ALG Ü*

167) (1) zz: $C_n \times C_m$ ... zyklisch $\Leftrightarrow$ $ggT(n,m)=1$

($\Leftarrow$) $f: C_{nm} \to C_n \times C_m$ $\qquad$ • $f(\overline{0}^{nm}) = (\overline{0}^n, \overline{0}^m)$ ... neutrales Element von $C_n \times C_m$

$\overline{a}^{nm} \mapsto (\overline{a}^n, \overline{a}^m)$ $\qquad$ • $f(\overline{a+b}^{nm}) = (\overline{a+b}^n, \overline{a+b}^m) = (\overline{a}^n, \overline{a}^m) + (\overline{b}^n, \overline{b}^m)$

• Sei $\overline{a}^{nm}$ mit $f(\overline{a}^{nm}) = (\overline{0}^n, \overline{0}^m)$ bel. $\qquad = f(\overline{a}^{nm}) + f(\overline{b}^{nm})$ $\Rightarrow$ Homomorphismus

$\Rightarrow f(\overline{a}^{nm}) = (\overline{a}^n, \overline{a}^m) = (\overline{0}^n, \overline{0}^m)$ $\qquad \overline{a}^n = \overline{0}^n \Leftrightarrow a \in n\mathbb{Z}$, $\overline{a}^m = \overline{0}^m \Leftrightarrow a \in m\mathbb{Z}$

Da $ggT(n,m)=1 \Rightarrow a \in nm\mathbb{Z} \Rightarrow \overline{a}^{nm} = \overline{0}^{nm}$ $\Rightarrow$ injektiv

• $|C_{nm}| = nm = |C_n \times C_m| \Rightarrow$ bijektiv $\qquad \Rightarrow$ Isomorphismus

$\Rightarrow C_{nm} \simeq C_n \times C_m$ und da C_{nm} zyklisch ist folgt das auch $C_n \times C_m$ zyklisch sein muss.

($\Rightarrow$) $C_n \times C_m$ ... zyklisch $\Rightarrow \exists (x,y) \in C_n \times C_m : \langle (x,y) \rangle = C_n \times C_m$

$nm = ord(x,y) = kgV(ord(x), ord(y)) = \dfrac{ord(x) \cdot ord(y)}{ggT(ord(x), ord(y))} = \dfrac{nm}{ggT(n,m)}$

(da $kgV(a,b) \cdot ggT(a,b) = ab$) $\qquad \Rightarrow ggT(n,m) = 1$

(2) zz: C_n ... zyklische Gruppe $\quad n = \prod_{p \in \mathbb{P}} p^{e_p} \Rightarrow C_n \simeq \bigoplus_{p \in \mathbb{P}} C_{p^{e_p}}$

wobei e^p nur endlich oft $\neq 0$ ist. Sei $z \in \mathbb{N}$ maximal mit z-te Primzahl $p: e^p \neq 0$.

$D_k := C_{2^{e_2}} \times C_{3^{e_3}} \times \ldots \times C_{p^{e_p}}$ $\qquad o_k := 2^{e_2} \cdot 3^{e_3} \cdot \ldots \cdot p^{e_p}$ jeweils bis zur k-te Primzahl.

Vollständige Induktion um zu zeigen $D_k \simeq C_{o_k}$ $\forall k$

$k=1$: $\quad D_1 = C_{2^{e_2}} \quad o_k = 2^{e_2} \quad \Rightarrow C_{2^{e_2}} \cong C_{2^{e_2}}$

$k+1$: Angenommen $D_k \simeq C_{o_k}$ $\qquad$ Sei p' die $k+1$-te Primzahl

Oben haben wir gezeigt, dass $ggT(o_k, p'^{e_{p'}}) = 1 \Rightarrow C_{o_k} \times C_{p'^{e_{p'}}} \cong C_{o_{k+1}}$

Da $D_k \cong C_{o_k} \Rightarrow D_k \times C_{p'^{e_{p'}}} = D_{k+1} \cong C_{o_{k+1}}$

