VO ALGEBRA FÜR LAK

11:10 - 12:50 10 min Pause

DI 13:30 Tutorium Besprechungszimmer

I Einführung

1. lineare diophantische Gleichungen

$ax_1 + bx_2 = c \quad a,b,c \in \mathbb{Z}$ gesucht: ganzzahlige Lösungen

Bsp $70x_1 + 126x_2 = 742$ 1 Gleichung mit 2 Unbekannten

$a \mid b \cdot c$ und $\overset{ggT}{gcd}(a,b) = 1 \Rightarrow a \mid c$

$(4 \mid 6 \cdot 10)$

Prop: Seien $a,b \in \mathbb{Z}$ mit $ggT(a,b) = 1$ dann erfüllt $\binom{x_1}{x_2} \in \mathbb{Z}^2$

$ax_1 + b \cdot x_2 = 0$ genau dann wenn $\exists\, t \in \mathbb{Z}$ mit $\binom{x_1}{x_2} = t \cdot \binom{b}{-a}$

$\left(t \cdot \binom{b}{-a},\ t \in \mathbb{Z}\right)$

Beweis

$\Leftarrow \quad x = t \cdot \binom{b}{-a} \Rightarrow a \cdot \underbrace{x_1}_{tb} + b \underbrace{x_2}_{-ta} = 0$

$\Rightarrow \quad x$ sei Lösung von $ax_1 + bx_2 = 0$

$\Rightarrow \quad ax_1 = -bx_2 \Rightarrow a \mid bx_2 \overset{ggT(a,b)=1}{\Rightarrow} a \mid x_2$

$\Rightarrow \exists\, t \in \mathbb{Z} : x_1 = -t \cdot a$

$\Rightarrow \quad ax_1 = \underbrace{-bx_2}_{-t \cdot a} = t \cdot a \cdot b \Rightarrow x_1 = t \cdot b \Rightarrow x = t\binom{b}{-a}$ □

Satz Seien $a,b,c \in \mathbb{Z}$, $d := ggT(a,b)$

dann besitzt die Gleichung $ax_1 + bx_2 = c$ genau dann ganzzahlige Lösungen, wenn $d \mid c$ weiters gilt, falls $x_0 \in \mathbb{Z}^2$ eine Lösung ist, dann erhält man alle Lösungen von $ax_1 + bx_2 = c$ als $x_0 + t \cdot \begin{pmatrix} \frac{b}{d} \\ \frac{a}{d} \end{pmatrix}$

Beweis

$\Rightarrow$ $\exists$ x Lösung von $ax_1 + bx_2 = c$ $\quad d|a$ und $d|b$

$\Rightarrow d | ax_1 + bx_2 = c$

$\Leftarrow$ wir wissen aus Zahlentheorie $\exists y_1, y_2 \in \mathbb{Z}$ mit $d = ay_1 + by_2$

$\frac{c}{d} \in \mathbb{Z}$ (weil $d|c$) Setze $x_1 := y_1 \frac{c}{d}$ und $x_2 := y_2 \frac{c}{d}$

$$\underbrace{ax_1}_{=y_1 \frac{c}{d}} + b \underbrace{x_2}_{=y_2 \frac{c}{d}} = \frac{c}{d}(\underbrace{ay_1 + by_2}_{d}) = c$$

$$\frac{a}{d}x_1 + \frac{b}{d}x_2 = \frac{c}{d} \qquad ggT\left(\frac{a}{d}, \frac{b}{d}\right) = 1$$

$$x = \underbrace{x_0}_{=\binom{x_0^{(1)}}{x_0^{(2)}}} + t\begin{pmatrix}\frac{b}{d}\\ -\frac{a}{d}\end{pmatrix} \Rightarrow \frac{a}{d}x_1 + \frac{b}{d}x_2 = \underbrace{\frac{a}{d}x_0^{(1)} + \frac{b}{d}x_0^{(2)}}_{=\frac{c}{d}} + \underbrace{t\cdot\left(\frac{a}{d}\frac{b}{d}\right) - t\left(\frac{b}{d}\frac{a}{d}\right)}_{=0} = \frac{c}{d}$$

Sei x eine Lösung von $ax_1 + bx_2 = c$

$y = (x - x_0)$ ist Lösung von $ay_1 + by_2 = \underbrace{ax_1 + bx_2}_{=c} - \underbrace{(ax_0^{(1)} + bx_0^{(2)})}_{=c} = 0$

$$\Rightarrow \frac{a}{d}y_1 + \frac{b}{d}y_2 = 0 \overset{\text{Prop.}}{\Rightarrow} y = t\cdot\begin{pmatrix}\frac{b}{d}\\ -\frac{a}{d}\end{pmatrix} \Rightarrow x = x_0 + t\begin{pmatrix}\frac{b}{d}\\ -\frac{a}{d}\end{pmatrix} \qquad \square$$

Bsp $70x_1 + 126x_2 = 742$

70 | ②	126 | ②
35 | 5	63 | 3
7 | ⑦	21 | 3
1 |	7 | ⑦
	1 |

$\Rightarrow ggT(70, 126) = 2 \cdot 7 = 14$

$14 \mid 742 \qquad \frac{742}{14} = 53$

$5x_1 + 9x_2 = 53$

mod 5 $\qquad 4x_2 \equiv 3 \equiv 8 \quad \Rightarrow x_2 = 2 \Rightarrow x_1 = 7$

Lösungen $\begin{pmatrix}7\\2\end{pmatrix} + t\begin{pmatrix}9\\-5\end{pmatrix}, \quad t \in \mathbb{Z}$

Bsp $325x_1 + 143x_2 = 9978$

$ggT(325, 143) = 13 \qquad 13 \mid 9978 \qquad \frac{9978}{13} = 767\frac{7}{13}$

325 | 5	143 | 11
65 | 5	13 | 13
13 | 13	1 |
1 |	

Lösungen: $\emptyset$

Bsp $1656x_1 + 1173x_2 = 76\,314$

$1656 = 1 \cdot 1173 + 483$

$1173 = 2 \cdot 483 + 207$

$483 = 2 \cdot 207 + \boxed{69}$ ggT

$207 = 3 \cdot 69$

$ggT(1656, 1173) = 69$

$69 = 1 \cdot 483 - 2 \cdot 207 = -2 \cdot 1173 + 5 \cdot 483 =$

$1 \times 1173 - 2 \cdot 483 \qquad = 1 \times 1656 - 1 \times 1173$

$= 5 \times 1656 - 7 \times 1173$

$69 \mid 76\,314 \qquad \frac{76\,314}{69} = 1106$

$24x_1 + 17x_2 = 1106$

mod 17: $24 \equiv 7 \ (17) \quad 7x_1 \equiv 1 \equiv 18 \equiv 35 \quad \Rightarrow x_1 = 5$

$\Rightarrow x_2 = \frac{986}{17} = 58$

Lösung: $\begin{pmatrix} 5 \\ 58 \end{pmatrix} + t \cdot \begin{pmatrix} 17 \\ -24 \end{pmatrix}$

Bsp $1656x_1 + 1173x_2 = 76\,314 \quad x_1, x_2 \geq 0$!

$0 \leq 5 + 17t \quad \Rightarrow t \geq -\frac{5}{17} \geq 0$

$0 \leq 58 - 24t \quad \Rightarrow t \leq \frac{58}{24} = \frac{29}{12} \quad \Rightarrow t \leq 2$

$t = 0, 1, 2$ einsetzen

einfacher:

$\begin{pmatrix} 5 \\ 58 \end{pmatrix} \xrightarrow{+\begin{pmatrix} 17 \\ -24 \end{pmatrix}} \begin{pmatrix} 22 \\ 34 \end{pmatrix} \xrightarrow{+\begin{pmatrix} 17 \\ -24 \end{pmatrix}} \begin{pmatrix} 39 \\ 10 \end{pmatrix}$ 3 Lösungen

2. Permutationen

Def: Sei $M \neq \emptyset$. Dann heißt eine bijektive Funktion $\sigma: M \to M$ eine Permutation auf M

falls M endlich ist, also n Elemente hat, dann kann man o.B.d.A annehmen, dass $M = \{1, 2, 3 \ldots\}$

Def: $S_n = \{\sigma : \text{Permutation auf } \{1,2,\dots,n\}\}$

Beispiel S_3

$\sigma \in S_n$

Matrixschreibweise $\begin{pmatrix} 1 & 2 & 3 & \dots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \dots & \sigma(n) \end{pmatrix}$ ← auf welche Elemente sie abgebildet werden

z.B $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 1 & 3 & 2 \end{pmatrix}$ ← jedes Element aus der 1. Zeile genau 1 mal!

σ, τ Permutationen $\sigma \cdot \tau = \sigma \circ \tau$ Permutation bijektiv
Hintereinander

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 1 & 3 & 2 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 2 & 5 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 5 & 2 & 3 \end{pmatrix}$$

von rechts nach links!
nicht kommutativ!

σ Permutation $\Rightarrow \sigma^{-1}$ Permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 1 & 3 & 2 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 1 & 2 \end{pmatrix}$$

Wir nennen $(x_1\ x_2\ \dots\ x_r)$ einen Zyklus (r-Zyklus, $r \geq 2$) wobei

$\sigma = (x_1\ x_2\ \dots\ x_r)$ heißt $\sigma(x_j) = x_{j+1}$ $j = 1,2,\dots,r-1$ $\sigma(x_r) = x_1$ und $\sigma(x) = x$

$\forall x \in \{1,2,\dots,n\} \setminus \{x_1,\dots,x_r\}$

also z.B $S_3 : (1\ 3)$

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

Jedes $\sigma \in S_n$ lässt sich als Produkt von elementfremden Zyklen schreiben.

z.B $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 1 & 3 & 2 \end{pmatrix} = (1\ 4\ 3) \cdot (2\ 5)$

Bsp

$\sigma = (1\ 5\ 2) \cdot (3\ 4)$ $\tau = (1\ 3)(2\ 5)$

$\sigma \cdot \tau = (1\ 4\ 3\ 5)$
1 Element gleich, andere von hinten nach vorne

$\sigma^{-1} = (1\ 2\ 5)\ (3\ 4)$

Jede Permutation lässt sich als Produkt von (nicht elementfremden) Zweierzyklen schreiben.

Beweis im PS

Beispiel

$\sigma = (1\,2)\,(1\,5)\,(3\,4)$ nicht eindeutig

siehe vorher $\sigma = (1\,2\,5)\,(3\,4)$

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & & \sigma(n) \end{pmatrix}$$

$$j \in \{1, \dots, n\} : \quad n_j := \underset{\text{Anzahl}}{\operatorname{card}} \{m > j : \sigma(m) < \sigma(j)\}$$

z.B. $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 1 & 4 & 2 \end{pmatrix}$

$n_1 = 2$

$n_2 = 3$ nach dem 5er 3 Einträge größer als 5

$n_3 = 0$

$n_4 = 1$

$\sum_{j=1}^{5} n_j = 6$ (gerade) ← entscheidend

$j, k \in \{1, 2, \dots n\}, \; j < k$

$$n(j,k) := \begin{cases} 1 & \text{falls } \sigma(j) > \sigma(k) \\ 0 & \text{falls } \sigma(j) < \sigma(k) \end{cases}$$

$\sum_{k=j+1}^{n} n(j,k) = 2$ Zählt bei wie vielen Elementen $\sigma(k) < \sigma(j)$

Def: $\operatorname{sgn} \sigma := (-1)^{\sum_{j=1}^{n} n_j}$ Potenz

Proposition

$\sigma \in S_n, \; x_1 \neq x_2 \in \{1, 2, \dots, n\}$ Dann gilt $\operatorname{sgn}(\sigma(x_1\, x_2)) = -\operatorname{sgn}\sigma$

Permutation multiplizieren mit zweier Zyklus ergibt umgekehrtes Vorzeichen

Beweis: $x_1 < x_2$

$$\sigma = \begin{pmatrix} 1 & \dots & x_1 - 1 & x_1 & \dots & x_2 - 1 & x_2 & x_2 + 1 & \dots & n \\ \sigma(1) & & \sigma(x_1 - 1) & \sigma(x_1) & \dots & \sigma(x_2 - 1) & \sigma(x_2) & \sigma(x_2 + 1) & \dots & \sigma(n) \end{pmatrix}$$

$$\sigma(x_1\, x_2) = \begin{pmatrix} 1 & \dots & x_1-1 & x_1 & x_1+1 & \dots & x_2-1 & x_2 & x_2+1 & \dots & n \\ \sigma(1) & \dots & \sigma(x_1-1) & \sigma(x_2) & \sigma(x_1+1) & & \sigma(x_2-1) & \sigma(x_1) & \sigma(x_2+1) & & \sigma(n) \end{pmatrix}$$

für $j < x_1$ oder $j > x_2$ ist $\tilde{n}_j = n_j$ (für $\sigma(x_1 \cdot x_2)$)

$x_1 < j < x_2$ und $k > j$, $k \neq x_2$

$\tilde{n}(j,k) = n(j,k)$

1. Fall $\sigma(x_1) < \sigma(x_2)$

1. Fall a: $\sigma(j) < \sigma(x_1)$

$\tilde{n}(j, x_2) = 0 = n(j, x_2)$

$\tilde{n}(x_1, j) = 1 = n(x_1, j)$

1. Fall b: $\sigma(j) > \sigma(x_2)$ analog

1. Fall c: $\sigma(x_1) < \sigma(j) < \sigma(x_2)$

$\tilde{n}(j, x_2) = 1$	$n(j, x_2) = 0$
$\tilde{n}(x_1, j) = 1$	$n(x_1, j) = 0$
$\Sigma = 2$	$\Sigma = 0$

$(-1)^2 = (-1)^0 = 1$

$(-1)^{\Sigma} = 1$ $\Rightarrow$ Ändert nichts am Vorzeichen □

$\tilde{n}(x_1, x_2) = 1$ $\quad n(x_1, x_2) = 0$

$\Rightarrow \operatorname{sgn}(\sigma(x_1 x_2)) = -\operatorname{sgn}\sigma$

2. Fall analog $\sigma(x_2) < \sigma(x_1)$ □

Korollar

Sei $\sigma = \theta_1 \cdot \theta_2 \cdot \dots \cdot \theta_k \Rightarrow \operatorname{sgn}\sigma = (-1)^k$

(Zweierzyklen)

Beweis

$\operatorname{sgn}\sigma = \operatorname{sgn}(\theta_1 \theta_2 \dots \theta_k) = (-1)\ \operatorname{sgn}(\theta_1 \theta_2 \dots \theta_{k-1}) = \dots$

$\dots = (-1)^k$ □

entweder nur gerade oder nur ungerade Anzahl von Zweierzyklen möglich

Korollar

$\operatorname{sgn}(\sigma\tau) = \operatorname{sgn}\sigma \cdot \operatorname{sgn}\tau$

Beweis

$\sigma = \sigma_1 \sigma_2 \cdots \sigma_{k_1}$ (Zweierzyklen) $\qquad \tau = \tau_1 \cdots \tau_{k_2}$ (Zweierzyklen)

$\operatorname{sgn}\sigma = (-1)^{k_1} \qquad \operatorname{sgn}\tau = (-1)^{k_2}$

$\operatorname{sgn}(\sigma\cdot\tau) = \operatorname{sgn}(\sigma_1 \cdots \sigma_{k_1} \cdot \tau_1 \cdots \tau_{k_2}) = (-1)^{k_1+k_2} =$

$= (-1)^{k_1} \cdot (-1)^{k_2} = \operatorname{sgn}\sigma \cdot \operatorname{sgn}\tau$ □

Def: (1) $\sigma \in S_n$ heißt gerade, falls $\operatorname{sgn}\sigma = 1$

(2) -"- ungerade, -"- $\operatorname{sgn}\sigma = -1$

(3) A_n sei die Menge aller geraden Permutationen

Proposition

$\sigma \in A_n \Rightarrow \sigma$ ist Produkt von Dreierzyklen

Beweis

$\sigma = \sigma_1 \sigma_2 \cdots \sigma_k = (\sigma_1\sigma_2)(\sigma_3\sigma_4)\cdots(\sigma_{k-1}\sigma_k)$

Zweierzyklen, k gerade

es genügt also das Produkt von zwei Zweierzyklen zu betrachten

$(x_1\ x_2)(x_1\ x_2) = (x_1\ x_2\ x_3)(x_1\ x_3\ x_2)$ (Inverses 1 gleich anderen vertauschen)

$(x_1\ x_3)\cdot(x_1\ x_2) = (x_1\ x_2\ x_3)$

$(x_1\ x_2)\cdot(x_3\ x_4) = (x_1\ x_3\ x_2)\cdot(x_1\ x_3\ x_4)$ □

$(\sigma_1\cdot\sigma_2)\cdot\sigma_3 = \sigma_1(\sigma_2\sigma_3)$

eigentlich $\sigma\cdot\tau = \sigma\circ\tau$ assoziativ

II Algebraische Strukturen

1) Gruppen

Def: $G \neq \emptyset$ Dann heißt $\cdot$ eine Operation auf G, falls

$\forall\, a,b \in G \quad \exists!\; a\cdot b \in G \qquad (\cdot : G\times G \to G)$

manchmal auch additiv $a+b$ (Kommutativgesetz i.A. vorausgesetzt)

Def $(G,\cdot)$ ist assoziativ falls $\forall\, a,b,c \in G: (ab)c = a(bc)$

(Halbgruppe)

$(G,\cdot)$ ist kommutativ falls $\forall\, a,b \in G: a\cdot b = b\cdot a$

Allgemeines Assoziativgesetz

Prop:

$(G,\cdot)$ assoziativ, $a_1, a_2, \dots, a_n \in G$. Dann ergeben alle Produkte von $a_1, a_2, \dots, a_n$ (in dieser Reihenfolge) denselben Wert.

