

ALG Ü8

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

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

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 $\text{ord}(g) < \infty$
 $\Rightarrow \text{ord}(g^k) = \frac{\text{ord}(g)}{\text{ggT}(\text{ord}(g), k)}$)

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

Für $k \in \{0, \dots, t-1\}$ gilt

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

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

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

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

Für jeden Teiler t von n gibt es eine Untergruppe U mit $\text{ord}(U) = t$, 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.

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



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

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

$\{k \in \mathbb{N}; 0 \leq k < n, \text{ggT}(k, n) \neq 1\}$ 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.

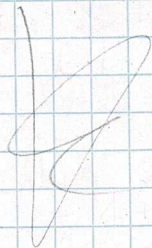
$$\Rightarrow \varphi(n) = n - |\{k \in \mathbb{N}; 0 \leq k < n, \text{ggT}(k, n) \neq 1\}| = n - |\{0, 1, \dots, p^{e-1} - 1\}| = n - p^{e-1}$$

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

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

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

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



Alg Ü8

290) K ... Klasse von Algebren selber Typs $SK = K$ $F \in K$

$X \subseteq F$ (1) $\forall A \in K \forall j: X \rightarrow A \exists \varphi: F \rightarrow A$... Homomorphismus, $j \subseteq \varphi$

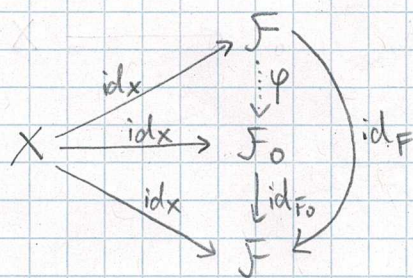
(2) F wird von X erzeugt also $\exists U \subseteq F: X \subseteq U$

zz: F frei über $X \Leftrightarrow (1) \wedge (2)$

(\Leftarrow) Es ist nun 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 $F_0 \subseteq F$ mit $X \subseteq F_0$ bel. zz: $F_0 = F$



φ ist Hom.

$\exists! \varphi: F \rightarrow F_0: id_X = \varphi \circ id_X$ da F frei über X

id_{F_0} ist ein Homomorphismus von F_0 nach F

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

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

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

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



ALG 08

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

Nach UE 290 bzw. Lemma 4.1.2.2. gilt:

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

F ... frei über $X \Leftrightarrow (1) \forall A \in \mathbf{Ab} \forall j: X \rightarrow A \exists \varphi: F \rightarrow A$ Hom mit $j \subseteq \varphi$

(2) F wird von X erzeugt

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

(2) wird trivialerweise erfüllt.

zz: (1) Sei $A \in \mathbf{Ab}$, $j: X \rightarrow A$ 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

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

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

$$\Rightarrow t(j(x_1), \dots, j(x_n)) = t'(j(x_1), \dots, j(x_n)) \quad \text{also ist } \varphi \text{ wohldefiniert}$$

φ ist Hom. nach Definition

$\Rightarrow F$ ist frei über X

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

ALG 08

297) $t(x_1, \dots, x_n), t'(x_1, \dots, x_n)$ Terme in fester Sprache L
 V ... Varietät zu Sprache L $F \in V$... frei über $\{b_1, \dots, b_n\}$ in V

\Rightarrow (a) $\Delta \models F$ gilt $t(b_1, \dots, b_n) = t'(b_1, \dots, b_n)$

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

(c) $F \models t \approx t'$

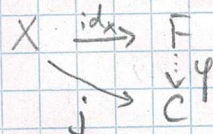
zz: (a) \Leftrightarrow (b) \Leftrightarrow (c)

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

(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 $C \in V$ bel.