Nach endlich vielen Schritten erreichen wir $z \Rightarrow D_z \simeq C_{o_z}$

$\bigoplus_{p \in \mathbb{P}} C_{p^{e_p}} \simeq D_z \simeq C_{o_z} = C_n$ $\qquad \square$

$f: C_n \to C_{2^{e_2}} \times C_{3^{e_3}} \times \ldots$

$\overline{a}^n \mapsto (\overline{a}^{2^{e_2}}, \overline{a}^{3^{e_3}}, \ldots)$

ALG Ü*

213) A ... abelsche Gruppe $|A|<\infty \Rightarrow \exists n\in\mathbb{N}\ \exists m_i>1$ mit $m_1|m_2|\dots|m_n: A\cong\bigoplus_{i=1}^{n} C_{m_i}$

Sei $k:=|A|\in\mathbb{N} \Rightarrow \exists (e_p)_{p\in\mathbb{P}}$ aus $\mathbb{N}$: $k=\prod_{p\in\mathbb{P}} p^{e_p} = 2^{e_2}\cdot 3^{e_3}\cdot\dots$ mit nur endlich vielen $e_p\neq 0$

$$\begin{array}{rl} k= & 2\cdot 3\cdot 5\cdot 7\cdot\dots \\ & 2\quad 3\quad 5 \\ \vdots & 2\qquad\ \ 5 \\ m_3 & 2\qquad\ \ 5 \\ m_2 & 2 \\ m_1 & 2 \end{array}$$

Sei $n:=\max_{p\in\mathbb{P}} e_p$ ($\exists$ da nur endlich viele $\neq 1$)

Sei $m_i :=$ Produkt der $(n-i+1)$-te Zeile.

Klarerweise gilt $\forall i\in\{1,\dots,n-1\}: m_i | m_{i+1}$ da alle Primfaktoren von m_i auch in m_{i+1} vorkommen. Auch klar ist $m_i>1\ \forall i$.

zz: $\bigoplus_{i=1}^{n} C_{m_i}\cong\bigoplus_{p\in\mathbb{P}} C_{p^{e_p}}$

$f: C_{m_1}\times C_{m_2}\times\dots\times C_{m_n}\longrightarrow C_{2^{e_2}}\times C_{3^{e_3}}\times\dots$

$(\overline{a_{m_1}}^{m_1},\overline{a_{m_2}}^{m_2},\dots,\overline{a_{m_n}}^{m_n})\longmapsto(\overline{\sum_{i=1}^{n} a_{m_i}}^{2},\overline{\sum_{i=1}^{n} a_{m_i}}^{3},\dots)$

$f(\overline{0}^{m_1},\overline{0}^{m_2},\dots,\overline{0}^{m_n})=(\overline{0}^{2},\overline{0}^{3},\dots)$

$f((\overline{a_{m_1}}^{m_1},\dots,\overline{a_{m_n}}^{m_n})+(\overline{b_{m_1}}^{m_1},\dots,\overline{b_{m_n}}^{m_n}))=f(\overline{a_{m_1}+b_{m_1}}^{m_1},\dots,\overline{a_{m_n}+b_{m_n}}^{m_n})=(\overline{\sum_{i=1}^{n} a_{m_i}+b_{m_i}}^{2},\dots)$

$=(\sum_{i=1}^{n}\overline{a_{m_i}}^{2}+\overline{b_{m_i}}^{2},\dots)=(\sum_{i=1}^{n}\overline{a_{m_i}}^{2},\dots)+(\sum_{i=1}^{n}\overline{b_{m_i}}^{2},\dots)=f(\overline{a_{m_1}}^{m_1},\dots,\overline{a_{m_n}}^{m_n})+f(\overline{b_{m_1}}^{m_1},\dots,\overline{b_{m_n}}^{m_n})$

Sei $(\overline{a_{m_1}}^{m_1},\dots,\overline{a_{m_n}}^{m_n})$ mit $f(\overline{a_{m_1}}^{m_1},\dots,\overline{a_{m_n}}^{m_n})=(\overline{0},\overline{0},\dots)$ bel.