Beweis

$a_1 \cdot a_2 \qquad n>2: \quad a_1 \cdot \dots \cdot a_n := (a_1 \cdot \dots \cdot a_{n-1}) \cdot a_n$

$= (((\dots) a_{n-2}) a_{n-1}) a_n$

Induktion: $n=1$, $n=2$ ✓

Sei $n>2$ $\qquad P(a_1, \dots, a_n) = \underbrace{P(a_1, \dots, a_k)}_{\overset{IV}{=} a_1 \cdot \dots \cdot a_k} \cdot \underbrace{P(a_{k+1}, \dots, a_n)}_{\overset{IV}{=} a_{k+1} \cdot \dots \cdot a_n}$ (Produkt)

1. Fall $k = n-1$

$P(a_1, \dots, a_n) = (a_1 \cdot \dots \cdot a_{n-1}) \cdot a_n = a_1 \cdot \dots \cdot a_n$

2. Fall $k < n-1$

$P(a_1, \dots, a_n) = (a_1 \cdot \dots \cdot a_k) \cdot \underbrace{(a_{k+1} \cdot \dots \cdot a_n)}_{(a_{k+1} \cdot \dots \cdot a_{n-1}) a_n} = (a_1 \cdot \dots \cdot a_k) \cdot ((a_{k+1} \cdot \dots \cdot a_{n-1}) \cdot a_n) \overset{AG}{=}$

$= \Big(\underbrace{(a_1 \cdot \dots \cdot a_k) \cdot (a_{k+1} \cdot \dots \cdot a_{n-1})}_{\overset{IV}{=} a_1 \cdot \dots \cdot a_{n-1}} \Big) \cdot a_n = a_1 \cdot a_2 \cdot \dots \cdot a_n$ $\qquad \square$

Def $(G, \cdot)$ sei assoziativ, dann heißt $(G, \cdot)$ <u>Gruppe</u> falls

(1) $\exists\, 1 \in G$ mit $1 \cdot a = a \quad \forall a \in G$ (Links-Einselement)

(2) $\forall a \in G \; \exists\, a^{-1} \in G$ mit $a^{-1} \cdot a = 1$ (Links-Inverses)

Def eine Gruppe $(G, \cdot)$ heißt Abelsch (<u>Abelsche Gruppe</u>) falls sie kommutativ ist.

<u>additiv</u>: $0 + a = a$, $(-a) + a = 0$

Proposition

Sei $(G, \cdot)$ eine Gruppe

(1) $a \cdot 1 = a \quad \forall a \in G$

(2) $a \cdot a^{-1} = 1 \quad \forall a \in G$

(3) 1 ist eindeutig bestimmt

(4) $\forall a \in G$ ist a^{-1} eindeutig bestimmt.

<u>Beweis</u>

(2) $a \cdot a^{-1} = \underbrace{1 \cdot (a \cdot a^{-1})}_{= (a \cdot a^{-1})^{-1} (a \cdot a^{-1})} = (a \cdot a^{-1})^{-1} \cdot (a \cdot \underbrace{a^{-1} \cdot a}_{=1} \cdot a^{-1}) =$ $\quad = a^{-1}$

$= (a \cdot a^{-1})^{-1} \cdot (a \cdot a^{-1}) = 1$ □

(1) $a \cdot \underbrace{1}_{= a^{-1} \cdot a} = \underbrace{a \cdot a^{-1}}_{\overset{(2)}{=} 1} \cdot a = a$ ◇

(3) Sei $1'$ so, dann $1' \cdot a = a \quad \forall a \in G$

$1' \overset{(1)}{=} 1' \cdot 1 = 1$ ◇

(4) Sei a' so, dann $a' \cdot a = 1$

$a' \overset{(1)}{=} a' \cdot \underbrace{1}_{\overset{(2)}{=} a \cdot a^{-1}} = \underbrace{a' \cdot a}_{=1} \cdot a^{-1} = a^{-1}$ □

Prop

$(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$

Beweis

$(b^{-1} \cdot a^{-1})(a\,b) = b^{-1} \cdot \underbrace{a^{-1} \cdot a}_{=1} \cdot b = 1$ ($a^{-1} \cdot a = 1$, $= b$)

wegen der Eindeutigkeit $(ab)^{-1}$ gilt $(ab)^{-1} = b^{-1} a^{-1}$ □

$(a^{-1})^{-1} = a$: $a \cdot a^{-1} = 1 \Rightarrow (a^{-1})^{-1} = a$

Beispiele für Gruppen

$(\mathbb{Z}, +)$ abelsch

$(\mathbb{N}, +)$ Problem: neutrales Element, Inverses $\Rightarrow$ KEINE Gruppe

$(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ $(\mathbb{C}, +)$ abelsche Gruppen

$(\mathbb{R}, \cdot)$ KEINE Gruppe Problem: Inverses zu 0 ∄

z.B. $(\mathbb{R} \setminus \{0\}, \cdot)$, $(\mathbb{C} \setminus \{0\}, \cdot)$ } abelsche Gruppen

$(\mathbb{R}^+, \cdot)$

$\mathbb{Z}_n$ ... Restklassen modulo n $(\mathbb{Z}_n, +)$ Gruppe

V ... Vektorraum $\Rightarrow$ $(V, +)$ abelsche Gruppe

$(\mathbb{Z}^n, +)$ abelsche Gruppe

(S_n) Gruppe aber nicht abelsch!
Permutationen
allgemein: alle Permutationsgruppen -"-

$(M_n, \cdot)$ keine Gruppe : Problem : ∄ Inverses
n×n Matrizen

$(GL_n, \cdot)$ Gruppe
↳ invertierbare n×n Matrizen

Def: $(G, \cdot)$ assoziativ

(1) Für $n \in \mathbb{N}$ $a^1 := a$, für $n > 1$ $a^n := a^{n-1} \cdot a$

(additiv $n \cdot a$)

(2) $(G, \cdot)$ Gruppe $a^0 := 1$, für $n \in \mathbb{Z}$ $n < 0$ $a^n := (a^{-1})^{-n}$

es gelten die üblichen Rechenregeln

ACHTUNG: $(a\,b)^n = a^n \cdot b^n$ gilt nur in abelschen Gruppen, nicht allgemein

Proposition älteste Motivation (Lösen von Gleichungen)

$(G, \cdot)$ assoziativ. Dann ist G genau dann eine Gruppe, wenn

$\forall a,b \in G \quad \exists x,y \in G$ mit $a \cdot x = b$ und $y \cdot a = b$

Beweis

Proseminar!

Proposition

$(G, \cdot)$ Gruppe. Dann gelten die Kürzungsregeln

$a,b,x \in G$

$$ax = bx \Rightarrow a = b$$
$$xa = xb \Rightarrow a = b$$

Beweis

es genügt die 1. Kürzungsregel zu zeigen

$\cdot x^{-1}$ von rechts!!

$$ax = bx \Rightarrow a = a\underbrace{xx^{-1}}_{=1} = b\underbrace{x \cdot x^{-1}}_{=1} = b$$ □

! Kürzungsregeln $\not\Rightarrow$ Gruppe (z.B. $(\mathbb{N}, +)$)

Bsp $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a,b \in \mathbb{Q}\}$

$$(a_1 + b_1\sqrt{2}) \cdot (a_2 + b_2\sqrt{2}) = (\underbrace{a_1 \cdot a_2 + 2 \cdot b_1 \cdot b_2}_{\in \mathbb{Q}}) + \sqrt{2}(\underbrace{a_1 \cdot b_2 + a_2 \cdot b_1}_{\in \mathbb{Q}})$$

$\in \mathbb{Q}$ liegt wieder in Gruppe

Assoziativgesetz gilt, weil es in $\mathbb{R}$ gilt

Def: $(G, \cdot)$ Gruppe, $U \subseteq G$ heißt Untergruppe, falls U (mit der selben Operation wie in G) eine Gruppe ist. G heißt dann Obergruppe von U

$U \neq \emptyset$

Proposition

$(G, \cdot)$ Gruppe, $U \subseteq G$, $U \neq \emptyset$ dann sind äquivalent:

(1) U ist Untergruppe

(2) $\forall a,b \in U$ ist $a \cdot b \in U$ und $a^{-1} \in U$ $(\Rightarrow 1 \in U)$

(3) $\forall a,b \in U : a \cdot b^{-1} \in U$

wenn G abelsch $\Rightarrow U$ abelsch

Beweis

(1) $\Rightarrow$ (2) $a,b \in U \Rightarrow a \cdot b \in U$, $a^{-1} \in U$, $1 \in U$

(2) $\Rightarrow$ (3) $a,b \in U \Rightarrow b^{-1} \in U \Rightarrow a \cdot b^{-1} \in U$

(3) $\Rightarrow$ (1) $a,b \in U$, $1 = a \cdot a^{-1} \in U$, $a^{-1} = 1 \cdot a^{-1} \in U$ $\Rightarrow b^{-1} \in U$

$a \cdot b = a(b^{-1})^{-1} \in U$ □

„Def"

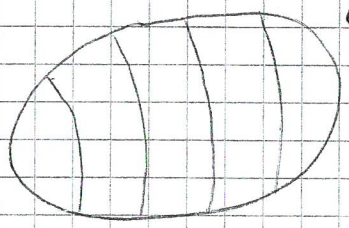
$(G, \cdot)$ Gruppe, $A \subseteq G$, $B \subseteq G$, $a \in G$

$a \cdot A := \{a \cdot x : x \in A\}$, $A \cdot a := \{x \cdot a : x \in A\}$ $a \cdot A = \{a\} \cdot A$

$A \cdot B := \{x \cdot y : x \in A, y \in B\}$

Def: $(G, \cdot)$ Gruppe, $U \subseteq G$ Untergruppe. Dann nennt man $G/U := \{a \cdot U : a \in G\}$ die Linksnebenklassen von G bezüglich U.

($U \backslash G$ ... Rechtsnebenklassen)



Unterklassen liegen nebeneinander und ergeben insgesamt alles

- $aU = bU \Leftrightarrow b^{-1} \cdot a \in U$

Beweis

$\Rightarrow$ $a \cdot \underbrace{x}_{\in U} = b \cdot \underbrace{y}_{\in U} \Rightarrow b^{-1} \cdot a \cdot x = \underbrace{b^{-1} \cdot b}_{1} \cdot y \Rightarrow b^{-1} \cdot a = y \cdot x^{-1} \in U$

$\Leftarrow$ sei $b^{-1} \cdot a \in U$ betrachte $a \cdot \underbrace{x}_{\in U}$, $a^{-1} \cdot b = (b^{-1} \cdot a)^{-1} \in U$

$b(\underbrace{\underbrace{b^{-1} \cdot a}_{\in U} \cdot \underbrace{x}_{\in U}}_{\in U}) = a \cdot x \Rightarrow ax \in bU$ □

- $aU \cap bU \neq \emptyset \Rightarrow aU = bU$

Beweis

$\exists$ Element das $a \cdot \underbrace{x}_{\in U} = b \cdot \underbrace{y}_{\in U} \Rightarrow b^{-1}a = y \cdot x^{-1} \in U$

$\Rightarrow aU = bU$ □

- $f: U \to aU$, $f(x) := ax$ bijektiv

Beweis

surjektiv: ✓

injektiv: $x_1, x_2 \in U$, $f(x_1) = f(x_2)$

$\Rightarrow a \cdot x_1 = a \cdot x_2 \overset{\text{KüR}}{\Rightarrow} x_1 = x_2$ □

Proposition

Sei $(G, \cdot)$ endliche Gruppe, $U \leq G$ Untergruppe. Dann gilt

$\text{card } G = (\text{card } U) \cdot (\text{card } (G/U))$ insbesondere

$\text{card } U \mid \text{card } G$ (Teiler) card = Anzahl der Elemente

Beweis

es gibt card G/U versch. Linksnebenklassen, paarweise disjunkt mit jeweils card U Elementen. Daher

$\text{card } G = (\text{card } U) \cdot (\text{card } (G/U))$ □

vgl Dimensionsformel (Algebra)

Proposition

$(G, \cdot)$ Gruppe, $(U_j)_{j \in J}$ beliebig viele Familie von Untergruppen. Dann ist

$\bigcap_{j \in J} U_j$ ebenfalls Untergruppe

Beweis

$U := \bigcap_{j \in J} U_j$ Sei $a, b \in U$ Sei $j \in J$ beliebig

$\Rightarrow a \cdot b \in U_j \Rightarrow a \cdot b^{-1} \in U_j$ Daher $a \cdot b^{-1} \in U$

$\Rightarrow U$ ist Untergruppe □

Def: Sei $(G, \cdot)$ eine Gruppe, $A \subseteq G$ Dann ist

$\langle A \rangle = \bigcap_{\substack{U \supseteq A \\ U \text{ Untergruppe}}} U$ (kleinste Untergruppe die A enthält)

die von A erzeugte Untergruppe

A selber muss nicht Untergruppe sein!

$A = \{a\}$, $\langle \{a\} \rangle = \langle a \rangle$

17

Proposition (kommutativ weil von 1 Element erzeugt ⇒ abelsch)

$(G,\cdot)$ Gruppe, $a \in G$, Dann ist $\langle a \rangle = \{a^n \cdot n \in \mathbb{Z}\}$

Beweis

für $n \in \mathbb{Z}$ muss $a^n \in \langle a \rangle$, also $\langle a \rangle \supseteq \{a^n : n \in \mathbb{Z}\}$ (Obermenge)

noch zu zeigen $\{a^n : n \in \mathbb{Z}\}$ ist Untergruppe

Seien $x, y \in \{a^n : n \in \mathbb{Z}\} \Rightarrow \exists\, n_1, n_2 \in \mathbb{Z} \;\; x = a^{n_1} \;\; y = a^{n_2}$

$x \cdot y^{-1} = a^{n_1} \cdot a^{-n_2} = a^{\underbrace{n_1 - n_2}_{\in \mathbb{Z}}} \in \{a^n : n \in \mathbb{Z}\}$ □

Def: $(G,\cdot)$ heißt <u>zyklisch</u>, falls $\exists\, a \in G$ mit $G = \langle a \rangle$

(insbesondere G abelsch)

Def: Sei $(G,\cdot)$ Gruppe, $a \in G$. Dann definiert man die <u>Ordnung</u> $\operatorname{ord}(a)$ von a als

$$\operatorname{ord}(a) := \begin{cases} \infty, & \text{falls } a^n \neq 1 \;\forall n \in \mathbb{N} \\ \min\{n \in \mathbb{N} : a^n = 1\} & \text{sonst} \end{cases}$$

Proposition

$(G,\cdot)$ Gruppe, endlich, $a \in G$. Dann gilt $\operatorname{ord}(a) \mid \operatorname{card} G$

Beweis

$$\langle a \rangle = \{a^k \;\; k \in \mathbb{Z}\} = \{1, a, a^2, \ldots, a^{n-1}\}$$

$n := \operatorname{ord}(a)$

hat n Elemente, weil

$a^{k_1} = a^{k_2} \;\; (0 \leq k_1 \leq k_2 < n) \Rightarrow 1 = a^{k_2 - k_1}$

$(0 \leq k_2 - k_1 < n) \Rightarrow k_2 - k_1 = 0 \Rightarrow k_2 = k_1$ somit

$\operatorname{ord}(a) = n = \operatorname{card}\langle a \rangle \mid \operatorname{card} G$ □

Korollar

$(G,\cdot)$ Gruppe, $n = \operatorname{card} G$, $a \in G \Rightarrow a^n = 1$

Beweis

$k = \operatorname{ord}(a) \Rightarrow k \mid n \Rightarrow a^n = (\underbrace{a^k}_{1})^{\frac{n}{k}} = 1$ □

Einfacher für abelsche Gruppen

$G = \{x_1, \dots, x_n\}$ $\quad a^n \cdot x_1 x_2 \dots x_n = (ax_1)(ax_2) \dots (ax_n) = x_1 \dots x_n$

$\Rightarrow a^n = 1$ □

Druckfehler bei den Beispielen:

ad Bsp 14 $\quad a \neq 0$ <u>oder</u> $b \neq 0$

ad Bsp 23 ... Abel'schen Gruppen ✗

U Untergruppe von G

$U \cdot U = U$

G/U Gruppe? $\quad (a \cdot U)(b \cdot U) = \underbrace{a \cdot U \cdot b}_{\text{falls } = b \cdot U} \cdot U = a \cdot b \cdot \underbrace{U \cdot U}_{=U} = a \cdot b \cdot U$

gilt im Allgemeinen NICHT Rechtsnebenklasse ≠ Linksnebenklasse

Def: Sei $(G, \cdot)$ eine Gruppe. Eine Untergruppe U heißt <u>Normalteiler</u>, falls $\forall a \in G : a \cdot U = U \cdot a$

Proposition

U Normalteiler $\Rightarrow$ G/U Gruppe

<u>Beweis</u>

$(aU)(bU) = a \cdot b \cdot U \in G/U$

Assoziativgesetz ✓

Einselement $= U \; (= 1 \cdot U) \qquad U \cdot (a \cdot U) = a \cdot U \cdot U = a \cdot U$

Inverses $(a \cdot U)^{-1} = a^{-1} \cdot U$ weil $a^{-1} \cdot U \; a \cdot U = \underbrace{a^{-1} \cdot a}_{=1} \underbrace{U \cdot U}_{=U} = U$ □

G/U heißt dann Faktorgruppe der Quotientengruppe

Def: Seien $(G_1, \cdot)$ $(G_2, \cdot)$ Gruppen, $\varphi : G_1 \to G_2$ eine Funktion

(1) φ heißt <u>Homomorphismus</u> (Gruppenhomomorphismus) falls

$\forall a, b \in G : \varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$

(2) φ heißt <u>Isomorphismus</u> falls φ ein Homomorphismus und bijektiv ist.