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

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

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

* folgt aus Prop. 2.3.3.2.1

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

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

□

ALG Ü8

2008) \mathcal{K} -Varietät von Algebren oder Klasse aller Körper

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

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

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

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

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

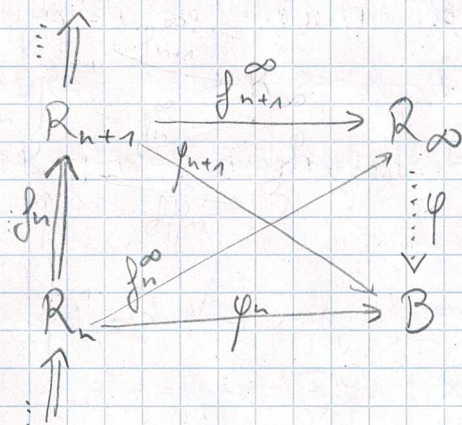
$\exists! \varphi: R_\infty \rightarrow B$... Hom. mit $\forall n: \varphi \circ f_n^\infty = \varphi_n$

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

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

$$\text{Ob}(\mathcal{C}) = \mathcal{C} = \mathcal{K}$$

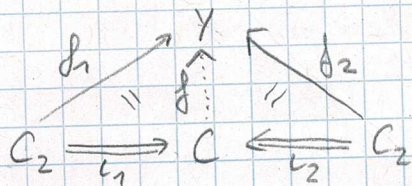
$$\text{Hom}(\mathcal{C}) =$$



R_∞ ist initiales Obj
 $\Leftrightarrow \forall B \in \mathcal{C} \exists! \varphi: R_\infty \rightarrow B$

ALG 08

2009)



$\mathbb{Z}\mathbb{Z}: |C| = \infty$ und C nicht kommutativ

$K \dots$ Klasse aller Gruppen

$(C, l_1, l_2) \dots$ Koproduct von C_2 mit C_2

also $\forall Y \dots G. \forall f_1, f_2: C_2 \rightarrow Y \exists! f: C \rightarrow Y$

mit $f_1 = f \circ l_1$ und $f_2 = f \circ l_2$

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

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

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

$C_2 := (\{\bar{0}, \bar{1}\}, +, \bar{0}, -) \dots$ Gruppe

$$l_1(\bar{0}) := \text{id}$$

$$l_2(\bar{0}) := \text{id}$$

$$l_1(\bar{1}) := s: \mathbb{Z} \rightarrow \mathbb{Z} \\ x \mapsto -x$$

$$l_2(\bar{1}) := v: \mathbb{Z} \rightarrow \mathbb{Z} \\ x \mapsto -(x+1)$$

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

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

$$\Rightarrow |v(x) - v(y)| = |-(x+1) - (-(y+1))| = |y - x + 1 - 1| = 1 \Rightarrow v \in G$$

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

$$l_1(\bar{1}) \circ l_1(\bar{1}) = l_1(\bar{1} + \bar{1}) = l_1(\bar{0}) = \text{id} \text{ f\"ur } l_1 \text{ und } l_2 \text{ gelten.}$$

$$(l_1(\bar{1}) \circ l_1(\bar{1}))(x) = l_1(\bar{1})(-x) = x; \quad l_2(\bar{1})(-(x+1)) = -(-(x+1)+1) = x$$

$\Rightarrow l_1, l_2 \dots$ Hom. von C_2 nach C

Behauptung: $G = \langle s, v \rangle$ jeder Homomorphismus in G wird bereits

durch das Bild der 1 festgelegt. $s \circ v = x \mapsto x+1$; $(s \circ v) \circ \dots \circ (s \circ v) = x \mapsto x+k \quad \forall k \in \mathbb{N}$

$s \circ ((s \circ v) \circ \dots \circ (s \circ v)) = x \mapsto x-k \quad \forall k \in \mathbb{N}$ also gibt es Verk\"ufungen von s und v sodass

1 auf jeden bel. Wert abgebildet wird.

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

also ist C Koproduct von C_2 mit C_2 und bereits bekannt ist $|C| = \infty$ und

C ist nicht kommutativ. (bis auf Isomorphie eindeutig?)