$\Rightarrow f(\overline{a_{m_1}}^{m_1},\dots,\overline{a_{m_n}}^{m_n})=(\overline{\sum_{i=1}^{n} a_{m_i}}^{2},\overline{\sum_{i=1}^{n} a_{m_i}}^{3},\dots)=(\overline{0}^{2},\overline{0}^{3},\dots)$

$\Rightarrow\forall p\in\mathbb{P}: \overline{\sum_{i=1}^{n} a_{m_i}}^{p}=\overline{0}^{p}\Rightarrow\sum_{i=1}^{n} a_{m_i}\in p\mathbb{Z}\Rightarrow\forall i\in\{1,\dots,n\}: a_{m_i}\in p\mathbb{Z}$

$\Rightarrow\forall i\in\{1,\dots,n\}: a_{m_i}\in m_i\mathbb{Z}\ \Rightarrow\forall i: \overline{a_{m_i}}^{m_i}=\overline{0}^{m_i}$

$\Rightarrow$ injektiver Homomorphismus da $\operatorname{ord}\bigoplus_{i=1}^{n} C_{m_i}=\operatorname{ord}\bigoplus_{p\in\mathbb{P}} C_{p^{e_p}}\Rightarrow$ Isomorphismus

$\Rightarrow A\cong\bigoplus_{p\in\mathbb{P}} C_{p^{e_p}}\cong\bigoplus_{i=1}^{n} C_{m_i}$

$\square$

ALG Ü*

393) $L = \mathbb{Q}(x)$

(1) ges: $[L:K]$ $K := \mathbb{Q}(x^3) \leq L$

Satz 6.1.34. x ... algebraisch über K $m(y)$ ... Minimalpolynom von x über K $\Rightarrow [K(x):K] = \text{grad}(m)$

$K(x) = \mathbb{Q}(x^3)(x) = \mathbb{Q}(x) = L$ $m(y) = y^3 - x^3$ ist normiert und erfüllt $m(x) = 0$

$\forall p \in \mathbb{Q}(x^3): \text{grad}(p) \in 3\mathbb{Z}$ Angenommen $\exists \tilde{m}(y): \text{grad}(\tilde{m}) < 3$ und $\tilde{m}(x) = 0$ und $\tilde{m}$ normiert

1. Fall $\tilde{m}(y) = y + p$ $p \in \mathbb{Q}(x^3)$ $\tilde{m}(x) = x + p = 0 \Rightarrow p = -x \notin \mathbb{Q}(x^3)$ ↯

2. Fall $\tilde{m}(y) = y^2 + py + q$ $p, q \in \mathbb{Q}(x^3)$ $\tilde{m}(x) = x^2 + px + q = 0 \Rightarrow x^2 = -px - q$

$\text{grad}(x^2) = 2 \overset{!}{=} \text{grad}(-px - q) = \max(\underbrace{\text{grad}(px)}_{\in 3\mathbb{Z}+1}, \underbrace{\text{grad}(q)}_{\in 3\mathbb{Z}})$ Da $2 \notin (3\mathbb{Z}) \cup (3\mathbb{Z}+1)$ ↯

$\Rightarrow y^3 - x^3$ ist Minimalpolynom $\Rightarrow [L:K] = 3$

(2) ges: $[L:K]$ $K = \mathbb{Q}(x + \frac{1}{x})$

$x + \frac{1}{x}$ ist algebraisch über $\mathbb{Q}(x)$, da $p(y) = xy - x^2 - 1 \in \mathbb{Q}(x)[y]$ eine Nullstelle bei $x + \frac{1}{x}$ hat:

$p(x + \frac{1}{x}) = x(x + \frac{1}{x}) - x^2 - 1 = x^2 + 1 - x^2 - 1 = 0$

Da $\varphi: \mathbb{Q}(x) \to \mathbb{Q}(\frac{1}{x})$ ein Automorphismus auf $\mathbb{Q}(x)$ ist und zwar nicht die Identität, da

$\varphi(x) = \frac{1}{x} \neq x$, jedoch auf $\mathbb{Q}(x + \frac{1}{x})$ die Identität ist, kann x nicht in $\mathbb{Q}(x + \frac{1}{x})$ liegen.