Proposition

φ Homomorphismus

(1) $\varphi(1) = 1$

(2) $\varphi(a^{-1}) = (\varphi(a))^{-1} \quad \forall a \in G_1$

(3) φ Isomorphismus $\Rightarrow \varphi^{-1}$ Isomorphismus

Beweis

(1) $\varphi(\underbrace{1}_{=1\cdot 1}) = \varphi(1)\cdot\varphi(1) \overset{\text{Kürzungsregel}}{\Rightarrow} 1 = \varphi(1)$

(2) $\varphi(a^{-1})\cdot\varphi(a) = \varphi(\underbrace{a^{-1}\cdot a}_{1}) \overset{(1)}{=} 1 \qquad |\cdot(\varphi(a))^{-1}$

$\Rightarrow \varphi(a^{-1}) = (\varphi(a))^{-1}$

(3) Seien $a,b \in G_2$

$\varphi(\varphi^{-1}(a)\,\varphi^{-1}(b)) = \underbrace{\varphi(\varphi^{-1}(a))}_{=a}\,\underbrace{\varphi(\varphi^{-1}(b))}_{=b} = a\cdot b$

$\Rightarrow \varphi^{-1}(a)\cdot\varphi^{-1}(b) = \varphi^{-1}(a\cdot b)$ □

Bsp

* $S_n, (\mathbb{R}\setminus\{0\}, \cdot) \qquad \operatorname{sgn}: S_n \to \mathbb{R}\setminus\{0\}$

$\operatorname{sgn}(\sigma\tau) = \operatorname{sgn}\sigma\cdot\operatorname{sgn}\tau$ d.h. Homomorphismus

* $(\mathbb{R}^+, \cdot), (\mathbb{R}, +) \qquad \log: \mathbb{R}^+ \to \mathbb{R}$

$\log(xy) = \log x + \log y$ d.h. ist Homomorphismus + bijektiv → Isomorphismus

Umkehrfkt: e^x

Def: $\varphi: G_1 \to G_2$ Homomorphismus $\quad \underline{\operatorname{im}\varphi} = \varphi(G_1) = \{x \in G_2 : \exists y \in G_1 \text{ mit } x = \varphi(y)\}$

Bild von φ, $\quad \underline{\ker\varphi} := \{x \in G_1 : \varphi(x) = 1\} = \varphi^{-1}(1)$ Kern von φ

Proposition

$\varphi: G_1 \to G_2$ Homomorphismus

(1) $\operatorname{im}\varphi$ Untergruppe von G_2

(2) $\ker\varphi$ ist Normalteiler von G_1

Beweis

(1) Seien $a, b \in \operatorname{im}\varphi$. $\exists x, y \in G_1 : \varphi(x) = a, \ \varphi(y) = b$

$\Rightarrow a \cdot b^{-1} = \varphi(x) \cdot \underbrace{\varphi(y)^{-1}}_{=\varphi(y^{-1})} = \varphi(\underbrace{x \cdot y^{-1}}_{\in G_1}) \in \operatorname{im}\varphi$

(2) seien $a, b \in \ker\varphi \Rightarrow \varphi(a) = \varphi(b) = 1$

$\varphi(ab^{-1}) = \varphi(a)\,\varphi(b)^{-1} = 1 \Rightarrow a \cdot b^{-1} \in \ker\varphi$

Sei $a \in G_1$. Sei $x \in a \cdot (\ker\varphi) \Rightarrow x = a \cdot \underbrace{y}_{\in \ker\varphi} =$

$= a \cdot y \cdot a^{-1} \cdot a$

$\varphi(a \cdot y \cdot a^{-1}) = \varphi(a) \cdot \underbrace{\varphi(y)}_{=1} \cdot \underbrace{\varphi(a^{-1})}_{=(\varphi(a))^{-1}} = 1$ weil φ Homomorphismus

$\Rightarrow a \cdot y \cdot a^{-1} \in \ker\varphi$

$\Rightarrow x \in (\ker\varphi) \cdot a$ □

$G_1 \overset{\text{isomorph}}{\cong} G_2$ falls es einen Isomorphismus $G_1 \to G_2$ gibt

Proposition

$\varphi : G_1 \to G_2$ Homomorphismus. Dann gilt $G/\ker\varphi \cong \operatorname{im}\varphi$

Beweis

$\Psi : G/\ker\varphi \to \operatorname{im}\varphi$ durch $\Psi(a \cdot \ker\varphi) := \underbrace{\varphi(a)}_{\in \operatorname{im}\varphi}$

müssen zeigen, dass Ψ eine Funktion ist!

wir zeigen Ψ ist injektive Funktion

$a \cdot \ker\varphi = b \cdot \ker\varphi \iff b^{-1} \cdot a \in \ker\varphi \iff \underbrace{\varphi(b^{-1} \cdot a)}_{=(\varphi(b))^{-1}\cdot\varphi(a)} = 1$

$\iff \varphi(a) = \varphi(b) \iff \Psi(a \cdot \ker\varphi) = \Psi(b \ker\varphi)$

$\Psi(\underbrace{(a \ker\varphi)\,(b \ker\varphi)}_{=a\cdot b \ker\varphi}) = \varphi(a \cdot b) = \varphi(a) \cdot \varphi(b) = \Psi(a \ker\varphi)\,\Psi(b \ker\varphi)$

surjektiv: sei $x \in \operatorname{im}\varphi \Rightarrow \exists a \in G_1 : x = \varphi(a) = \Psi(a \cdot \ker\varphi)$

also Ψ ist Isomorphismus □

$U \leq G$ Normalteiler. Dann ist $\varphi : G \to G/U$, $\varphi(a) := a \cdot U$ ein Homomorphismus mit $\ker\varphi = U$, $\operatorname{im}\varphi = G/U$

Def: Sei $(G,\cdot)$ eine Gruppe. Dann nennt man $D(G) := \langle \{aba^{-1}b^{-1} : a,b \in G\} \rangle$ Kommutatorgruppe von G.

Bemerkung:

G Abel'sch $\Rightarrow D(G) = \{1\}$ $\quad (a \underbrace{b \cdot a^{-1}}_{=a^{-1}\cdot b} \cdot b^{-1} = 1)$

Proposition

$(G,\cdot)$ Gruppe

(1) $D(G)$ ist ein Normalteiler von G

(2) $G/D(G)$ ist Abel'sch

Beweis

(1) sei $a \in G$, Sei $x \in a \cdot D(G) \Rightarrow \exists y \in D(G)$ mit $x = a \cdot y$

$x = a \cdot y = a \cdot y \cdot a^{-1} \cdot y^{-1} \cdot y \cdot a = \underbrace{(\underbrace{a \cdot y \cdot a^{-1} \cdot y^{-1}}_{\in D(G)} \cdot \underbrace{y}_{\in D(G)} \cdot a}_{\in D(G)} \in D(G) \cdot a$

analog umgekehrt

also $D(G)$ Normalteiler

(2) Seien $a,b \in G$

$(a\,D(G))\,(b\,D(G)) = a \cdot b \cdot D(G) = (*)$

Sei $x \in a \cdot b \cdot D(G) \Rightarrow \exists y \in D(G) : x = a \cdot b \cdot y$

$x = a \cdot b \cdot y = b \cdot a \cdot a^{-1} \cdot b^{-1} \cdot a \cdot b \cdot y = b \cdot a \underbrace{(\underbrace{a^{-1} \cdot b^{-1} \cdot a \cdot b}_{\in D(G)} \underbrace{y}_{\in D(G)})}_{\in D(G)} \in b \cdot a \cdot D(G)$

$(*) = b \cdot a \cdot D(G) = (b\,D(G))\,(a\,D(G))$ □

Proposition

$(G,\cdot)$ Gruppe, $(\tilde{G},\cdot)$ Abel'sche Gruppe, $\varphi : G \to \tilde{G}$ Homomorphismus

Dann gilt $\ker \varphi \supseteq D(G)$

Beweis

Seien $a,b \in G$

$\varphi(aba^{-1}b^{-1}) = \varphi(a) \cdot \underbrace{\varphi(b) \cdot \varphi(a)^{-1}}_{=\varphi(a)^{-1}\cdot\varphi(b)} \cdot \varphi(b)^{-1} = 1$

$\Rightarrow a \cdot b \cdot a^{-1} \cdot b^{-1} \in \ker \varphi \Rightarrow D(G) \leq \ker \varphi$ □

Proposition

Für $n \in \mathbb{N}$ ist $D(S_n) = A_n$ (gerade Permutationen, sgn = 1)

Beweis

seien $\sigma, \tau \in S_n$

$\operatorname{sgn}(\sigma \tau \sigma^{-1} \tau^{-1}) = \operatorname{sgn}\sigma \cdot \operatorname{sgn}\tau \cdot \operatorname{sgn}\sigma \cdot \operatorname{sgn}\tau = 1$

$\Rightarrow \sigma \tau \sigma^{-1} \tau^{-1} \in A_n \Rightarrow D(S_n) \leq A_n$

$n = 1, 2$ ✓

$n \geq 3$ Sei $(x_1\ x_2\ x_3)$ ein Dreierzyklus

$$\underbrace{(x_1\ x_2)\,(x_1\ x_3)\,\underbrace{(x_1\ x_2)^{-1}}_{=(x_1\ x_2)}\,\underbrace{(x_1\ x_3)^{-1}}_{=(x_1\ x_3)}}_{\in D(S_n)} = (x_1\ x_2\ x_3)$$

$\sigma \in A_n \Rightarrow \sigma = \underbrace{\tau_1 \tau_2 \dots \tau_k}_{\text{Dreierzyklen}} \in D(S_n) \Rightarrow A_n \leq D(S_n)$

somit $D(S_n) = A_n$ □

Proposition

Sei $n \in \mathbb{N}$, $n \geq 5$. Dann ist $D(A_n) = A_n$

Beweis

$D(A_n) \leq A_n$

sei $(x_1\ x_2\ x_3)$ ein Dreierzyklus. Wähle $x_4 \neq x_5 \in \{1, 2, \dots, n\} \setminus \{x_1, x_2, x_3\}$

$$\underbrace{(x_1\ x_2\ x_4)\,(x_1\ x_3\ x_5)\,\underbrace{(x_1\ x_2\ x_4)^{-1}}_{=(x_1\ x_4\ x_2)}\,\underbrace{(x_1\ x_3\ x_5)^{-1}}_{=(x_1\ x_5\ x_3)}}_{\in D(A_n)} = (x_1\ x_2\ x_3)$$

sei $\sigma \in A_n \Rightarrow \sigma = \underbrace{\tau_1 \cdot \tau_2 \cdot \dots \cdot \tau_k}_{\text{Dreierzyklen}} \in D(A_n)$

daher $A_n \leq D(A_n)$, somit $D(A_n) = A_n$ □

Def: Sei G eine Gruppe. Setze $D^{(1)}(G) := D(G)$ und für $n > 1$ $D^{(n)}(G) := D(D^{(n-1)}(G))$. Dann heißt G auflösbar, falls es ein $n \in \mathbb{N}$ mit $D^{(n)}(G) = \{1\}$ gibt.

Proposition

G ist genau dann auflösbar, wenn $G_0 := G \geq G_1 \geq \dots \geq G_n = \{1\}$ sodass $\forall j \in \{1, 2, \dots, n\}$ G_j ist Normalteiler von G_{j-1} und G_{j-1}/G_j ist Abel'sch

Beweis

($\Rightarrow$) $G_0 := G$, $G_j := D^{(j)}(G)$

$G_0 \geq G_1 \geq \dots \geq G_n = \{1\}$ Sei $j \in \{1, 2, \dots, n\}$

$G_j = \underbrace{D^{(j)}(G)}_{D(D^{(j-1)}(G))} = D(G_{j-1})$ Normalteiler in G_{j-1}

G_{j-1}/G_j Abel'sch

($\Leftarrow$) Behauptung $\forall j \in \{1, \dots, n\}$ ist $D^{(j)}(G) \leq G_j$

Beweis der Behauptung: Induktion

$j=1$: $G_0/G_1 = G/G_1$ Abelsch $\Rightarrow G_1 = \ker \varphi \geq D(G) = D^{(1)}(G)$

Sei $j \in \{2, \dots, n\}$ $D^{(j-1)}(G) \leq G_{j-1}$

G_{j-1}/G_j Abelsch $\Rightarrow G_j = \ker \varphi \geq D(\underbrace{G_{j-1}}_{\geq D^{(j-1)}(G)}) \geq D(D^{(j-1)}(G)) = D^{(j)}(G)$ ◇

insbesondere $D^{(n)}(G) \leq G_n = \{1\} \Rightarrow D^{(n)}(G) = \{1\}$

$\Rightarrow G$ auflösbar □

Proposition

Sei $n \geq 5$. Dann ist S_n nicht auflösbar

Beweis $D^{(1)}(S_n) = D(S_n) = A_n$

$D^{(2)}(S_n) = D(\underbrace{D^{(1)}(S_n)}_{A_n}) = A_n$

$\vdots$

$D^{(k)}(S_n) = D(\underbrace{D^{(k-1)}(S_n)}_{A_n}) = A_n$

□

Proposition

S_3 und S_4 sind auflösbar

Beweis

S_4 ... Proseminar

S_3: $D^{(1)}(S_3) = A_3 = \{id, (1\,2\,3), (1\,3\,2)\}$

$(1\,2\,3)^1 = (1\,2\,3)$

$(1\,2\,3)^2 = (1\,3\,2)$

$(1\,2\,3)^3 = id \Rightarrow \operatorname{ord}(1\,2\,3) = 3$

$\Rightarrow \langle (1\,2\,3) \rangle = A_3 \Rightarrow A_3$ ist zyklisch $\Rightarrow A_3$ ist Abelsch

$\Rightarrow D^{(2)}(S_n) = D(A_3) = \{id\} \Rightarrow S_3$ auflösbar $\square$

2) Ringe

Def: eine nichtleere Menge R mit 2 Operationen $+$ und $\cdot$ heißt Ring falls $(R,+)$ ist Abelsche Gruppe, die Multiplikation ist assoziativ und es gelten die Distributivgesetze

$\forall a,b,c \in R: (a+b)\cdot c = a\cdot c + b\cdot c$ und $c\cdot(a+b) = c\cdot a + c\cdot b$

Proposition

$(R,+,\cdot)$ Ring, $a \in R \Rightarrow 0\cdot a = a\cdot 0 = 0$

Beweis

$$a\cdot 0 = \underbrace{0}_{=-(a0)+a0} + a\cdot 0 = -a0 + \underbrace{a0 + a0}_{=a(0+0)} = -a0 + a0 = 0$$

$\square$

Proposition

$(R,+,\cdot)$ Ring, $a,b \in R \Rightarrow (-a)b = -a\cdot b = a\cdot(-b)$

Beweis

$$a(-b) + ab = a\cdot\underbrace{(-b+b)}_{0} = a\cdot 0 = 0$$

$\Rightarrow a\cdot(-b) = -a\cdot b$ $\square$

Def: ein Ring $(R,+,\cdot)$ heißt

(1) Ring mit Einselement falls $\exists 1 \in R: 1a = a\cdot 1 = a \ \forall a \in R$ und $1 \neq 0$

(2) kommutativer Ring falls die Multiplikation kommutativ ist

(3) kommutativer Ring mit Einselement ...

(4) Schiefkörper, falls R Ring mit Eins und $\forall a \in R, a \neq 0 \; \exists a^{-1} \in R$ mit $a^{-1} \cdot a = a \cdot a^{-1} = 1$ (engl: division ring, ital: corpo)

NICHT: kommutativ gesetzt bzgl Multiplikation

(5) Körper, falls R kommutativer Ring mit Eins ist und $\forall a \in R$ mit $a \neq 0 \; \exists a^{-1} \in R : a^{-1} \cdot a = 1$ (kommutativer Schiefkörper)

(englisch: field, ital: campo)

Beispiele für Ringe

- $\mathbb{Z}$ kR1 = kommutativer Ring mit 1
- $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ Körper
- $\mathbb{Z}_n$ (Restklassen modulo n) kR1 (Körper wenn n Primzahl)
- $M_n\begin{pmatrix} \mathbb{R} \\ \mathbb{C} \end{pmatrix}$ $n \times n$ Matrizen R1 NICHT kommutativ
- $\mathbb{H}$ Quaternionen

  $\mathbb{H} := \{a_1 + i a_2 + j a_3 + k a_4 : a_1, a_2, a_3, a_4 \in \mathbb{R}\}$

  $i^2 = j^2 = k^2 = -1$, $i \cdot j = k = -j \cdot i$, $j \cdot k = i = -k \cdot j$, $k \cdot i = j = -i \cdot k$

  Schiefkörper
- $\mathbb{Z}[\sqrt{2}] := \{a + b\sqrt{2}, a, b \in \mathbb{Z}\}$ kR1

  $\mathbb{Z}[\sqrt{-2}]$, $\mathbb{Z}[\sqrt{-5}]$

Def Sei $(R, +, \cdot)$ ein Ring mit Eins. Dann heißt $a \in R$ eine Einheit falls $\exists x, y \in R$ mit $x \cdot a = a \cdot y = 1$. Man definiert

$R^* := \{a \in R : a \text{ Einheit}\}$

$0 \notin R^*$ d.h. keine Einheit, angen. $0 \in R^* \Rightarrow \exists x : 1 = 0 \cdot x = 0$ ↯ WID

Proposition

Sei $(R, +, \cdot)$ ein Ring mit Eins, dann ist $(R^*, \cdot)$ Gruppe.

Beweis
Proseminar

Sei $a \in R^* \Rightarrow \exists x, y \in R$ mit $x \cdot a = a \cdot y = 1$

$x = x \cdot \underbrace{1}_{a \cdot y} = \underbrace{x \cdot a}_{=1} \cdot y = 1 \cdot y = y$

zu x gibt es ein Element, nämlich a mit $a \cdot x = x \cdot a = 1$ und

somit $x \in R^*$ □

- $\mathbb{Z}^* = \{1, -1\}$
- $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$
- K Schiefkörper $\Rightarrow K^* = K \setminus \{0\}$
- $M_n^* = GL_n$ invertierbare Matrizen
- $\mathbb{Z}[\sqrt{2}]$: $(1+\sqrt{2}) \cdot (-1+\sqrt{2}) = 1$

  $(1+\sqrt{2})^n \cdot (-1+\sqrt{2})^n = 1$ $\quad 1 < 1+\sqrt{2} < (1+\sqrt{2})^2 < \dots$

  $\Rightarrow \mathbb{Z}[\sqrt{2}]^*$ hat ∞ viele (abzählbar) Elemente
- $\mathbb{Z}[\sqrt{-5}]^* = \{-1, 1\}$

Sei $a + b\sqrt{-5}$ Einheit $\Rightarrow 1 = (a+b\sqrt{-5}) \cdot (x + y\sqrt{-5})$

$1 = (a - b\sqrt{-5}) \cdot (x - y\sqrt{-5})$

$\Rightarrow 1 = (a^2 + 5b^2) \cdot \underbrace{(x^2 + 5y^2)}_{\geq 1} \geq a^2 + 5b^2$

angen: $b \neq 0 \rightarrow \underbrace{a^2 + 5b^2}_{5 \leq} \leq 1$ ↯ wid $\Rightarrow b = 0$

$a^2 \leq 1 \Rightarrow a = \pm 1$

- $\mathbb{Z}[\sqrt{-1}]^* = \{1, -1, i, -i\}$

Def: $U \subseteq R$, R Ring heißt Unterring falls U Ring ist

Proposition

R Ring, $U \subseteq R$, $U \neq \emptyset$ U ist Unterring $\Leftrightarrow \forall a, b \in R : a - b \in$ und $a \cdot b \in U$

analog wie bei Gruppen $R/U = \{a + U : a \in R\}$

$(a+U)\cdot(b+U) = (\text{wollen} = a\cdot b + U)$

$= a\cdot b + aU + U\cdot b + \underbrace{U\cdot U}_{\subseteq U}$

Def: Sei $(R,+,\cdot)$ ein Ring, $I \subseteq R$, $I \neq \emptyset$

1) I heißt <u>Linksideal</u>, falls I Unterring $(\forall a,b \in I : a-b \in I)$
und $\forall a \in I \ \forall r \in R : r\cdot a \in I$

2) I heißt <u>Rechtsideal</u> ...

