $\mathcal{F}$ wird von X erzeugt also $\nexists\, U \subsetneq \mathcal{F} : X \subseteq U$

zz: $\mathcal{F}$ ... frei über $X \iff (1) \wedge (2)$

($\Leftarrow$) Es ist nur mehr zu zeigen, dass φ eindeutig ist, das folgt aus $\langle X\rangle = F$ und Proposition 2.3.1.13.

($\Rightarrow$) (1) klar, da sogar ein eindeutiges φ existiert

(2) Sei $\mathcal{F}_0 \subseteq \mathcal{F}$ mit $X \subseteq \mathcal{F}_0$ bel. $\qquad$ zz: $F_0 = F$

$$\begin{tikzcd}
 & \mathcal{F} \arrow[d, dashed, "\varphi"] \arrow[dd, bend left=60, "id_F"] \\
X \arrow[ur, "id_X"] \arrow[r, "id_X"] \arrow[dr, "id_X"'] & \mathcal{F}_0 \arrow[d, "id_{F_0}"] \\
 & \mathcal{F}
\end{tikzcd}$$

φ ist Hom.

$\exists!\, \varphi: \mathcal{F}\to\mathcal{F}_0 : id_X = \varphi \circ id_X$ da $\mathcal{F}$ frei über X

id_{F_0} ist ein Homomorphismus von $\mathcal{F}_0$ nach $\mathcal{F}$

id_F ist Hom. von $\mathcal{F}$ nach sich selbst (sogar eindeutig mit $id_X: X\to F$ vorgegeben)

Es gilt $\quad id_F = id_{F_0} \circ \varphi$

$\Rightarrow \varphi(F) \subseteq F_0 \wedge \varphi(F) = id_{F_0}(\varphi(F)) = id_F(F) \qquad \Rightarrow F \subseteq F_0$

und da auch $F_0 \subseteq F \Rightarrow F_0 = F$

$\square$

ALG Ü8

292) Beschreiben Sie freie Objekte über einer beliebigen vorgegebenen Menge X in der Kategorie Ab der abelschen Gruppen.

Nach UE 290 bzw. Lemma 4.1.2.2. gilt:

Da Ab unter Unteralgebren abgeschlossen ist gilt für $\mathfrak{F} \in Ab$ mit $X \subseteq F$

$\mathfrak{F}$... frei über X $\Longleftrightarrow$ (1) $\forall \mathcal{A} \in Ab\ \forall j: X \to A\ \exists \varphi: \mathfrak{F} \to \mathcal{A}$ .. Hom mit $j \subseteq \varphi$

(2) $\mathfrak{F}$ wird von X erzeugt

Also kommt für gegebenes X nur $\mathfrak{F} = \langle X \rangle$ in Frage.

(2) wird trivialerweise erfüllt.

zz: (1) Sei $\mathcal{A} \in Ab$, $j: X \to A$ bel. Sei $f \in F$ bel.

$\Rightarrow \exists t \in \mathbb{T}\ \exists x_1, \dots, x_n \in X : f = t(x_1, \dots, x_n)$

$\varphi(f) = \varphi(t(x_1, \dots, x_n)) = t(\varphi(x_1), \dots, \varphi(x_n)) = t(j(x_1), \dots, j(x_n))$

φ setzt j fort zz: wohldefiniert

$t(x_1, \dots, x_n) = t'(x_1, \dots, x_n)$ (mit genügend großem n, es müssen nicht alle x_i verwendet werden)

$\Rightarrow$ aus UE 297, dass $\forall \mathcal{A} \in Ab: \mathcal{A} \models t \approx t'$

$\Rightarrow t(j(x_1), \dots, j(x_n)) = t'(j(x_1), \dots, j(x_n))$ also ist φ wohldefiniert