$\Rightarrow$ Minimalpolynom hat mindestens grad 2 $m(y) = y^2 - (x + \frac{1}{x})y + 1 \in \mathbb{Q}(x + \frac{1}{x})[y]$

$m(x) = x^2 - (x + \frac{1}{x})x + 1 = x^2 - x^2 - 1 + 1 = 0$ $\Rightarrow [L:K] = 2$

(3) $\alpha \in \mathbb{Q}(x) \setminus \mathbb{Q}$ $K := \mathbb{Q}(\alpha)$ zz: $[\mathbb{Q}(x) : \mathbb{Q}(\alpha)] < \infty$

$\alpha = \frac{\sum_{i=0}^{n} a_i x^i}{\sum_{j=0}^{m} b_j x^j} \in \mathbb{Q}(x) \setminus \mathbb{Q}$ $p(y) := \alpha \left(\sum_{j=0}^{m} b_j y^j\right) - \sum_{i=0}^{n} a_i y^i \in \mathbb{Q}(\alpha)[y]$

$p(x) = \alpha \left(\sum_{j=0}^{m} b_j x^j\right) - \sum_{i=0}^{n} a_i x^i = \sum_{i=0}^{n} a_i x^i - \sum_{i=0}^{n} a_i x^i = 0$

$p(y) \neq 0$, da für $\beta \in \mathbb{Q}$ keine Nullstelle von $\sum_{j=0}^{m} b_j x^j$ gilt

$p(\beta) = \underbrace{\alpha}_{\in \mathbb{Q}(x)\setminus\mathbb{Q}} \underbrace{\left(\sum_{j=0}^{m} b_j \beta^j\right)}_{\in \mathbb{Q}\setminus\{0\}} - \underbrace{\sum_{i=0}^{n} a_i \beta^i}_{\in \mathbb{Q}} \in \mathbb{Q}(x) \setminus \mathbb{Q}$ und daher $p(\beta) \neq 0$

p ist wahrscheinlich nicht das Minimalpolynom, aber das Minimalpolynom existiert und hat

grad kleiner gleich $\text{grad}(p)$. $\Rightarrow [\mathbb{Q}(x) : \mathbb{Q}(\alpha)] \leq \text{grad}(p) < \infty$

$\square$

ALG Ü*

339) R... Integritätsbereich   zz: $R[x]$... Hauptidealring $\Leftrightarrow$ R... Körper

($\Leftarrow$) Sei $I \trianglelefteq R[x]$... Ideal beliebig.

1. Fall $I=\{0\}$ $\Rightarrow$ $I=\langle 0\rangle$ also Hauptideal

2. Fall $I=R[x]$ $\Rightarrow$ $I=\langle 1\rangle$ also Hauptideal

3. Fall $I\neq\{0\} \wedge I\neq R[x]$ $\Rightarrow \exists p\in R[x]\setminus\{0\}: p\in I$ Wir wählen p mit geringstem Grad

Für $p\in R \Rightarrow p\cdot\frac{1}{p}=1\in I \Rightarrow I=R[x]$ also Hauptideal

Für $p\notin R$ Sei $f\in I$ bel.   zz: $f\in(p)$, da dann $I=(p)$ also Hauptideal

$\exists q,r\in R[x]:$ $f=q\cdot p+r$ $\Rightarrow r=\underbrace{f-q\cdot p}_{\in I}\in I$

Da $\text{grad}(r)<\text{grad}(p)$ oder $r=0$ muss, da $\text{grad}(p)$ minimal gewählt war gelten, dass $r=0$. $\Rightarrow f=q\cdot p\in(p)$

$\Rightarrow I=(p)$ $\Rightarrow$ $R[x]$ ist Hauptidealring

($\Rightarrow$) zz: $\forall r\in R\setminus\{0\}\ \exists r^{-1}\in R: r\cdot r^{-1}=1$

Sei $r\in R\setminus\{0\}$ bel. $I:=(r,x)\trianglelefteq R[x]$ Da $R[x]$ ein Hauptidealring ist

$\exists p\in I: (p)=I \Rightarrow \exists z_1,z_2\in R[x]: r=z_1 p \wedge x=z_2 p$