3) I heißt <u>Ideal</u> falls I Links- und Rechtsideal ist
(d.h. $\forall a,b \in I : a-b \in I$, $\forall a \in I \ r \in R : a\cdot r, r\cdot a \in I$)

<u>weitere Eigenschaften</u>

* I Ideal, $a,b \in I$, $x,y \in R \Rightarrow a\cdot x \pm y\cdot b \in I$
* $\{0\}$, R sind stets Ideale (trivialen Ideale)
im Schiefkörper sind die einzigen Ideale die trivialen
siehe Kopie!
* R Ring mit Eins, I Ideal, $1 \in I \Rightarrow I = R$

Beweis: $a \in R$: $a = a\cdot \underbrace{1}_{\in I} \in I$

Proposition

$(R,+,\cdot)$ Ring, I Ideal in $R \Rightarrow {}^{R}/_{I}$ ist ein Ring

<u>Beweis</u>

$(a+I)+(b+I) = (a+b)+I$ ✓

$(a+I)\cdot(b+I) = a\cdot b + I$ .... □

Proposition

Sei $(R,+,\cdot)$ ein Ring, $(I_j)_{j\in J}$ beliebige Familie von Idealen in R. Dann ist $\bigcap_{j\in J} I_j$ Ideal

<u>Beweis</u>

Seien $a,b \in I = \bigcap_{j\in J} I_j$ Sei $j \in J \Rightarrow a,b \in I_j \Rightarrow a-b \in I_j$

$\Rightarrow a-b \in I$

$a \in I$, $r \in R$ Sei $j \in J \Rightarrow a \in I_j \Rightarrow r\cdot a, a\cdot r \in I_j \Rightarrow$

$\Rightarrow r\cdot a, a\cdot r \in I$

□

Ideale in Matrizenalgebren

Für $n \in \mathbb{N}$ und $j, k \in \{1, 2, \ldots, n\}$ definiere die $n \times n$-Matrix $1_{j,k} := (a_{p,q})_{p,q=1}^{n}$ durch

$$a_{p,q} := \begin{cases} 1, & \text{falls } (p,q) = (j,k), \\ 0, & \text{falls } (p,q) \neq (j,k). \end{cases}$$

Es ist also $1_{j,k}$ die Matrix, die 1 als (j,k)-te Eintragung und sonst nur die Eintragungen 0 hat.

Proposition 1. *Sei $(K, +, \cdot)$ ein Körper und $n \in \mathbb{N}$. Weiters sei I ein Ideal im Ring $M_n(K)$ der $n \times n$-Matrizen über K. Dann ist $I = \{0\}$ oder $I = M_n(K)$.*

Beweis. Es sei $I \subseteq M_n(K)$ ein Ideal mit $I \neq \{0\}$. Daher gibt es ein $A := (A_{p,q})_{p,q=1}^{n} \in I$ mit $A \neq 0$. Weil $A \neq 0$ ist, gibt es eine Eintragung von A, die nicht 0 ist, also es gibt $j, k \in \{1, 2, \ldots, n\}$ mit $A_{j,k} \neq 0$.

Sei $r \in \{1, 2, \ldots, n\}$. Setze $C_1 := 1_{r,j}$ und $C_2 := \frac{1}{A_{j,k}} 1_{k,r}$. Nachdem I ein Ideal ist, ist $C_1 A C_2 \in I$. Es ist $C_1 A C_2 = 1_{r,r}$ und somit ist $1_{r,r} \in I$. Weil I ein Ideal ist, ist $\sum_{r=1}^{n} 1_{r,r} \in I$. Offensichtlich ist $\sum_{r=1}^{n} 1_{r,r} = \mathrm{id}$ und deshalb ist $\mathrm{id} \in I$.

Jetzt sei $B \in M_n(K)$ beliebig. Da I ein Ideal ist und $\mathrm{id} \in I$ gilt, ergibt sich, dass $B = \mathrm{id} \cdot B \in I$. Daher ist $I = M_n(K)$. □

Bemerkung. Für $n \geq 2$ ist $M_n(K)$ kein Schiefkörper. Um das zu zeigen betrachte $N := 1_{1,n}$. Dann ist $N \neq 0$ und $N \cdot N = N^2 = 0$. Deswegen ist N ein Nullteiler. Nachdem es in einem Schiefkörper keine Nullteiler gibt, kann $M_n(K)$ kein Schiefkörper sein.

Bemerkung. Wenn $(S, +, \cdot)$ ein Schiefkörper ist, dann sind $\{0\}$ und S die einzigen Ideale in S. Nach Proposition 1 ist die Umkehrung im Allgemeinen nicht richtig, also es gibt Ringe $(R, +, \cdot)$ mit Eins, die nur $\{0\}$ und R als Ideale haben, aber keine Schiefkörper sind.

Bemerkung. Anders ist die Situation im kommutativen Fall. Ein kommutativer Ring $(R, +, \cdot)$ mit nichttrivialer Multiplikation ist genau dann ein Körper, wenn $\{0\}$ und R die einzigen Ideale in R sind. Dabei heißt die Multiplikation nichttrivial, falls es $a, b \in R$ gibt, sodass $ab \neq 0$. Aus dieser Definition ergibt sich, dass ein kommutativer Ring mit nichttrivialer Multiplikation mindestens zwei Elemente enthalten muss.

Bemerkung. Insbesondere ist ein kommutativer Ring $(R, +, \cdot)$ mit Eins genau dann ein Körper, wenn $\{0\}$ und R die einzigen Ideale in R sind.

Bemerkung. Jetzt zeigen wir, dass ein kommutativer Ring $(R, +, \cdot)$ mit nichttrivialer Multiplikation, der nur $\{0\}$ und R als Ideale hat, ein Einselement besitzt, also ein kommutativer Ring mit Eins ist. Weil die Multiplikation nichttrivial ist, gibt es $a, b \in R$ mit $ab \neq 0$. Deshalb ist $a \neq 0$. Betrachte jetzt die Menge aR. Falls $x, y \in aR$, dann gibt es $\widetilde{x}, \widetilde{y} \in R$ mit $x = a\widetilde{x}$ und $y = a\widetilde{y}$. Dann ist $x - y = a(\underbrace{\widetilde{x} - \widetilde{y}}_{\in R}) \in aR$. Wenn $x \in aR$ und $y \in R$, dann gibt es ein $\widetilde{x} \in R$ mit $x = a\widetilde{x}$. Es ist dann $yx = ya\widetilde{x} = a\underbrace{y\widetilde{x}}_{\in R} \in aR$. Daher ist aR ein Ideal in R. Nachdem $ab \neq 0$ und $ab \in aR$, ist $aR \neq \{0\}$. Somit muss $aR = R$ gelten. Da $a \in R = aR$, gibt es ein $1 \in R$ mit $a = a1 = 1a$. Sei $x \in R$. Dann ist $x \in aR$ und deshalb gibt es ein $y \in R$ mit $x = ay$. Deshalb gilt $1x = 1\underbrace{x}_{=ay} = \underbrace{1a}_{=a} y = ay = x$ und wegen der Kommutativität auch $x1 = x$.

Def: Sei $(R,+,\cdot)$ ein Ring, $A \subseteq R$ $(A \neq \emptyset)$. Dann heißt

$(A) := \bigcap_{\substack{I \supseteq A \\ I \text{ Ideal}}}$ das von A erzeugte Ideal

(kleinstes Ideal das A enthält)

$(\{a_1, a_2, \dots, a_n\}) =: (a_1, \dots, a_n)$ da bequemer

$(\{a\}) =: (a)$

Def: (1) ein Ideal I heißt Hauptideal, falls $\exists\, a \in R : I = (a)$
Ideal das nur von einem Element erzeugt wird, heißt HI

(2) R heißt Hauptidealring, falls jedes Ideal Hauptideal ist
jeder Körper, Schiefkörper ist HIR

Proposition

Sei $(R,+,\cdot)$ ein kommutativer Ring mit Eins

(1) Seien $a_1, \dots, a_n \in R$ dann ist $(a_1, \dots, a_n) = \sum_{j=1}^{n} a_j R = a_1 R + \dots + a_n R$

(2) Für $a \in R$ ist $(a) = a \cdot R$

Beweis

offensichtlich (1) $\Rightarrow$ (2)

Setze $I := (a_1, \dots, a_n)$ $\quad J := \sum_{j=1}^{n} a_j \cdot R$ wollen zeigen dass $I = J$

seien $a, b \in J \Rightarrow \exists\, x_1, \dots, x_n, y_1, \dots, y_n \in R$ mit $a = \sum_{j=1}^{n} a_j \cdot x_j$

$b = \sum_{j=1}^{n} a_j \cdot y_j$

$$a - b = \sum_{j=1}^{n} a_j \underbrace{(x_j - y_j)}_{\in R} \quad \in J$$

sei $a \in J$ und $r \in R \Rightarrow \exists\, x_1, \dots, x_n \in R$ mit $a = \sum_{j=1}^{n} a_j \cdot x_j$

$$\Rightarrow a \cdot r = \sum_{j=1}^{n} a_j \cdot \underbrace{x_j \cdot r}_{\in R} \quad \in J \Rightarrow J \text{ ist Ideal}$$

sei $j \in \{1, 2, \dots, n\}$ $\quad a_j = 0 \cdot a_1 + \dots + 0 \cdot a_{j-1} + 1 \cdot a_j + 0 \cdot a_{j+1} + \dots + 0 \cdot a_n \quad \in J$

$\Rightarrow I \subseteq J$

sei $x \in J \Rightarrow \exists\, x_1, \dots, x_n \in R$ mit $x = \underbrace{a_1}_{\in I} \underbrace{x_1}_{\in I} + \dots + \underbrace{a_n}_{\in I} \underbrace{x_n}_{\in I} \quad \in I$

$\Rightarrow J \subseteq I \qquad \Rightarrow I = J$ $\qquad \square$

$\varphi : R \to R/I \quad : \varphi(a) := a + I$ ist (surjektiver) Homomorphismus

$\ker \varphi = I$

Def: Seien $(R_1, +, \cdot)$, $(R_2, +, \cdot)$ Ringe $\varphi : R_1 \to R_2$ heißt

(Ring-) Homomorphismus falls $\forall a, b \in R_1 : \varphi(a+b) = \varphi(a) + \varphi(b)$

und $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$

weitere Eigenschaften:

* $\varphi(0) = 0$, $\varphi(-a) = -\varphi(a)$
* $(R_1, +, \cdot)$ Ring mit Eins falls $\varphi(1) = 0 \Rightarrow \varphi = 0$ (Nullabbildung), weil:

  sei $a \in R_1 \Rightarrow \varphi(a) = \varphi(1 \cdot a) = \underbrace{\varphi(1)}_{=0} \cdot \varphi(a) = 0$

  ! im Allgemeinen ist $\varphi(1) = 1$ NICHT richtig (auch für $\varphi \neq 0$)

Def: ein bijektiver Homomorphismus heißt (Ring-) Isomorphismus

Proposition

(1) φ_1, φ_2 Homomorph. $\Rightarrow \varphi_2 \circ \varphi_1$ Homomorph.

(2) φ Isomorph. $\Rightarrow \varphi^{-1}$ Isomorph.

Beweis

(1) Proseminar

(2) z.z. φ^{-1} Homomorphismus

seien $a, b \in R_2$ $\varphi(\varphi^{-1}(a) \cdot \varphi^{-1}(b)) = \underbrace{\varphi(\varphi^{-1}(a))}_{=a} \cdot \underbrace{\varphi(\varphi^{-1}(b))}_{b} = a \cdot b$

$\Rightarrow \varphi^{-1}(a) \cdot \varphi^{-1}(b) = \varphi^{-1}(a \cdot b)$ □

Def: Seien $(R_1, +, \cdot)$, $(R_2, +, \cdot)$ Ringe, $\varphi : R_1 \to R_2$ ein Homomorphismus,

$\operatorname{im} \varphi := \varphi(R_1) = \{x \in R_2 : \exists y \in R_1 \text{ mit } \varphi(y) = x\}$ und

$\ker \varphi := \{x \in R_1 : \varphi(x) = 0\}$

Proposition

(1) $\operatorname{im}\varphi$ Unterring von R_2

(2) $\ker\varphi$ Ideal in R_1

Beweis

(1) $a,b \in \operatorname{im}\varphi \Rightarrow \exists x,y \in R_1 : a=\varphi(x),\ b=\varphi(y) \Rightarrow$

$\Rightarrow a-b = \varphi(x)-\varphi(y) = \varphi(\underbrace{x-y}_{\in R_1}) \in \operatorname{im}\varphi$

$a\cdot b = \varphi(x)\cdot\varphi(y) = \varphi(\underbrace{x\cdot y}_{\in R_1}) \in \operatorname{im}\varphi$

(2) Seien $a,b \in \ker\varphi \Rightarrow \varphi(a)=\varphi(b)=0 \Rightarrow$

$\Rightarrow 0 = \varphi(a)-\varphi(b) = \varphi(a-b) \Rightarrow a-b \in \ker\varphi$

Seien $a \in \ker\varphi,\ r \in R_1 \quad \varphi(r\cdot a) = \varphi(r)\cdot\underbrace{\varphi(a)}_{=0} = 0 \Rightarrow r\cdot a \in \ker\varphi$

analog $a\cdot r \in \ker\varphi$

$\Rightarrow \ker\varphi$ ist Ideal $\square$

Proposition

Seien $(R_1,+,\cdot)$, $(R_2,+,\cdot)$ Ringe, $\varphi: R_1 \to R_2$ Homomorphismus. Dann ist $R_1/\ker\varphi$ isomorph zu $\operatorname{im}\varphi$

Beweis

$\psi: R_1/\ker\varphi \to \operatorname{im}\varphi, \quad \psi(a+\ker\varphi) = \varphi(a) \in \operatorname{im}\varphi$

$a+\ker\varphi = b+\ker\varphi \Leftrightarrow a-b \in \ker\varphi \Leftrightarrow 0=\varphi(a-b)=\varphi(a)-\varphi(b)$

$\Leftrightarrow \psi(a+\ker\varphi) = \varphi(a) = \varphi(b) = \psi(b+\ker\varphi)$

ψ injektive Funktion

$\psi((a+\ker\varphi)+(b+\ker\varphi)) = \psi((a+b)+\ker\varphi) = \varphi(a+b) = \varphi(a)+\varphi(b) =$

$= \psi(a+\ker\varphi) + \psi(b+\ker\varphi)$

$\psi((a+\ker\varphi)\cdot(b+\ker\varphi)) = \psi(ab+\ker\varphi) = \varphi(a\cdot b) = \varphi(a)\cdot\varphi(b) =$

$= \psi(a+\ker\varphi)\cdot\psi(b+\ker\varphi)$

$\square$

Bsp

$\mathbb{Z}, \quad \overbrace{n\cdot\mathbb{Z}}^{=(n)} = \{k \in \mathbb{Z} : n \mid k\}$ ist Ideal in $\mathbb{Z}$

$\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$ Restklassen mod n

Proposition

$(R_1, +, \cdot)$, $(R_2, +, \cdot)$ Ringe, $\varphi: R_1 \to R_2$ Isomorphismus

(1) R_1 Ring mit Eins $\Rightarrow R_2$ Ring mit Eins und $\varphi(1) = 1$

(2) R_1 Schiefkörper $\Rightarrow R_2$ Schiefkörper, $\varphi(1) = 1$ und $\varphi(a^{-1}) = (\varphi(a))^{-1}$ $\forall a \neq 0$

(3) R_1 Körper $\Rightarrow R_2$ Körper, $\varphi(1) = 1$ und $\varphi(a^{-1}) = (\varphi(a))^{-1}$

Beweis

offensichtlich (2) $\Rightarrow$ (3)

(1) sei $a \in R_2$ Setze $x = \varphi^{-1}(a) \in R_1$

$\varphi(1) \cdot \underbrace{a}_{=\varphi(x)} = \varphi(1 \cdot \underbrace{x}_{x}) = \varphi(x) = a$ analog $a \cdot \varphi(1) = a$

damit $\varphi(1)$ ist Einselement in R_2

(2) wegen (1) hat R_2 Eins und $\varphi(1) = 1$

sei $a \neq 0$ (in R_2) $\quad \underset{\neq 0}{x} = \varphi^{-1}(a)$ $(\varphi(x) = a)$

$\exists x^{-1} \in R_1$ mit $x^{-1} \cdot x = x \cdot x^{-1} = 1 \Rightarrow$

$\Rightarrow 1 = \varphi(1) = \varphi(x^{-1} \cdot x) = \varphi(x^{-1}) \cdot \underbrace{\varphi(x)}_{a}$ analog $\underbrace{\varphi(x)}_{a} \cdot \varphi(x^{-1}) = 1$

$\varphi(x^{-1}) = (\varphi(x))^{-1}$ □

Bsp $\mathbb{Z}_{10}$: Restklassen mod 10 $\quad 4 \neq 0$, $5 \neq 0$

$4 \cdot 5 = 0$

$\varphi: \mathbb{Z}_{10} \to \mathbb{Z}_{10}$: $\varphi(x) = 5x$ ist Homomorphismus weil:

$\varphi(x+y) = 5 \cdot (x+y) = 5x + 5y = \varphi(x) + \varphi(y)$ und

$\underbrace{\varphi(x)}_{5x} \cdot \underbrace{\varphi(y)}_{5y} = \underbrace{25}_{=5} xy = 5 \cdot xy = \varphi(x \cdot y)$!

da mod 10

$\varphi(1) = 5 \neq 1$ Homomorph wo 1 nicht auf 1 abgebildet

Def: Sei $(R, +, \cdot)$ Ring, $a \in R$, Dann heißt a <u>Nullteiler</u>, falls

$a \neq 0$ und $\exists b \in R$, $b \neq 0$ mit $a \cdot b = 0$ oder $b \cdot a = 0$

Def: (1) ein Ring heißt <u>nullteilerfrei</u>, falls es in R keine Nullteiler gibt

(2) R heißt <u>Integritätsbereich</u> (Integritätsring) falls R ein nullteilerfreier kommutativer Ring mit Eins ist

Kürzungsregel

Proposition

Sei $(R,+,\cdot)$ ein nullteilerfreier Ring!, $a,b,x \in R$, $x \neq 0$!