φ ist Hom. nach Definition

$\Rightarrow \mathfrak{F}$ ist frei über X

$\Rightarrow$ genau $\langle X \rangle$ ist frei über X in der Kategorie Ab

ALG Ü8

297) $t(x_1,\dots,x_n)$, $t'(x_1,\dots,x_n)$ ... Terme in fester Sprache L

$\mathcal{V}$ ... Varietät zu Sprache L $\qquad$ $F \in \mathcal{V}$ ... frei über $\{b_1,\dots,b_n\} \overset{X}{=}$ in $\mathcal{V}$

(a) In F gilt $t(b_1,\dots,b_n) = t'(b_1,\dots,b_n)$

(b) $\forall C \in \mathcal{V}: C \models t \approx t'$

(c) $F \models t \approx t'$ $\qquad$ zz: (a) $\Leftrightarrow$ (b) $\Leftrightarrow$ (c)

(b) $\Rightarrow$ (c) klar, da $F \in \mathcal{V}$

(c) $\Rightarrow$ (a) $F \models t \approx t' \Rightarrow \forall f_1,\dots,f_n \in F: t(f_1,\dots,f_n) = t'(f_1,\dots,f_n)$

Da $\{b_1,\dots,b_n\} \subseteq F \Rightarrow t(b_1,\dots,b_n) = t'(b_1,\dots,b_n)$

(a) $\Rightarrow$ (b) Sei $C \in \mathcal{V}$ bel.

$$\begin{array}{ccc} X & \xrightarrow{id_X} & F \\ & \searrow^{j} & \downarrow \varphi \\ & & C \end{array}$$

Sei $c_1,\dots,c_n \in C$ bel.

$j: X \to C$, $\quad b_i \mapsto c_i \quad \forall i \in \{1,\dots,n\}$ $\Rightarrow \exists! \varphi: F \to C$ .. Hom. $j = \varphi \circ id_X = \varphi$

$t(c_1,\dots,c_n) = t(j(b_1),\dots,j(b_n)) = t(\varphi(b_1),\dots,\varphi(b_n)) \overset{*}{=} \varphi(t(b_1,\dots,b_n)) = \dots$

* folgt aus Prop. 2.3.3.21

$\dots = \varphi(t'(b_1,\dots,b_n)) \overset{*}{=} t'(\varphi(b_1),\dots,\varphi(b_n)) = t'(c_1,\dots,c_n)$

$\Rightarrow C \models t \approx t'$

$\square$

ALG Ü8

2008) K ... Varietät von Algebren oder Klasse aller Körper

$(R_n)_{n\in\mathbb{N}}$ ... Familie von Algebren in K $\quad$ $(f_n)_{n\in\mathbb{N}}$ ... Familie mit

$\forall n\in\mathbb{N}: f_n: R_n \to R_{n+1}$ ... Homomorphismus

Satz 2342: $\exists$ bis auf Isomorphie eindeutige Algebra $R_\infty \in K$ und

Homomorphismen $f_n^\infty: R_n \to R_\infty$ mit

$\forall B\in K\ \forall (\varphi_n)_{n\in\mathbb{N}}$ ... Hom. von R_n nach B mit $\forall n: \varphi_n = \varphi_{n+1}\circ f_n$ gilt

$\exists!\ \varphi: R_\infty \to B$ ... Hom. mit $\forall n: \varphi\circ f_n^\infty = \varphi_n$

(Es gilt $R_\infty = \bigcup_{n\in\mathbb{N}} f_n^\infty(R_n)$)

ges: Kategorie $\mathcal{C}$, sodass $\exists$ initiales Element in C ist Umformulierung von Folgerung in Satz 2342.