$\Rightarrow 0=\text{grad}(r)=\text{grad}(z_1)+\text{grad}(p) \Rightarrow \text{grad}(z_1), \text{grad}(p)=0$

$\Rightarrow 1=\text{grad}(x)=\text{grad}(z_2)+\text{grad}(p)=\text{grad}(z_2)+0 \Rightarrow \text{grad}(z_2)=1$

$\Rightarrow \exists a,b\in R: z_2=a+bx \Rightarrow x=z_2 p=ap+bpx \Rightarrow bp=1$

$\Rightarrow b=p^{-1} \Rightarrow p\in E(R) \Rightarrow I=(p)=R[x]$

$\Rightarrow \exists c,d\in R[x]: cr+dx=1 \Rightarrow rc_1+\ldots=1 \Rightarrow c_1=r^{-1}\in R$

$\Rightarrow R$ ist Körper

$\square$

ALG Ü *

399) ges: unendlicher Körper K, $char(K)=p$ mit $a \mapsto a^p$ ist Automorphismus auf K

$\tilde{K} = \bigotimes_{i=1}^{\infty} GF(p^i)$ $\quad$ $\mathcal{U}$ ... Ultrafilter von $\mathbb{N}$ (sicherheitshalber freier Ultrafilter)

$(\tilde{a}_i)_{i\in\mathbb{N}}, (\tilde{b}_i)_{i\in\mathbb{N}} \in \tilde{K}$ $\quad$ $(\tilde{a}_i)_{i\in\mathbb{N}} \sim (\tilde{b}_i)_{i\in\mathbb{N}} \Leftrightarrow \{i\in\mathbb{N} : \tilde{a}_i = \tilde{b}_i\} \in \mathcal{U}$ $\quad$ $K = \tilde{K}/_\sim$

$+, \cdot$ wohldefiniert? $\quad$ Sei $a = (a_i)_{i\in\mathbb{N}}, a', b, b' \in \tilde{K}$ bel. mit

$a \sim a' \wedge b \sim b' \Rightarrow M_a := \{i\in\mathbb{N} : a_i = a'_i\} \in \mathcal{U}$, $M_b := \{i\in\mathbb{N} : b_i = b'_i\} \in \mathcal{U}$

$M_+ := \{i\in\mathbb{N} : a_i + b_i = a'_i + b'_i\} \supseteq M_a \cap M_b \in \mathcal{U}$, da $\mathcal{U}$ ... Filter

$(F_1, \dots, F_n \in \mathcal{F} \Rightarrow \bigcap_{i=1}^{n} F_i \in \mathcal{F})$ $\quad \Rightarrow a+b \sim a'+b'$

$M_\cdot := \{i\in\mathbb{N} : a_i b_i = a'_i \cdot b'_i\} \supseteq M_a \cap M_b \in \mathcal{U}$ $\quad \Rightarrow ab \sim a'b'$

Multiplikativ Inverses Element? $\quad$ Sei $a = [(a_i)_{i\in\mathbb{N}}]_\sim \in K \setminus \{[(0)_{i\in\mathbb{N}}]_\sim\}$ bel.

$\Rightarrow M := \{i\in\mathbb{N} : a_i = 0\} \notin \mathcal{U}$ $\quad \Rightarrow \neg M \in \mathcal{U}$, da $\mathcal{U}$ Ultrafilter

$\neg M = \{i\in\mathbb{N} : a_i \neq 0\} \in \mathcal{U}$ $\quad$ Sei $b_i = \begin{cases} a_i^{-1}, & i \in \neg M \\ 0, & i \in M \end{cases}$ ... existiert in $GF(p^i)$

$\Rightarrow a \cdot b = [(a_i \cdot b_i)_{i\in\mathbb{N}}]_\sim = [(\mathbb{1}_{\neg M}(i))_{i\in\mathbb{N}}]_\sim$

$L := \{i\in\mathbb{N} : a_i b_i = 1\} = \{i\in\mathbb{N} : i \in \neg M\} = \neg M \in \mathcal{U}$

$\Rightarrow a \cdot b = 1 \in K$

$\Rightarrow K$ ... Körper $\quad$ Restlicher Beweis nie gehabt