(1) $x \cdot a = x \cdot b \Rightarrow a = b$

(2) $a \cdot x = b \cdot x \Rightarrow a = b$

Beweis

$$x \cdot a = x \cdot b \Rightarrow 0 = x \cdot b - x \cdot a = \underbrace{x}_{\neq 0} \cdot (b-a) \Rightarrow b - a = 0 \Rightarrow a = b$$

(2) analog □

Proposition

Sei $(R_1,+,\cdot)$ ---------- Ring mit Eins, $(R_2,+,\cdot)$ nullteilerfreier Ring mit Eins,

$\varphi: R_1 \to R_2$ Homomorphismus, $\varphi \neq 0$ Dann gilt $\varphi(1) = 1$

Beweis

$$1 \cdot \varphi(1) = \varphi(\underbrace{1}_{=1\cdot 1}) = \varphi(1) \cdot \varphi(1) \overset{\text{Kürzungsregel}}{\Rightarrow} 1 = \varphi(1)$$ □

Proposition

Sei $n \in \mathbb{N}$, $n \geq 2$. Dann sind äquivalent

(1) $\mathbb{Z}_n$ ist nullteilerfrei (Integritätsbereich)

(2) $\mathbb{Z}_n$ ist Körper

(3) n ist Primzahl

Beweis

(2) $\Rightarrow$ (1) ✓

(1) $\Rightarrow$ (3) angen. $n \notin \mathbb{P} \Rightarrow n = n_1 \cdot n_2$ $\quad 1 \leq n_1, n_2 \leq n-1$

$n_1 \cdot n_2 \equiv 0 \mod n \Rightarrow n_1$ Nullteiler ↯ WID

(3) $\Rightarrow$ (2) $k \in \mathbb{Z}_n$, $k \neq 0$ $\quad (k \in \{1,2,\dots,n-1\})$

$ggT(k,n) = 1 \Rightarrow \exists\, a,b$ mit $a \cdot k + b \cdot n = 1$

$\Rightarrow a \cdot k \equiv 1 \mod n \Rightarrow a = k^{-1}$ □

Allgemein gilt: a Nullteiler $\Rightarrow a \notin R^*$, weil:

$a \in R^* \Rightarrow \exists x : x \cdot a = 1$ $\quad \exists\, b \overset{\neq 0}{} \text{ mit } a \cdot b = 0$

$0 = x \cdot a \cdot b$

$0 = x \cdot \underbrace{a \cdot b}_{=0} = \underbrace{x \cdot a}_{=1} \cdot b = b$ ↯ WID

Polynomringe

Def: Sei $(R, +, \cdot)$ kommutativer Ring. $\{(a_n)_{n\in\mathbb{N}} = (a_0, a_1, \ldots) : a_n \in R \ \forall n \in \mathbb{N}_0\}$ sind die formalen Potenzreihen über R

$(a_n) + (b_n) := (a_n + b_n)$ komponentenweise $(a_0, a_1, \ldots) + (b_0, b_1, \ldots) := a_0 + b_0, a_1 + b_1, \ldots$

$(a_n) \cdot (b_n) := (c_n)_{n\in\mathbb{N}_0}$, wobei für $n \in \mathbb{N}_0$: $c_n := \sum_{k=0}^{n} a_k \cdot b_{n-k}$

Proposition

Formale Potenzreihen sind kommutativer Ring. Falls R Einselement hat, dann auch die formalen Potenzreihen

Beweis Addition ✓, Kommutativität - Multiplikation ✓

Distributivgesetz: $(a_n) \cdot (\underbrace{(b_n) + (c_n)}_{(b_n + c_n)}) = \sum_{k=0}^{n} a_k \underbrace{(b_{n-k} + c_{n-k})}_{= a_k b_{n-k} + a_k c_{n-k}} =$

$= \left(\sum_{k=0}^{n} a_k b_{n-k}\right) + \left(\sum_{k=0}^{n} a_k c_{n-k}\right) = (a_n)(b_n) + (a_n)(c_n)$

R hat Einselement 1: $(1, 0, 0, 0, \ldots)$, weil

$\underbrace{(1, 0, 0, \ldots)}_{b_n} \cdot (a_n) = \left(\sum_{k=0}^{n} b_k \cdot a_{n-k}\right) = (a_n)$

Assoziativgesetz der Multiplikation: $(a_n), (b_n), (c_n)$

$\underbrace{(a_n)}_{a} \cdot \left(\underbrace{(b_n)}_{b} \cdot \underbrace{(c_n)}_{c}\right) = \left(\sum_{k=0}^{n} a_k \underbrace{(b \cdot c)_{n-k}}_{\sum_{j=0}^{n-k} b_j \cdot c_{n-k-j} = \sum_{j=k}^{n} b_{j-k}\, c_{n-j}}\right) =$

$= \left(\sum_{k=0}^{n} \sum_{j=k}^{n} a_k\, b_{j-k}\, c_{n-j}\right) = \left(\sum_{j=0}^{n} \sum_{k=0}^{j} a_k\, b_{j-k} \underbrace{c_{n-j}}_{\text{herausheben}}\right) =$

j \ k	0	1	2	. . .	n
0	*				
1	*	*			
2	*	*	*		
⋮	⋮	⋮	⋮		
n	*	*	*		*

$$= \sum_{j=0}^{n} \underbrace{\left(\sum_{k=0}^{j} a_k b_{j-k} \right)}_{(ab)_j} c_{n-j} = \left(\sum_{j=0}^{n} (ab)_j \cdot c_{n-j} \right) = \left((a_n) \cdot (b_n) \right) \cdot (c_n) \quad \checkmark$$

□

$x := (0, 1, 0, 0, \ldots)$

$x^2 = (0, \underbrace{0}_{0\cdot 1 + 1 \cdot 0}, 1, 0, 0, \ldots)$

$x^3 = (0, 0, 0, 1, 0, 0, \ldots)$

$x^n = (0, 0, \ldots, \underbrace{0}_{n\text{-te Stelle}}, 1, 0, \ldots)$ formal: Beweis mit Induktion

$(a_n) = a_0 + a_1 x + a_2 x^2 + \ldots = \sum_{n=0}^{\infty} a_n x^n$

Def: Sei $(R, +, \cdot)$ ein kommutativer Ring. Dann heißt eine formale Potenzreihe $\triangleq$ Polynom über R (in einer Variable), falls es ein $N \in \mathbb{N}_0$ sodass $\forall n \geq N : a_n = 0$ $(a_n)_{n \in \mathbb{N}_0}$ alle bis auf endlich viele sind null

es kann $p = 0$ $(= (0, 0, 0, \ldots))$ sein, oder $p \neq 0$. Für $p \neq 0$ heißt $\max \{ n \in \mathbb{N}_0 : a_n \neq 0 \}$ größter Koeffizient $\neq 0$ der Grad von p (grad p, deg p)

Bemerkungen:

* $p = \sum_{k=0}^{n} a_k x^k$ Bitte Polynom und Polynomfunktion unterscheiden!
* $p = 0$ Nullpolynom hat keinen Grad (manchmal grad $0 := -\infty$) NICHT grad 0!

  $p \neq 0 \Rightarrow$ grad $p \geq 0$

  grad $p = 0 \Leftrightarrow p \in R \setminus \{0\}$ eine Konstante $\neq 0$
* R Körper: grad $p = 0 \Leftrightarrow p \in R^*$ Einheiten

Def: Die Menge aller Polynome über R bezeichnen wir mit $R[x]$

$(R[x], +, \cdot)$

Proposition

Sei $(R, +, \cdot)$ kommutativer Ring! (NICHT Körper), $p, q \in R[x]$, $p \neq 0$, $q \neq 0$

1) es ist $p + q = 0$ oder grad $(p+q) \leq \max \{$grad p, grad $q\}$
2) es ist $p \cdot q = 0$ oder grad $(p \cdot q) \leq$ grad p + grad q

Beweis $p = \sum_{k=0}^{n_1} a_k x^k = (a_0, a_1, \ldots, \underbrace{a_{n_1}}_{\neq 0}, 0, 0, \ldots)$

$q = \sum_{k=0}^{n_2} b_k x^k = (b_0, b_1, \ldots, \underbrace{b_{n_2}}_{\neq 0}, 0, 0, \ldots)$

(1) $p+q = (a_0+b_0, a_1+b_1, \ldots, \underbrace{a_n + b_n}_{n := \max\{n_1, n_2\}}, 0, 0 \ldots)$

$\Rightarrow \operatorname{grad}(p+q) \leq n$

(2) $n > n_1 + n_2 \qquad p \cdot q = (c_n)$

$c_n = \sum_{k=0}^{n} a_k b_{n-k} = \sum_{k=0}^{n_1} a_k \underbrace{b_{n-k}}_{\substack{n-k \geq n-n_1 > n_2 \\ = 0}} = 0$

$\Rightarrow \operatorname{grad}(p \cdot q) \leq n_1 + n_2$ □

Proposition

$(R, +, \cdot)$ kommutativer Ring (+Einselement) $\Rightarrow (R[x], +, \cdot)$ sind kommutativer Ring (mit Einselement)

Beweis: Gradformel

Skizze: nur noch zeigen $\forall$ p und q auch Polynom

$p = 0 \Rightarrow p+q = q$ Polynom

$p \neq 0 \quad q \neq 0 \Rightarrow \operatorname{grad}(p+q)$ höchstens … $\Rightarrow$ Polynom

$p = 0 \qquad p \cdot q = 0 \cdot q = 0$ → Polynom

$p \neq 0 \quad q \neq 0 \qquad p \cdot q = \operatorname{grad} \leq n_1 + n_2$ → Polynom

formale PR sind kRing → Polynome sind k. Ring □

Bsp $\mathbb{Z}_5$ Restklassen mod 5 Körper (da 5 Primzahl)

$p := x^5, \quad q := \underbrace{x}_{52 \bmod 5} \qquad p \neq q \qquad (\operatorname{grad} p = 5, \operatorname{grad} q = 1)$

x	0	1	2	3	4
p(x)	0	1	2	3	4
q(x)	0	1	2	3	4

$3^5 = \underbrace{9}_{\equiv 4} \cdot 3^3 = \underbrace{4 \cdot 3}_{\equiv 2} \cdot 3^2 \equiv \underbrace{2 \cdot 3}_{\equiv 1} \cdot 3 \equiv 3$

es gilt also $p(x) = q(x) \; \forall x \in \mathbb{Z}_5$

→ unterscheide genau zw. Polynom und Polynomfunktion

Bsp $\mathbb{Z}_{10}$

$p = 6x^4 + 2x^3 + 8x + 7$

$q = 5x^3 + 5$

grad $p = 4$, grad $q = 3$

$p \cdot q = 30x^7 + 10x^6 + 0x^4 + 45x^3 + 40x + 35 \quad \text{mod } 10$

$= 5x^3 + 5 = q$

grad $p \cdot q = 3 < 7 = \text{grad } p + \text{grad } q$

$p \cdot q = 1 \cdot q$ aber $p \neq 1$ (Kürzungsregel gilt i. A. nicht)

Bsp $\mathbb{Z}_6$

$p = 3x^2$ grad $p = 2$, grad $q = 1$

$q = 2x$

$p \cdot q = 6x^3 \overset{\text{mod } 6}{=} 0$ (2 Polynome die $\neq 0$ können Nullpolynom ergeben)

Grund: nicht nullteilerfrei

Proposition

$(R, +, \cdot)$ nullteilerfrei $\Rightarrow (R[x], +, \cdot)$ ist Nullteilerfrei. Weiters gilt für $p, q \in R[x]$, $p \neq 0$, $q \neq 0$, dann grad $(p \cdot q) = \text{grad } p + \text{grad } q$

Beweis

$p = \sum_{k=0}^{n_1} a_k x^k \quad (a_{n_1} \neq 0) \qquad q = \sum_{k=0}^{n_2} b_k x^k \quad (b_{n_2} \neq 0)$

Koeffizient von $x^{n_1+n_2}$ bei $p \cdot q$: $\underbrace{a_{n_1}}_{\neq 0} \cdot \underbrace{b_{n_2}}_{\neq 0} \neq 0$ da nullteilerfrei

$\Rightarrow p \cdot q \neq 0$ und grad $(p \cdot q) = n_1 + n_2$ □

Korollar (Kürzungsregel)

$(R, +, \cdot)$ nullteilerfrei, p_1, p_2, q Polynome $\in R[x]$, $q \neq 0$

$p_1 \cdot q = p_2 \cdot q \Rightarrow p_1 = p_2$

Beweis

nicht notwendig da KR für nullteilerfreie Ringe bereits bewiesen

Def: Sei $(R, +, \cdot)$ kommutativer Ring, $p = \sum_{k=0}^{n} a_k x^k$ ein Polynom. Setze

$p' = \sum_{k=1}^{n} k \cdot a_k \cdot x^{k-1} = \sum_{k=0}^{n-1} (k+1) \cdot a_{k+1} \cdot x^k$

Proposition

$(r_1 \cdot p + r_2 \cdot q)' = r_1 \cdot p' + r_2 \cdot q'$ Linearität

$(p \cdot q)' = p' \cdot q + p \cdot q'$ Produktregel

Beweis

1. Formel: nachrechnen

$(x^n \cdot x^k)' = (x^{n+k})' = (n+k) \cdot x^{n+k-1}$

$(x^n)' \cdot x^k + x^n \cdot (x^k)' = n \cdot x^{n-1} \cdot x^k + x^n \cdot k \cdot x^{k-1} = (n+k) \cdot x^{n+k-1} = (x^n \cdot x^k)'$

$(x^n \cdot \underbrace{q}_{=\sum_{k=0}^{n_1} b_k x^k})' = \sum_{k=0}^{n_1} b_k \cdot \underbrace{(x^n \cdot x^k)'}_{=(x^n)' \cdot x^k + x^n (x^k)'} = (x^n)' \underbrace{\sum_{k=0}^{n_1} b_k x^k}_{q} + x^n \underbrace{\left(\sum_{k=0}^{n_1} b_k x^k\right)'}_{=q'} =$

$= (x^n)' \cdot q + x^n \cdot q'$

$(\underbrace{p}_{=\sum_{k=0}^{n_2} a_k x^k} \cdot q)' = \sum_{k=0}^{n_2} a_k \underbrace{(x^k q)'}_{=(x^k)' q + x^k q'} = \underbrace{\left(\sum_{k=0}^{n_2} a_k x^k\right)'}_{=p'} \cdot q + \underbrace{\left(\sum_{k=0}^{n_2} a_k x^k\right)}_{=p} \cdot q' = p' \cdot q + p \cdot q'$ □

Proposition

Sei $(R, +, \cdot)$ kommutativer Ring mit Eins, $p \in R[x]$. Falls $p = 0$ oder $\operatorname{grad} p = 0$ dann ist $p' = 0$. Falls $\operatorname{grad} p > 0$, dann ist $p' = 0$ oder $\operatorname{grad} p' \leq \operatorname{grad} p - 1$

Beweis

$p = 0$ oder $\operatorname{grad} p = 0 \Rightarrow p = c$ für ein $c \in R \Rightarrow p' = 0$

$n = \operatorname{grad} p > 0 \Rightarrow p = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$

$\Rightarrow p' = n \cdot a_n x^{n-1} + (n-1) a_{n-1} x^{n-2} + \ldots + a_1$

$\Rightarrow p' = 0$ oder $\operatorname{grad} p' \leq n-1 = \operatorname{grad} p - 1$ □

Def: Sei $(K, +, \cdot)$ ein Körper. Falls $n \cdot 1 \neq 0 \; \forall n \in \mathbb{N}$, dann $\operatorname{char} K := 0$ (Charakteristik von K)

Andernfalls ist $\operatorname{char} K := \min \{n \in \mathbb{N} : n \cdot 1 = 0\}$

Proposition

Sei $(K,+,\cdot)$ Körper mit $\operatorname{char} K = 0$. Falls $x \neq 0$ dann ist $n \cdot x \neq 0 \ \forall n \in \mathbb{Z} \setminus \{$

Beweis

$$n \cdot x = \underbrace{n \cdot 1}_{\neq 0} \cdot \underbrace{x}_{\neq 0} \neq 0 \quad \text{für } n \in \mathbb{N}$$

für $n < 0$ $\quad n \cdot x = \underbrace{(-n)}_{\in \mathbb{N}} \cdot \underbrace{(-x)}_{\neq 0} \neq 0$ □

Proposition

$(K,+,\cdot)$ Körper mit $\operatorname{char} K = 0$, $p \in K[x]$ mit $\operatorname{grad} p > 0$. Dann ist

$\operatorname{grad} p' = \operatorname{grad} p - 1$

Beweis

$$n := \operatorname{grad} p \Rightarrow p = \underbrace{a_n}_{\neq 0} x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$$

$$\Rightarrow p' = \underbrace{n \cdot a_n}_{\neq 0} x^{n-1} + (n-1) \cdot a_{n-1} \cdot x^{n-2} + \ldots + a_1$$

$$\Rightarrow \operatorname{grad} p' = n - 1 = \operatorname{grad} p - 1$$ □

3) Teilbarkeit in Integritätsbereichen

ab jetzt immer $(R,+,\cdot)$ ... Integritätsbereich

↳ nullteilerfreier, kommutativer Ring mit Eins

$(K,+,\cdot)$ Körper

$(K[x],+,\cdot)$ ist ein Integritätsbereich (Polynomring über Körper)

Def: $(R,+,\cdot)$ $a,b \in R$ Dann sagt man a teilt b $(a|b)$ falls

$\exists x \in R$ mit $b = a \cdot x$

Proposition

$(R,+,\cdot)$ $a,b,c \in R$

(1) $a|b$ und $a|c \Rightarrow a|x \cdot b + y \cdot c \quad \forall x,y \in R$ (jede Linearkomb.)

(2) $a|b \Rightarrow a \cdot c | b \cdot c$ Teilbarkeit bleibt erhalten

(3) $a|a$

(4) $a|b$ und $b|c \Rightarrow a|c$ transitiv

(5) $a|b$ und $b|a \Rightarrow \exists x \in R^*$ (Einheit) mit $a = b \cdot x$

(3), (4), (5) im Wesentlichen Ordnungsrelation

(6) $a|0 \quad \forall a \in R$ heißt nicht dass a Nullteiler!