$Ob(\mathcal{C}) = C := K$ $\qquad$ $Hom(\mathcal{C}) =$

$$\begin{tikzcd}
\vdots \\
R_{n+1} \arrow[u] \arrow[r, "f_{n+1}^\infty"] \arrow[dr, "\varphi_{n+1}" near start] & R_\infty \arrow[d, dashed, "\varphi"] \\
R_n \arrow[u, "f_n"] \arrow[ur, "f_n^\infty"'] \arrow[r, "\varphi_n"] & B \\
\vdots \arrow[u]
\end{tikzcd}$$

R_∞ ist initiales Obj

$\Leftrightarrow \forall B\in C\ \exists!\ \varphi: R_\infty \to B$

ALG Ü8

200 g)

$$\begin{tikzcd} & Y & \\ C_2 \arrow[ur, "f_1"] \arrow[r, "\iota_1"'] & C \arrow[u, dotted, "f"] & C_2 \arrow[ul, "f_2"'] \arrow[l, "\iota_2"] \end{tikzcd}$$

K ... Klasse aller Gruppen

(C, ι_1, ι_2) ... Koprodukt von C_2 mit C_2

also $\forall Y$ ... Gr. $\forall f_1, f_2 : C_2 \to Y \ \exists! f : C \to Y$

mit $f_1 = f \circ \iota_1$ und $f_2 = f \circ \iota_2$

zz: $|C| = \infty$ und C ... nicht kommutativ

Nach Hinweis: $A := \{(x,y) \in \mathbb{Z}^2 : |x-y| = 1\}$

G ... Menge der Automorphismen der relationalen Struktur $(\mathbb{Z}, A)$

$C := (G, \circ, id, ^{-1})$ ... Gruppe

$C_2 := (\{\overline{0}, \overline{1}\}, +, \overline{0}, -)$ ... Gruppe

$\iota_1(\overline{0}) := id$ $\qquad$ $\iota_2(\overline{0}) := id$

$\iota_1(\overline{1}) := s : \mathbb{Z} \to \mathbb{Z}, \ x \mapsto -x$ $\qquad$ $\iota_2(\overline{1}) := v : \mathbb{Z} \to \mathbb{Z}, \ x \mapsto -(x+1)$

Sei $x, y \in \mathbb{Z}$ mit $|x-y| = 1$ bel.

$\Rightarrow |s(x) - s(y)| = |-x-(-y)| = |y-x| = 1 \qquad \Rightarrow s \in G$

$\Rightarrow |v(x) - v(y)| = |-(x+1)+(y+1)| = |y-x\cancel{+1}\cancel{-1}| = 1 \qquad \Rightarrow v \in G$

Da $\overline{1} + \overline{1} = \overline{0}$ in C_2 muss auch

$\iota(\overline{1}) \circ \iota(\overline{1}) = \iota(\overline{1}+\overline{1}) = \iota(\overline{0}) = id$ für ι_1 und ι_2 gelten.

$(\iota_1(\overline{1}) \circ \iota_1(\overline{1}))(x) = \iota_1(\overline{1})(-x) = x$; $\iota_2(\overline{1})(-(x+1)) = -(-(x+1)+1) = x$

$\Rightarrow \iota_1, \iota_2$ ... Hom. von C_2 nach C

Behauptung: $G = \langle\{s, v\}\rangle$ $\quad$ jeder Homomorphismus in G wird bereits durch das Bild der 1 festgelegt. $s \circ v = x \mapsto x+1$; $\underbrace{(s \circ v) \circ \ldots \circ (s \circ v)}_{k\text{-mal}} = x \mapsto x+k \ \forall k \in \mathbb{N}$

$s \circ ((s \circ v) \circ \ldots \circ (s \circ v)) = x \mapsto -x-k \ \forall k \in \mathbb{N}$ also gibt es Verknüpfungen von s und v sodass 1 auf jeden bel. Wert abgebildet wird.

$\Rightarrow f$ wird eindeutig durch das Bild der $\overline{1}$ von f_1 und f_2 festgelegt.

Also ist C Koprodukt von C_2 mit C_2 und bereits bekannt ist $|C| = \infty$ und C ist nicht kommutativ. (bis auf Isomorphie eindeutig?!) $\square$