(7) $1|a \quad \forall a \in R$

Beweis

(1) $\exists u, v \in R$ mit $b = a \cdot u$ und $c = a \cdot v$

$\Rightarrow x \cdot \underbrace{b}_{a \cdot u} + y \cdot \underbrace{c}_{a \cdot v} = a \cdot (xu + yv) \Rightarrow a | x \cdot b + y \cdot c$

(2) $\exists u \in R$ mit $b = a \cdot u \Rightarrow b \cdot c = a \cdot u \cdot c = (a \cdot c) \cdot u$

$\Rightarrow a \cdot c \mid b \cdot c$

(3) $a = 1 \cdot a \Rightarrow a|a$

(4) $\exists x, y \in R$ mit $b = a \cdot x$ und $c = b \cdot y \Rightarrow c = \underbrace{b}_{a \cdot x} \cdot y = a(x \cdot y) \Rightarrow a | c$

(5) $\exists x, y \in R$ mit $b = a \cdot x$ und $a = b \cdot y$

1. Fall: $a = 0 \Rightarrow b = 0 \Rightarrow b = a = a \cdot \underbrace{1}_{\in R^*}$

2. Fall: $a \neq 0 \Rightarrow a \cdot 1 = a = \underbrace{b}_{= a \cdot x} \cdot y = a(x \cdot y) \Rightarrow x \cdot y = 1$ (Kürzungsregel)

$\Rightarrow y \in R^*$

(6) $0 = a \cdot 0 \Rightarrow a|0$

(7) $a = 1 \cdot a \Rightarrow 1|a$ □

Def: $(R, +, \cdot)$, $p \in R \setminus (R^* \cup \{0\})$

(1) p heißt <u>prim</u>, falls $p | a \cdot b \Rightarrow p|a$ oder $p|b$

(2) p heißt <u>irreduzibel</u>, falls $p = a \cdot b \Rightarrow a \in R^*$ oder $b \in R^*$

Bemerkung

$(K, +, \cdot)$ Körper $\Rightarrow \nexists$ prime oder irreduzible Elemente $(K = K^* \cup \{0\})$

Proposition

$(R, +, \cdot)$ $p \in R$ prim $\Rightarrow$ p ist irreduzibel

Umkehrung gilt im Allgemeinen nicht

Beweis

Seien $a,b \in R$ so, dass $p = a \cdot b \Rightarrow p \mid a \cdot b \overset{p \text{ prim}}{\Rightarrow} p \mid a$ oder $p \mid b$

o.B.d.A $p \mid a \Rightarrow \exists x$ mit $a = p \cdot x$

$\Rightarrow \underbrace{a}_{\neq 0} \cdot 1 = a = \underbrace{p}_{= a \cdot b} \cdot x = a \cdot (b \cdot x) \overset{KR \text{ Kürzungsregel}}{\Rightarrow} bx = 1 \Rightarrow b \in R^*$

also p ist irreduzibel $\square$

Sei $d \in \mathbb{Z}$ eine quadratfreie Zahl (d.h. $\forall p \in P,\ p^2 \nmid d$)

$d \not\equiv 1 \pmod 4$:

$\mathbb{Z}[\sqrt{d}] := \{a + b\sqrt{d} : a,b \in \mathbb{Z}\}$ Integritätsbereich

Def: Sei $x \in \mathbb{Z}[\sqrt{d}]$. Dann $x = a + b\sqrt{d}$ für passende $a,b \in \mathbb{Z}$

Setze $N(x) := a^2 - db^2 = (a + b\sqrt{d}) \cdot (a - b\sqrt{d})$ (Norm von x) $N(x) \in \mathbb{Z}$

Proposition

Seien $x,y \in \mathbb{Z}[\sqrt{d}]$. Dann gilt $N(xy) = N(x) \cdot N(y)$

Beweis

$x = a_1 + b_1\sqrt{d}$, $y = a_2 + b_2\sqrt{d}$

$N(x) \cdot N(y) = (a_1 + b_1\sqrt{d}) \cdot (a_1 - b_1\sqrt{d}) \cdot (a_2 + b_2\sqrt{d}) \cdot (a_2 - b_2\sqrt{d}) =$

$= \underbrace{(a_1 + b_1\sqrt{d}) \cdot (a_2 + b_2\sqrt{d})}_{= x \cdot y} \cdot (a_1 - b_1\sqrt{d}) \cdot (a_2 - b_2\sqrt{d}) = N(xy)$ $\square$

Proposition

$\mathbb{Z}[\sqrt{d}]$, $x,y \in \mathbb{Z}[\sqrt{d}]$

(1) $x \mid y \Rightarrow N(x) \mid N(y)$ (und $|N(x)| \mid |N(y)|$)

(2) x ist Einheit in $\mathbb{Z}[\sqrt{d}] \Leftrightarrow |N(x)| = 1$

(für $d < 0$: $N(x) = 1$)

Beweis

(1) $x \mid y \Rightarrow \exists u$ mit $y = x \cdot u$

$\Rightarrow N(y) = N(x \cdot u) = N(x) \cdot N(u) \Rightarrow N(x) \mid N(y)$

(2) ($\Rightarrow$) x Einheit $\Rightarrow x \mid 1 \Rightarrow N(x) \mid N(1) = 1$

$\Rightarrow N(x) \in \{1, -1\} \Rightarrow |N(x)| = 1$

($\Leftarrow$) $x = a + b\sqrt{d}$, $|N(x)| = 1$

1. Fall $N(x) = 1$ $\Rightarrow$ $1 = N(x) = \underbrace{(a+b\sqrt{d})}_{x} \cdot \underbrace{(a-b\sqrt{d})}_{\in \mathbb{Z}[\sqrt{d}]}$ $\Rightarrow x$ Einheit

2. Fall $N(x) = -1$ $\Rightarrow$ $-1 = N(x) = \underbrace{(a+b\sqrt{d})}_{x} \cdot (a + b\sqrt{d})$ $\Rightarrow$

$\Rightarrow$ $1 = x \cdot \underbrace{(-a + b\sqrt{d})}_{\in \mathbb{Z}[\sqrt{d}]}$ $\Rightarrow$ x Einheit $\square$

Korollar

$x \in \mathbb{Z}[\sqrt{d}]$ und $|N(x)| \in \mathbb{P}$ $\Rightarrow$ x irreduzibel

Beweis

$x = u \cdot v$ $\Rightarrow$ $\underbrace{|N(x)|}_{\in \mathbb{P}} = \underbrace{|N(uv)|}_{= N(u) \cdot N(v)} = |N(u)| \cdot |N(v)|$ $\Rightarrow$

$\Rightarrow \underbrace{|N(u)| = 1}_{\Rightarrow u \text{ Einheit}}$ oder $\underbrace{|N(v)| = 1}_{\Rightarrow v \text{ Einheit}}$ Somit ist x irreduzibel $\square$

Beispiel Umkehrung gilt nicht

z.B $\mathbb{Z}[\sqrt{-1}]$

NICHT: $N(2) = 4 \notin \mathbb{P}$ 2 nicht irreduzibel in $\mathbb{Z}[\sqrt{-1}]$ weil $2 = (1+\sqrt{-1}) \cdot (1 - \sqrt{-1})$

SCHON: $N(3) = 9 \notin \mathbb{P}$ z.z. 3 ist irreduzibel

$3 = u \cdot v$ $\Rightarrow$ $9 = N(3) = N(uv) = N(u) \cdot N(v)$

falls $N(u) = 1$ $\Rightarrow$ u Einheit

falls $N(u) = 9$ $\Rightarrow N(v) = 1$ $\Rightarrow$ v Einheit

angen. $N(u) = 3$ $u = a + b\sqrt{-1}$

$3 = N(u) = a^2 + b^2$ $\Rightarrow$ $a \in \{-1, 0, 1\}$, $b \in \{-1, 0, 1\}$

$\Rightarrow$ nicht erfüllbar Daher ist 3 irreduzibel

Beispiel $\mathbb{Z}[\sqrt{-5}]$

$2 \times 3 = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5})$

2 ist irreduzibel weil: $2 = u \cdot v$ $\Rightarrow$ $4 = N(2) = N(u) \cdot N(v)$

für $N(u) = 1$ ist u Einheit. für $N(u) = 4$ ist v Einheit

Falls $\underbrace{N(u)}_{= a + b\sqrt{-5}} = 2$ $2 = a^2 + 5b^2$ $\Rightarrow$ $b = 0$ $\Rightarrow$ nicht erfüllbar

3 ist irreduzibel, weil: $3 = u \cdot v \Rightarrow 9 = N(3) = N(u) \cdot N(v)$

für $N(u) = 1$ ist u Einheit, für $N(u) = 9$ ist v Einheit

falls $N(u) = 3$ $\quad 3 = a^2 + 5b^2 \mod 5$:

$\underbrace{N(u)}_{= a + b\sqrt{-5}}$

$3 \equiv a^2 \pmod 5$

a	0	1	2	3	4
a^2	0	1	4	4	1

$\Rightarrow$ nicht erfüllbar

$1 + \sqrt{-5}$ ist irreduzibel, weil $\quad 1 + \sqrt{-5} = u \cdot v \Rightarrow$

$\Rightarrow \quad 6 = N(1 + \sqrt{-5}) = N(u) \cdot N(v)$

für $N(u) = 1$ ist u Einheit $\quad$ für $N(u) = 6$ ist v Einheit

$N(u) = 2$ nicht möglich

$N(u) = 3$ nicht möglich

Genauso $1 - \sqrt{-5}$ ist irreduzibel

$2 \mid (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5})$ aber $\quad 2 \nmid 1 + \sqrt{-5}$, $\quad 2 \nmid 1 - \sqrt{-5}$

also 2 ist irreduzibel, aber nicht prim (Genauso $3, 1+\sqrt{-5}, 1-\sqrt{-5}$)

in $\mathbb{Z}[\sqrt{-5}]$ gibt es keine Eindeutige Zerlegung in Irreduzible (Primfaktorzerlegung) und Irreduzible müssen nicht prim sein:

$6 = 2 \cdot 3 = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5})$,

$2 \mid (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5})$ aber $\quad 2 \nmid (1 + \sqrt{-5})$ und $2 \nmid (1 - \sqrt{-5})$

Def: Seien $a, b \in R$. Dann heißt $d \in R$ der <u>größte gemeinsame Teiler</u> von a und b $(d = ggT(a,b))$, falls $d \mid a$ und $d \mid b$ und falls $s \in R$, $s \mid a$ und $s \mid b \Rightarrow s \mid d$

<u>Bemerkungen</u>

* $gcd(a,b)$ ist nicht eindeutig, aber $d, \tilde{d}$ der $gcd(a,b)$ sind, da $\exists\, c \in R^*$ mit $\tilde{d} = c \cdot d$

<u>Beweis</u>

$\tilde{d} \mid d$ und $d \mid \tilde{d} \Rightarrow \exists\, c \in R^*$ mit $\tilde{d} = c \cdot d$ $\square$

* es muss ggT(a,b) nicht existieren

z.B. in $\mathbb{Z}[\sqrt{-5}]$: $a = 6$, $b = 2+2\cdot\sqrt{-5}$

gemeinsame Teiler: $1, 2, 1+\sqrt{-5}$, also $\nexists$ ggT(a,b)

Def: Sei $p \in K[x]$

(1) p heißt <u>konstant</u>, wenn $\exists\, a \in K$ mit $p = a$

(2) p heißt <u>nichtkonstant</u>, wenn p nicht konstant ist

Bemerkungen

* p konstant $\Leftrightarrow$ $p = 0$ oder grad $p = 0$
* p nichtkonstant $\Leftrightarrow$ grad $p \geq 1$

Proposition

$p \in K[x]$ (1) p ist Einheit $\Leftrightarrow$ grad $p = 0$

(2) grad $p = 1$ $\Rightarrow$ p irreduzibel

<u>Beweis</u>

(1) ($\Rightarrow$) $\exists\, q$ mit $p \cdot q = 1$ $\Rightarrow$ grad p + grad q = grad $1 = 0$

$\Rightarrow$ grad $p = 0$

($\Leftarrow$) $\exists\, a \in K \setminus \{0\}$ mit $p = a$ $\Rightarrow$ $a^{-1} \cdot p = 1$

2) Seien $q_1, q_2 \in K[x]$ mit $p = q_1 \cdot q_2$ $\Rightarrow$

$1 = \text{grad } p = \text{grad } q_1 + \text{grad } q_2$ $\Rightarrow$ $\underbrace{\text{grad } q_1 = 0}_{\Rightarrow q_1 \text{ Einheit}}$ oder $\underbrace{\text{grad } q_2 = 0}_{\Rightarrow q_2 \text{ Einheit}}$

somit ist p irreduzibel $\square$

$a, b \neq 0 \in \mathbb{Z}$, $\exists q \in \mathbb{Z}$, $\underbrace{r \in \{0, 1, \ldots, b-1\}}_{|r| < |b|}$ mit $a = q \cdot b + r$

<u>Division mit Rest für Polynome:</u>

Proposition

Seien $p_1, p_2 \in K[x]$, $p_2 \neq 0$. Dann $\exists\, q, r \in K[x]$ mit $r = 0$ oder grad $r <$ grad p_2 mit $p_1 = q \cdot p_2 + r$

Beweis

falls $p_1 \neq 0$ sei $n := \operatorname{grad} p_1$, $k := \operatorname{grad} p_2$

$$p_1 = \sum_{j=0}^{n} a_j x^j, \quad p_2 = \sum_{j=0}^{k} b_j x^j$$

Induktion nach n: $p_1 = 0$ Setze $q := r := 0$

Dann gilt $p_1 = q \cdot p_2 + r$

$n = 0$: $p_1 = a_0$: 1. Fall $k = 0 \Rightarrow p_2 = b_0 \neq 0$

setze $q := \frac{a_0}{b_0}$ und $r = 0$. Dann $q \cdot p_2 + r = \frac{a_0}{b_0} \cdot b_0 + 0 = a_0 = p_1$

2. Fall: $k > 0$ Setze $q := 0$ und $r := a_0$

Dann $\operatorname{grad} r = 0 < k = \operatorname{grad} p_2$ und $p_1 = q \cdot p_2 + r$

Sei $n > 0$: 1. Fall: $k > n$ Setze $q := 0$ und $r := p_1$. Dann ist

$\operatorname{grad} r = n < k = \operatorname{grad} p_2$ und $p_1 = q \cdot p_2 + r$

2. Fall: $k \leq n$ Setze $\tilde{p} = p_1 - \frac{a_n}{b_k} x^{n-k} p_2 =$

$$= a_n x^n + \sum_{j=0}^{n-1} a_j x^j - \frac{a_n}{b_k} \underbrace{x^{n-k} \sum_{j=0}^{k} b_j x^j}_{= \sum_{j=n-k}^{n} b_{j-n+k} x^j} =$$

$$= \cancel{a_n x^n} + \sum_{j=0}^{n-1} a_j x^j - \underbrace{\frac{a_n}{b_k} \cancel{b_k}}_{a_n} x^n - \sum_{j=n-k}^{n-1} b_{j-n+k} x^j$$

$\Rightarrow \tilde{p} = 0$ oder $\operatorname{grad} \tilde{p} \leq n-1$

$\Rightarrow \exists\, \tilde{q}, r$ mit $r = 0$ oder $\operatorname{grad} r < \operatorname{grad} p_2$ mit $\tilde{p} = \tilde{q} \cdot p_2 + r$

$\Rightarrow p_1 = \underbrace{\tilde{p}}_{= \tilde{q} \cdot p_2 + r} + \frac{a_n}{b_k} x^{n-k} p_2 = (\underbrace{\tilde{q} + \frac{a_n}{b_k} x^{n-k}}_{=: q}) \cdot p_2 + r$ □

So etwas (man hat Division mit Rest) nennt man <u>Euklidischer Ring</u>

Euklidischer Algorithmus

Proposition

Seien $p_1, p_2 \in K[x]$, $p_2 \neq 0$. Dann $\exists n \in \mathbb{N}$, $n \geq 2$, $\exists p_3, p_4, \dots, p_n \in K[x]$
$\exists q_2, q_3, \dots, q_n \in K[x]$ mit $\operatorname{grad} p_2 > \operatorname{grad} p_3 > \dots > \operatorname{grad} p_n$
$p_{n+1} := 0$, sodass für $j \in \{2, 3, \dots, n\}$ gilt: $p_{j-1} = q_j p_j + p_{j+1}$
Setze $q := p_n$. Dann ist $q = ggT(p_1, p_2)$ und $\exists s_1, s_2 \in K[x]$
mit $q = s_1 \cdot p_1 + s_2 \cdot p_2$

Beweis

Behauptung: für $u \in \{2, 3, \dots, n\}$ $\exists p_3, \dots, p_u, p_{u+1}, q_2, \dots, q_u$ wie oben
und $\exists s_1^{(u)}, s_2^{(u)} \in K[x]$ mit $p_{u+1} = s_1^{(u)} p_1 + s_2^{(u)} p_2$

Beweis der Behauptung $u = 2$ nach der Division mit Rest
$\exists q_2, p_3$ mit $p_3 = 0$ ($\Rightarrow n = 2$) oder $\operatorname{grad} p_3 < \operatorname{grad} p_2$ mit:

$p_1 = q_2 \cdot p_2 + p_3$ $\qquad p_3 = \underbrace{1}_{= s_1^{(u)}} \cdot p_1 + \underbrace{(-q_2)}_{s_2^{(u)}} \cdot p_2$

Sei $u > 2$: $p_{u-2} = q_{u-1} p_{u-1} + p_u$, $p_u \neq 0$
$p_u = s_1^{(u-1)} p_1 + s_2^{(u-1)} p_2$

Nach der Division mit Rest $\exists q_u, p_{u+1} \in K[x]$ mit
$p_{u+1} = 0$ ($\Rightarrow n = u$) oder $\operatorname{grad} p_{u+1} < \operatorname{grad} p_u$ mit $p_{u-1} = q_u p_u + p_{u+1}$

$p_{u-1} = q_u p_u + p_{u+1}$ Dann $p_{u+1} = \underbrace{p_{u-1}}_{= (s_1^{(u-2)} p_1 + s_2^{(u-2)} p_2)} + (-q_u) \underbrace{p_u}_{= (s_1^{(u-1)} p_1 + s_2^{(u-1)} p_2)}$

$= (\underbrace{s_1^{(u-2)} - q_u s_1^{(u-1)}}_{=: s_1^{(u)}}) \cdot p_1 + (\underbrace{s_2^{(u-2)} - q_u s_2^{(u-1)}}_{=: s_1^{(u)}}) p_3$

◇

Dieses Verfahren muss wegen $\operatorname{grad} p_2 > \operatorname{grad} p_3 > \dots$ abbrechen
Setze $q := p_n$ $\qquad q = p_n = \underbrace{s_1^{(n-1)}}_{=: s_1} p_1 + \underbrace{s_2^{(n-1)}}_{=: s_2} p_2$

Behauptung: für $u \in \{1,2,\dots,n-1\}$ gilt $q \mid p_u$, $q \mid p_{u+1}, \dots, q \mid p_{n-1}$

Beweis der Behauptung („umgekehrte Induktion")

$u = n-1$ $\quad p_{n-1} = q_n \underbrace{p_n}_{q} + \underbrace{p_{n+1}}_{=0} = q_n \cdot q \Rightarrow q \mid p_{n-1}$

sei $u \in \{1,2,\dots,n-2\}$ $\quad q \mid p_{u+1}, q \mid p_{u+2}, \dots q \mid p_{n-1}$

$p_u = q_{u+1} \underbrace{p_{u+1}}_{q \mid p_{u+1}} + \underbrace{p_{u+2}}_{q \mid p_{u+2}} \Rightarrow q \mid p_u$ ◇

daher $q \mid p_1$ und $q \mid p_2$

Sei $s \in K[x]$, $s \mid p_1$ und $s \mid p_2$ $\Rightarrow$

$\Rightarrow s \mid s_1 p_1 + s_2 p_2 = q$ Somit ist $q = ggT(p_1, p_2)$ □

Ergänzung zu den Bemerkungen zum ggT

* $d = ggT(a,b)$ ist Einheit $\Rightarrow 1 = d^{-1} \cdot d = ggT(a,b)$
  (in diesem Fall schreiben wir stets $ggT(a,b) = 1$)

Proposition

$p \in K[x]$ Dann ist p genau dann irreduzibel, wenn p prim ist

Beweis

prim $\Rightarrow$ irreduzibel ✓ (gilt Allgemein)

Sei p irreduzibel, Seien $q_1, q_2 \in K[x]$ so, dass $p \mid q_1 \cdot q_2$

Falls $p \mid q_1$ ✓

es gelte $p \nmid q_1$ $\quad q := ggT(p, q_1)$

Angenommen q ist keine Einheit $\Rightarrow q \mid p \Rightarrow \exists\, u \in K[x]$ mit $p = q \cdot u$

$\Rightarrow u$ Einheit. $\exists\, s \in K[x]$ mit $q_1 = s \cdot q$

$\Rightarrow q_1 = s \cdot \underbrace{q}_{= u^{-1} p} = u^{-1} \cdot s \cdot p \Rightarrow p \mid q_1$ ↯ WID

Somit $ggT(p, q_1) = 1$

eukl. Algorithmus $\Rightarrow \exists\, s_1, s_2 \in K[x]$ mit $1 = s_1 p + s_2 \cdot q_1$

$\exists\, v \in K[x]$ mit $q_1 \cdot q_2 = v \cdot p$

$\Rightarrow q_2 = s_1 q_2 p + s_2 \underbrace{q_1 q_2}_{=v \cdot p} = (s_1 q_2 + s_2 v) \cdot p \Rightarrow p \mid q_2$ □

Eindeutige Primfaktorzerlegung

Proposition

Sei $p \neq 0 \in K[x]$ Dann $\exists\, n \in \mathbb{N}_0$, $c \in K \setminus \{0\}$, $p_1, p_2 \dots, p_n$ irreduzibel mit $p = c \cdot p_1 p_i \cdot \dots \cdot p_n$. Falls für $\tilde{n} \in \mathbb{N}_0$, $d \in K \setminus \{0\}$ $q_1, \dots, q_{\tilde{n}}$ irreduzibel gilt $p = d \cdot q_1 \cdot q_2 \cdot \dots \cdot q_{\tilde{n}}$, dann ist $\tilde{n} = n$ und $\exists\, \sigma : \{1, 2, \dots, n\} \supseteq$ bijektiv, $c_1, \dots, c_n \in K \setminus \{0\}$ mit $q_j = c_j p_{\sigma(j)}$

Beweis

Existenz: Induktion nach $n = \operatorname{grad} p$

$n = 0$ ✓ (da p Einheit)

Sei $n > 0$: falls p irreduzibel ✓

somit ist p nicht irreduzibel $\Rightarrow p = q_1 \cdot q_2$, q_1, q_2 keine Einheiten

$\Rightarrow \operatorname{grad} q_1 \geq 1$ und $\operatorname{grad} q_2 \geq 1$ $(n = \operatorname{grad} q_1 + \operatorname{grad} q_2)$

$\Rightarrow \operatorname{grad} q_1 \leq n$ und $\operatorname{grad} q_2 < n \Rightarrow \exists\, c_1, c_2, n_1, n_2, p_1 \dots p_{n_1}, \tilde{p}_1, \dots, \tilde{p}_{n_2}$ irreduzibel, sodass $q_1 = c_1 \cdot p_1 \cdot \dots \cdot p_{n_1}$, $q_2 = c_2 \tilde{p}_1 \cdot \dots \cdot \tilde{p}_{n_2}$

$\Rightarrow p = \underbrace{(c_1 \cdot c_2)}_{\text{Einheit}} p_1 \cdot \dots \cdot p_{n_1} \cdot \tilde{p}_1 \cdot \dots \cdot \tilde{p}_{n_2}$

Eindeutigkeit $p = \overbrace{c}^{\text{Einheiten}} \underbrace{p_1 \cdot \dots \cdot p_n}_{\text{irreduzibel}} = d \cdot q_1 \cdot \dots \cdot q_{\tilde{n}}$

$\Rightarrow p_1 \mid q_1 \dots q_{\tilde{n}} \Rightarrow \exists\, \sigma(1) \in \{1, 2, \dots, \tilde{n}\}$ mit $p_1 \mid q_{\sigma(1)}$

$\Rightarrow \exists$ Einheit c_1 mit $q_{\sigma(1)} = c_1 \cdot p_1$

$c \cdot p_2 \dots p_n = \frac{d}{c_1} q_1 \dots q_{\sigma(1)-1} q_{\sigma(1)+1} \dots q_{\tilde{n}} \dots$ (formal Induktion)

$\Rightarrow \tilde{n} = n$ und $\exists\, \sigma : \{1, 2, \dots, n\} \supseteq$ bijektiv

$\exists\, c_1, \dots, c_n$ Einheiten mit $q_{\sigma(j)} = c_j p_j$ □

$p = (x-1) \underbrace{(2x-2)}_{2(x-1)} = 2 \cdot (x-1)^2$

Standarddarstellung

$p = c \cdot p_1^{k_1} \cdot \ldots \cdot p_n^{k_n}$ $\quad p_1 \ldots p_n$ irreduzibel

$p_j \neq p_k$ für $j \neq k$

Partialbruchzerlegung

$\frac{p_1}{p_2}$: p_1, p_2 Polynome $p_2 \neq 0$

falls grad $p_1 \geq$ grad p_2 : $p_1 = q p_2 + r$ mit grad $r <$ grad p_2

$\frac{p_1}{p_2} = q + \frac{r}{p_2}$

Proposition

Seien $p, q \in K[x]$ mit $q \neq 0$ und $p = 0$ oder grad $p <$ grad q

(1) falls $q = q_1 \cdot q_2$ mit $\gcd(q_1, q_2) = 1$, dann $\exists!$ $p_1, p_2 \in K[x]$ mit $p_1 = 0$ oder grad $p_1 <$ grad q_1 und $p_2 = 0$ oder grad $p_2 <$ grad q_2, sodass $\frac{p}{q} = \frac{p_1}{q_1} + \frac{p_2}{q_2}$

(2) falls $q = c \cdot q_1^{k_1} \cdots q_n^{k_n}$ (in Standarddarstellung), dann

$\exists!$ $p_{1,0}, p_{1,1}, \ldots, p_{1,k_1-1}, p_{2,0}, \ldots, p_{n,k_n-1}$ mit $p_{r,s} = 0$ oder grad $p_{r,s} <$ grad p_r, sodass $\frac{p}{q} = \sum_{r=1}^{n} \sum_{s=0}^{k_r-1} \frac{p_{r,s}}{q_r^{s+1}}$

<u>Beweis</u>

(1) da $\gcd(q_1, q_2) = 1 \Rightarrow \exists u_1, u_2$ Polynome $u_1 q_1 + u_2 q_2 = 1$

$\Rightarrow p = (p u_1) q_1 + (p u_2) q_2$

Setze $k = \min \{\text{grad } u_1 : p = u_1 q_1 + u_2 q_2\}$

$(p = u_1 q_1 + u_2 q_2 = (u_1 + c x^m q_2) + (u_2 - c x^m q_1) q_2)$

es ist $k <$ grad q_2

$p = u_1 q_1 + u_2 q_2$ mit grad $u_1 <$ grad q_2

kann grad $u_2 \geq$ grad p? nein, weil grad $p <$ grad q

also grad $u_2 <$ grad q_1

$$\frac{p}{q} = \frac{u_1 q_1 + u_2 q_2}{q_1 \cdot q_2} = \frac{u_1}{q_2} + \frac{u_2}{q_1}$$

Eindeutigkeit: $\frac{p}{q} = \frac{p_1}{q_1} + \frac{p_2}{q_2} = \frac{\tilde{p_1}}{q_1} + \frac{\tilde{p_2}}{q_2} \Rightarrow$

$p_1 q_2 + p_2 q_1 = \tilde{p_1} q_2 + \tilde{p_2} q_1 \Rightarrow (p_2 - \tilde{p_2}) q_1 = (\tilde{p_1} - p_1) \cdot q_2$

$\Rightarrow q_1 \mid (\tilde{p_1} - p_1) q_2$ grad $(q_1, q_2) = 1$

$\Rightarrow q_1 \mid (\underbrace{\tilde{p_1} - p_1}_{\text{grad}})$ grad $q_1 \Rightarrow \tilde{p_1} - p_1 = 0 \Rightarrow \tilde{p_1} = p_1$

$\Rightarrow$ (durch einsetzen) $\tilde{p_2} = p_2$

(2) Induktion und (1)

$\frac{p}{q} = \frac{p_1}{q_1^{k_1}} + \frac{p_2}{q_2^{k_2}} + \ldots + \frac{p_n}{q_n^{k_n}}$

grad $p_r <$ grad $(q_j^{k_j}) = k_j$ grad q_j

$p_r \overset{DR}{=} q_j \tilde{p} + r$ grad $r <$ grad q_j

$\Rightarrow \frac{p_r}{q_j^{k_j}} = \frac{q_j \tilde{p} + r}{q_j^{k_j}} = \frac{\tilde{p}}{q_j^{k_j - 1}} + \frac{r}{q_j^{k_j}} \ldots$

$\frac{p_r}{q_j^{k_j}} = \frac{p_{j,k_j - 1}}{q_j^{k_j}} + \frac{p_{j,k_j - 2}}{q_j^{k_j - 1}} + \ldots + \frac{p_{j,0}}{q_j}$

Eindeutigkeit ähnlich wie oben □

Proposition

$K[x]$ ist ein Hauptidealring

Beweis

Sei $I \subseteq K[x]$ Ideal: falls $I = \{0\} = (0)$

Sei $I \neq \{0\}$ Setze $n := \min \{\text{grad } p : p \in I, p \neq 0\}$

$\exists p \in I$ mit grad $p = n$ offensichtlich $(p) \subseteq I$

Sei $q \in I \overset{DR}{\Rightarrow} \exists q_1, r$ mit $r = 0$ oder grad $r <$ grad p mit

$q = q_1 p + r \Rightarrow r = \underbrace{q}_{\in I} - \underbrace{q_1 p}_{\in I} \in I \Rightarrow r = 0$

$\Rightarrow q = q_1 p \in (p) \Rightarrow I \subseteq (p)$ □

In Hauptidealringen gilt: * eindeutige Primfaktorzerlegung
* irreduzibel $\Rightarrow$ prim

Proposition

Sei R Hauptidealring, $p \in R$ irreduzibel, dann ist p prim

Beweis

Seien $a, b \in R$ mit $p \mid a \cdot b$ falls $p \mid a$ ✓

es gelte jetzt $p \nmid a$. Setze $I := (a, p)$ Ideal

$\Rightarrow \exists q \in R$ mit $I = (q)$. Weil $p \in I \Rightarrow q \mid p$

angen. q keine Einheit $\exists x$ mit $p = x \cdot q \Rightarrow x$ Einheit

$a \in I \Rightarrow \exists u: a = u \cdot \underbrace{q}_{= x^{-1} \cdot p} = (u \cdot x^{-1}) \overset{\text{irred}}{p} \Rightarrow p \mid a$ ↯ WID

$\Rightarrow q$ Einheit $1 = q^{-1} \cdot \underbrace{q}_{\in I} \in I = (a, p) = aR + pR$

$\Rightarrow \exists u_1, u_2 \in R$ mit $1 = a u_1 + p u_2$

weil $p \mid a \cdot b$ $\exists u \in R$ mit $a \cdot b = u \cdot p$

$\Rightarrow b = \underbrace{a \cdot b}_{= u \cdot p} \cdot u_1 + p \cdot b \cdot u_2 = (u u_1 + b u_2) p \Rightarrow p \mid b$ □

---

p, q Polynome $p \circ q$ Polynom

Bsp: $p = x^3 + 2x + 5$ $q = x^2 + 3$

$p \circ q$: $x = y^2 + 3$

$p \circ q = (y^2 + 3)^2 + 2 \cdot (y^2 + 3) + 5$

$= y^6 + 9y^4 + 29 y^2 + 38$

Proposition

$p \in K[x]$, $q \in K[x]$ mit grad $q = 1$. Dann gilt

p irreduzibel $\Leftrightarrow$ $p \circ q$ irreduzibel

Beweis

$q = \underbrace{a_1}_{\neq 0} x + a_0$

angen: $p \circ q$ irreduzibel $p = q_1 \cdot q_2 \Rightarrow p \circ q = (q_1 \circ q) \cdot (q_2 \circ q)$

$\Rightarrow q_1 \circ q$ Einheit oder $q_2 \circ q$ Einheit. o.Bd.A $q_1 \circ q$ Einheit

angen: q_1 keine Einheit $\Rightarrow \exists\, n > 0 : \; q_1 = \sum_{j=0}^{n} b_j x^j$

$\Rightarrow q_1 \circ q = \sum_{j=0}^{n} b_j \underbrace{(a_1 y + a_0)^j}_{\text{bin. Lehrsatz}} = \underbrace{b_n}_{\neq 0} \underbrace{a_1^n}_{\neq 0} y^n + \ldots \Rightarrow q_1 \circ q$ keine Einheit

↯ WID

somit q_1 ist Einheit $\Rightarrow p$ irreduzibel

sei p irreduzibel.

$\tilde{q} := \frac{1}{a_1} x - \frac{a_0}{a_1}$ grad $\tilde{p} = 1$

$p \circ q \circ \tilde{q}$ $q \circ \tilde{q} = a_1 \left(\frac{1}{a_1} x - \frac{a_0}{a_1}\right) + a_0 = x$

$p \circ q \circ \tilde{q} = p$ $(p \circ q)$ ist irreduzibel, weil $(p \circ q) \circ \tilde{q}$ irreduzibel

□

Def: Sei K Körper, L Erweiterungskörper $(K \leq L)$

$p \in K[x]$. Dann heißt $a \in L$ <u>Nullstelle von p</u>, falls $p(a) = 0$

Proposition

$p \in K[x]$, $a \in K$ Nullstelle $\Rightarrow \exists\, q \in K[x]$ mit $p = (x-a) \cdot q$

Beweis

$\exists\, q, r$ mit $r = 0$ oder $r \in K \setminus \{0\}$

mit $p = (x-a) \cdot q + r \Rightarrow 0 = p(a) = 0 + r = r$ □

Def: Sei K Körper, L Körpererweiterung, $p \in K[x]$, $p \neq 0$

Weiters seien $a \in L$ und $n \in \mathbb{N}$. Dann heißt a eine <u>n-fache Nullstelle</u> von p, falls $\exists\, q \in L[x]$ mit $q(a) \neq 0$, sodass

$p = (x-a)^n \cdot q$

Proposition

char $K = 0$. Dann ist $a \in L$ genau dann n-fache Nullstelle, falls $p(a) = p'(a) = \ldots = p^{(n-1)}(a) = 0$ und $p^{(n)}(a) \neq 0$

falls p in K die Nullstellen $a_1, \ldots, a_n$ mit Vielfachheiten $k_1, \ldots, k_n$ hat, dann ist $\sum_{j=1}^{n} k_j \leq \text{grad } p$

K heißt <u>algebraisch abgeschlossen</u>, falls jedes nichtkonstante Polynom eine Nullstelle in K hat.

Fundamentalsatz der Algebra

Sei p ein nichtkonstantes Polynom über $\mathbb{C}$, dann gibt es ein $a \in \mathbb{C}$ mit $p(a) = 0$

Korollar

Sei $p \in \mathbb{C}[x]$ Dann ist p genau dann irreduzibel, wenn grad $p = 1$

Beweis

($\Leftarrow$) ✓

($\Rightarrow$) angen. grad $p > 1$ $\exists a \in \mathbb{C}$ mit $p(a) = 0$

$\Rightarrow p = (x-a) \underbrace{q}_{\text{nicht konstant}}$ ↯ WID also p irreduzibel □

über $\mathbb{C}$

z.B $5x - 3$ irreduzibel (Analysis: $5z - 3$ ↳ da komplexe Zahlen)

$x^2 + 1$ nicht irreduzibel

Zerlegung in Irreduzible: $p = a_n (x - x_1)^{k_1} \ldots (x - x_r)^{k_r}$

über $\mathbb{R}$

Proposition

Sei p ein Polynom über $\mathbb{R}$ mit grad $p = n \in \mathbb{N}$

Falls $a \in \mathbb{C}$ eine Nullstelle der Vielfachheit k ist, dann ist auch $\bar{a}$ eine Nullstelle der Vielfachheit k.

Es sei $a = b + ci$ mit $c \neq 0$ eine Nullstelle der Vielfachheit k. Dann ist $p = \underbrace{(x^2 - 2bx + (b^2 + c^2))^k}_{= (x-a)\cdot(x-\bar{a})} \cdot \underbrace{q}_{\in \mathbb{R}[x]}$, wobei $q(a) \neq 0$

Beweis

$p = \sum_{j=0}^{n} \underbrace{a_j}_{\in \mathbb{R}} x^j$, $p(a) = 0 \Rightarrow 0 = \bar{0} = \overline{p(a)} = \overline{\sum_{j=0}^{n} a_j \cdot a^j} = \sum_{j=0}^{n} \underbrace{\bar{a_j}}_{= a_j} \cdot \bar{a}^j =$

$= p(\bar{a})$

$(x-a)\cdot(x-\bar{a}) = (x^2 - \underbrace{(a+\bar{a})}_{2b} x + \underbrace{a\cdot\bar{a}}_{= b^2+c^2}) = x^2 - 2bx + (b^2+c^2) \in \mathbb{R}[x]$

$(x^2 - 2bx + (b^2+c^2)) = (x-a)\cdot(x-\bar{a}) \mid p$

Induktion $\Rightarrow p = (x^2 - 2bx + (b^2+c^2))^k \cdot q$ mit $q(a) \neq 0$ □

$x^2 + a_1 x + a_0$ ist irreduzibel über $\mathbb{R} \Leftrightarrow a_1^2 - 4a_0 < 0$

Proposition

p irreduzibel über $\mathbb{R} \Leftrightarrow$

1) grad $p = 1$

2) grad $p = 2$ und $p = a_2 x^2 + a_1 x + a_0$ mit $a_1^2 - 4a_0 a_2 < 0$ (= keine reellen NSt)

Beweis

($\Rightarrow$) ✓

($\Leftarrow$) sei grad $p > 2$

1. Fall p $a \in \mathbb{R}$ ist Nullstelle $\Rightarrow$ p nicht irreduzibel

2. Fall p hat keine reelle Nullstelle $\Rightarrow \exists\, a = b + ci$ $c \neq 0$ $\in \mathbb{C}$

mit $p(a) = 0 \overset{\text{Prop}}{\Rightarrow} p = (x^2 - 2bx + (b^2+c^2)) \cdot \underbrace{q}_{\text{grad} \geq 1}$

$\Rightarrow p$ nicht irreduzibel □

Zerlegung in Irreduzible: $p = a_n (x - x_1)^{k_1} \cdots (x - x_r)^{k_r} (x^2 + b_{1,1} x + b_{0,1})^{l_1} (x^2 + b_{1,s} + b_{0,s})^{l_s}$

über $\mathbb{Q}$

Def: Es sei $p = \sum_{j=0}^{n} a_j x^j \neq 0$ mit $a_0, a_1, \dots, a_n \in \mathbb{Z}$. Dann heißt p <u>primitiv</u>, falls $\gcd(a_0, a_1, \dots, a_n) = 1$

Es ist leicht zu sehen: $p \in \mathbb{Q}[x] \Rightarrow \exists\, c \in \mathbb{Q}$ mit $c \cdot p$ ist primitives Polynom über $\mathbb{Z}$

Def. Sei $q \in \mathbb{Q}$, $q \neq 0$ $\quad q = \prod_{\alpha \in \mathbb{P}} \alpha^{k_\alpha(q)}$ mit $k_\alpha(q) \in \mathbb{Z}$

Proposition

(1) $k_\alpha(q_1 \cdot q_2) = k_\alpha(q_1) + k_\alpha(q_2)$

(2) $k_\alpha(q_1 + q_2) \geq \min\{k_\alpha(q_1), k_\alpha(q_2)\}$

(3) falls $k_\alpha(q_1) < k_\alpha(q_2) \Rightarrow k_\alpha(q_1 + q_2) = \min\{k_\alpha(q_1), k_\alpha(q_2)\}$

<u>Beweis</u>

$$q_1 = \alpha^{k_\alpha(q_1)} \tilde{q}_1 \qquad q_2 = \alpha^{k_\alpha(q_2)} \cdot \tilde{q}_2$$

(1) $q_1 \cdot q_2 = \alpha^{k_\alpha(q_1) + k_\alpha(q_2)} \cdot \tilde{q}_1 \cdot \tilde{q}_2 \quad \Rightarrow k_\alpha(q_1 \cdot q_2) = k_\alpha(q_1) + k_\alpha(q_2)$

(2) $q_1 + q_2 = \alpha^{k} \left(\alpha^{\overbrace{k_\alpha(q_1) - k}^{\geq 0}} \tilde{q}_1 + \alpha^{\overbrace{k_\alpha(q_2) - k}^{\geq 0}} \tilde{q}_2 \right)$

$k = \min\{k_\alpha(q_1), k_\alpha(q_2)\}$

$\Rightarrow k_\alpha(q_1 + q_2) \geq k$

(3) $k = k_\alpha(q_1) \Rightarrow q_1 + q_2 = \alpha^{k} \left(\tilde{q}_1 + \alpha^{\overbrace{k_\alpha(q_2) - k}^{>0}} \cdot \tilde{q}_2 \right)$

$\Rightarrow k_\alpha(q_1 + q_2) = k$ $\square$

Sei $p = \sum_{j=0}^{n} a_j x^j$ Polynom über $\mathbb{Q}$, $p \neq 0$ und sei $\alpha \in \mathbb{P}$

Def $k_\alpha(p) := \min\{k_\alpha(a_j) : j \in \{0, 1, \dots, n\}, a_j \neq 0\}$

*) $p \in \mathbb{Z}[x] \Leftrightarrow k_\alpha(p) \geq 0 \quad \forall \alpha \in \mathbb{P}$

*) p primitiv über $\mathbb{Z} \Leftrightarrow k_\alpha(p) = 0 \quad \forall \alpha \in \mathbb{P}$

Proposition

$p_1 \neq 0,\ p_2 \neq 0 \ (\in \mathbb{Q}[x]),\ \alpha \in \mathbb{P}$. Dann gilt

$$k_\alpha(p_1 \cdot p_2) = k_\alpha(p_1) + k_\alpha(p_2)$$

Beweis

$$p_1 = \sum_{j=0}^{n_1} a_j x^j \qquad p_2 = \sum_{j=0}^{n_2} b_j x^j \qquad p_1 p_2 = \sum_{j=0}^{n_1+n_2} c_j x^j$$

$$c_j = \sum_{k=0}^{j} a_k \cdot b_{j-k}$$

$$k_\alpha(c_j) \geq \min\{\underbrace{k_\alpha(a_k b_{j-k})}_{\geq k_\alpha(a_k)+k_\alpha(b_{j-k}) \geq k_\alpha(p_1) \geq k_\alpha(p_2)}\ k\} \quad \Rightarrow k_\alpha(c_j) \geq k_\alpha(p_1) + k_\alpha(p_2)$$

$$\Rightarrow k_\alpha(p_1 \cdot p_2) \geq k_\alpha(p_1) + k_\alpha(p_2)$$

Sei $k := \max\{j : k_\alpha(a_j) = k_\alpha(p_1)\}$ und

$$\ell := \max\{j : k_\alpha(b_j) = k_\alpha(p_2)\}$$

$$c_{\ell+k} = a_k c_\ell + \sum_{j=k+1}^{\ell+k} a_j b_{\ell+k-j} + \sum_{j=0}^{k-1} a_j b_{\ell+k-j}$$

$$k_\alpha(\cdot) = \underbrace{k_\alpha(a_j)}_{>k_\alpha(p_1)} + \underbrace{k_\alpha(b_{\ell+k-1})}_{\geq k_\alpha(p_2)} \qquad k_\alpha(\cdot) = \underbrace{k_\alpha(a_j)}_{\geq k_\alpha(p_1)} + \underbrace{k_\alpha(b_{\ell+k-j})}_{>k_\alpha(p_2)}$$

$$\Rightarrow k_\alpha\Big(\sum_{\substack{j=0 \\ j\neq k}}^{\ell+k} a_j b_{\ell+k-j}\Big) > k_\alpha(p_1) + k_\alpha(p_2)$$

$$k_\alpha(a_k \cdot b_\ell) = k_\alpha(a_k) + k_\alpha(b_\ell) = k_\alpha(p_1) + k_\alpha(p_2)$$

$$\Rightarrow k_\alpha(c_{\ell+k}) = k_\alpha(p_1) + k_\alpha(p_2)$$

Somit $k_\alpha(p_1 \cdot p_2) = k_\alpha(p_1) + k_\alpha(p_2)$ □

Horner Schema

$x^3 + x^2 - x - 1$

	1	1	-1	-1
2	1	3	5	9
①	1	2	1	0

Proposition

es sei $p = \sum_{j=0}^{n} a_j x^j$ primitives Polynom über $\mathbb{Z}$. Dann ist p genau dann über $\mathbb{Q}$ irreduzibel, wenn p über $\mathbb{Z}$ irreduzibel ist.

Beweis

($\Rightarrow$) angen: p nicht irred. über $\mathbb{Z}$ $\Rightarrow p = \underbrace{q_1 \cdot q_2}_{\in \mathbb{Z}[x] \text{ keine Einheiten}}$ ↯ WID ($\mathbb{Z} \subseteq \mathbb{Q}$)

($\Leftarrow$) seien $q_1, q_2 \in \mathbb{Q}[x]$ so, dass $p = q_1 \cdot q_2$

sei $\alpha \in \mathbb{P}$ $\quad 0 = k_\alpha(\underbrace{p}_{q_1 \cdot q_2}) = k_\alpha(q_1) + k_\alpha(q_2)$

$\Rightarrow k_\alpha(q_1) = -k_\alpha(q_2)$

setze $c := \prod_{\alpha \in \mathbb{P}} \alpha^{-k_\alpha(q_1)} = \prod_{\alpha \in \mathbb{P}} \alpha^{k_\alpha(q_2)} \in \mathbb{Q}$ Einheiten

$c \cdot q_1 = k_\alpha(c \cdot q_1) = \underbrace{k_\alpha(c)}_{= -k_\alpha(q_1)} \cdot k_\alpha(q_1) = 0 \quad \Rightarrow c q_1 \in \mathbb{Z}[x]$

$\frac{1}{2} q_2 = k_\alpha(\frac{1}{c} q_2) = \underbrace{k_\alpha(\frac{1}{c})}_{= k_\alpha(q_1) = -k_\alpha(q_2)} k_\alpha(q_2) = 0 \quad \Rightarrow \frac{1}{c} q_2 \in \mathbb{Z}[x]$

$\Rightarrow p = q_1 \cdot q_2 = \underbrace{(c \cdot q_1)}_{\in \mathbb{Z}[x]} \cdot \underbrace{(\frac{1}{c} q_2)}_{\in \mathbb{Z}[x]} \quad \Rightarrow c \cdot q_1 \in \{1, -1\}$ oder

$\frac{1}{c} q_2 \in \{\pm 1\} \quad \Rightarrow q_1 \in \{\underbrace{\frac{1}{c}, -\frac{1}{c}}_{\text{Einheiten in } \mathbb{Q}}\}$ oder $q_2 \in \{\underbrace{c, -c}_{\text{Einheiten in } \mathbb{Q}}\}$

$\Rightarrow p$ ist irreduzibel über $\mathbb{Q}$

Korollar

$p = \underset{\neq 0}{a_n} x^n + \ldots + a_1 x + a_0 \in \mathbb{Z}[x]$

(1) falls $a \in \mathbb{Z}$, $b \in \mathbb{N}$ mit $\gcd(a,b) = 1$ mit $p(\frac{a}{b}) = 0$

$\Rightarrow a \mid a_0$ und $b \mid a_n$

(2) falls $a, b \in \mathbb{Z}$, $c \in \mathbb{N}$, $\gcd(a,b,c) = 1$ mit $p(\frac{a+bi}{c}) = 0$

und $b \neq 0 \Rightarrow c^2 \mid a_n$ und $(a^2 + b^2) \mid a_0$

(3) wenn $a_n = 1$ $q \in \mathbb{Q}$ Nullstelle $\Rightarrow q \in \mathbb{Z}$ und $q \mid a_0$

Beweis

(1) $(bx - a) \mid p \Rightarrow p = (bx - a) \cdot \underbrace{q}_{\in \mathbb{Z}[x]} \qquad q = \sum_{j=0}^{n-1} b_j x^j$

$a_n = b_{n-1} \cdot b$, $\quad a_0 = (-a) b_0 = -a b_0$

(2) analog (mit konjugiert Komplexem?)

(3) $q = \frac{a}{b} \overset{(1)}{\Longrightarrow} b \mid a_n = 1 \Rightarrow b = 1$ □

Satz von Eisenstein

es sei $p = \sum_{j=0}^{n} a_j x^j \in \mathbb{Z}[x]$ mit $a_n \neq 0$. Falls es eine Primzahl α gibt mit $\alpha \nmid a_n$, $\alpha \mid a_j$ für $j \in \{0,1,\dots,n-1\}$ und $\alpha^2 \mid a_0$, dann ist p irreduzibel über $\mathbb{Q}$

Beweis

$d := \gcd(a_n, a_{n-1}, \dots, a_0)$, $\gcd(\alpha, d) = 1$

($\alpha \nmid \frac{a_n}{d}$, $\alpha \mid \frac{a_j}{d}$ für $j \in 0,1,\dots,n-1$, $\alpha^2 \nmid \frac{a_0}{d}$)

o.B.d.A p primitiv

angen. p ist nicht irreduzibel

$\Rightarrow \exists\, q_1 = \sum_{j=0}^{n_1} b_j x^j$, $q_2 = \sum_{j=0}^{n_2} c_j x^j$ mit $n_1, n_2 \geq 1$

$n_1 + n_2 = n$ $\in \mathbb{Z}[x]$, sodass $p = q_1 q_2$

$a_0 = b_0 c_0$ $\alpha \mid a_0 = b_0 \cdot c_0 \Rightarrow \alpha \mid b_0$ oder $\alpha \mid c_0$

o.B.d.A $\alpha \mid b_0$

angen. $\alpha \mid c_0 \Rightarrow \alpha^2 \mid b_0 c_0 = a_0$ ↯ WID also $\alpha \nmid c_0$

Behauptung: für $j \in \{0,1,\dots,n_1\}$ $\alpha \mid b_j$

Beweis der Behauptung:

Induktion: $j = 0$: $\alpha \mid b_0$ ✓

sei $j > 0$ $\alpha \mid a_j = c_0 b_j + \sum_{k=0}^{j-1} \underbrace{b_k}_{\alpha \mid b_k} c_{j-k}$

$\Rightarrow \alpha \mid b_j c_0 \overset{\alpha \nmid c_0}{\Longrightarrow} \alpha \mid b_j$ ◇

insbesondere $\alpha \mid b_{n_1}$

$\alpha \mid b_{n_1} \cdot c_{n_2} = a_n$ ↯ WID

daher ist p irreduzibel □

Bsp $p = 2x^3 + 30x^2 - 90$ (normalerweise durch 2 dividieren)

$5 \in \mathbb{P}$, $5 \nmid 2$ ✓

$5 \mid 30$ ✓

$5 \mid 0$

$5 \mid (-90)$ $\quad 5^2 \nmid 90$ ✓

Satz v. Eisenstein $\Rightarrow$ p irreduzibel über $\mathbb{Q}$

Bsp $p = x^4 + x^3 + x^2 + x + 1$

Satz v. Eisenstein nicht anwendbar
endl. geom. Reihe → Analysis

$$= \frac{1-x^5}{1-x} = \frac{x^5-1}{x-1}$$

$x = y+1$ $\quad p(y+1) = \frac{(y+1)^5 - 1}{y} = y^5 + \binom{5}{1}y^4$

$$= \frac{y^5 + \binom{5}{4}y^4 + \binom{5}{3}y^3 + \binom{5}{2}y^2 + \binom{5}{1}y + 1 - 1}{y} =$$

$$= y^4 + \binom{5}{4}y^3 + \binom{5}{3}y^2 + \binom{5}{2}y + \binom{5}{1} = y^4 + 5y^3 + 10y^2 + 10y + 5$$

$5 \in \mathbb{P}$ $\quad 5 \nmid 1$

$5 \mid 5$, $5 \mid 10$, $5 \mid 10$, $5 \mid 5$

$5^2 \nmid 5$ $\quad \overset{\text{Eisenstein}}{\Rightarrow}$ p ist irreduzibel über $\mathbb{Q}$

n Primzahl, $j \in \{1, 2, \dots, n-1\} \Rightarrow n \mid \binom{n}{j}$

$$\binom{n}{j} \in \mathbb{Z}, \quad \binom{n}{j} := \frac{n \cdot (n-1) \cdot \dots \cdot (n+1-j)}{j!} \quad (n \nmid j! \text{ weil } n \in \mathbb{P}) =$$

$$= n \cdot \underbrace{\frac{(n-1) \cdot \dots \cdot (n+1-j)}{j!}}_{\in \mathbb{Z}} \Rightarrow n \mid \binom{n}{j}$$

III Körpererweiterungen

1) Einheitswurzel

Satz

Sei $K(+,\cdot)$ Körper, $G \subseteq K \setminus \{0\}$ eine endliche Gruppe. Dann ist G zyklisch und $\exists\, n$ mit $G = \{a \in K : a^n = 1\}$

Beweis

$n := \min \{ \operatorname{ord}(a) : a \in G \}$

$\exists\, a \in G$ mit $\operatorname{ord}(a) = n$

Sei $b \in G$. Annahme: $\underbrace{\operatorname{ord}(b)}_{=:k} \nmid n$

$\Rightarrow \exists\, p \in \mathbb{P}$ mit $k_p(n) < k_p(k)$ (wie oft etwas vorkommt siehe vorher)

$$\operatorname{ord}\left(\underbrace{a^{p^{k_p(n)}}}_{=:a_1}\right) = \frac{n}{p^{k_p(n)}} \qquad \operatorname{ord}\left(\underbrace{b^{\frac{k}{p^{k_p(k)}}}}_{=:b_1}\right) = p^{k_p(k)}$$

$$\gcd\left(\frac{n}{p^{k_p(n)}}, p^{k_p(k)}\right) = 1$$

$$\operatorname{ord}(a_1, b_1) = n \cdot \underbrace{p^{k_p(k) - k_p(n)}}_{>1} > 1$$

↯ WID zu n ist minimum aller ordnungen

also $\operatorname{ord}(b) \mid n$

$$\Rightarrow b^n = \left(\underbrace{b^{\operatorname{ord}(b)}}_{=1}\right)^{\frac{n}{\operatorname{ord}(b)}} = 1$$

b Nullstelle von $x^n - 1$ — es kann höchstens n Nullstellen haben

$\Rightarrow \operatorname{card}(G) \leq n$ (Anzahl der Elemente) $\qquad \{1, a, a^2, \ldots, a^{n-1}\} \subseteq G$

$\Rightarrow G = \{1, a, a^2, \ldots, a^{n-1}\}$ und daher auch zyklisch (a ist erzeugendes Element) □

2) Minimalpolynom

$K \subseteq L$ $\quad \hat{=}$ L ist Körpererweiterung von K

Def: $K \subseteq L$, $a \in L$ heißt <u>algebraisch über K</u> falls $\exists\, p \in K[x]$ (o.B.d.A irreduzibel) mit $p(a) = 0$

<u>algebraisch</u> ... $\hat{=}$ algebraisch über $\mathbb{Q}$

nicht algebraische Elemente heißen <u>transzendent</u>

Def: L heißt <u>algebraisch über K</u>, falls $\forall a \in L$ algebraisch über K sind.

L kann als ein Vektorraum über K aufgefasst werden

Def: L heißt <u>endliche Erweiterung</u> falls $\dim_K L$ endlich ist
($\dim_K L$ ist der grad der Erweiterung)

Def: $K \subseteq L$, $a_1, a_2, \ldots, a_n \in L$

$$K(a_1, \ldots, a_n) = \bigcap_{\substack{\tilde{L} \subseteq L \\ K \subseteq \tilde{L} \\ a_1 \ldots, a_n \in \tilde{L}}} \tilde{L}$$ <u>kleinster Körper, der $K, a_1, \ldots, a_n$ enthält</u>

$$K(a_1, a_2, \ldots, a_n) = K(a_1)(a_2)\ldots(a_n)$$

$$K(a) = \left\{ \sum_{j=0}^{n-1} x_j a^j : x_0, \ldots, x_{n-1} \in K \right\}$$ n... Grad vom Minimalpolynom p
$n = \dim_K L$

$$x^n + a_{n-1}x^{n-1} + \ldots + a_0 \qquad a^n = -a_{n-1}a^{n-1} - a_{n-2}a^{n-1} + \ldots - a_0$$

Def. $K \subseteq L$, $a \in L$ algebraisch. Dann heißt $p \in K[x]$
<u>Minimalpolynom</u> von a, falls $p(a) = 0$ und wenn $q \in K[x]$
$q(a) = 0 \Rightarrow \operatorname{grad} q \geq \operatorname{grad} p$

Proposition

$K \subseteq L$, $a \in L$, $p \in K[x]$

(1) p Minimalpolynom von a $q \in K[x]$, $q(a) = 0 \Rightarrow p \mid q$

(2) p, q Minimalpolynome von $a \Rightarrow \exists\, c \in K \setminus \{0\}$ mit $p = cq$

(3) p Minimalpolynom von $a \Rightarrow p$ irreduzibel über K

(4) p irreduzibel, $p(a) = 0 \Rightarrow p$ Minimalpolynom von a

(5) char $K = 0$, p irreduzibel, $p(a) = 0 \Rightarrow a$ einfache Nullstelle

Beweis

(1) $q = s \cdot p + r$ mit $r=0$ oder $\operatorname{grad} r < \operatorname{grad} p$

$0 = q(a) = s(a) \cdot \underbrace{p(a)}_{=0} + r(a) \Rightarrow r = 0 \Rightarrow p \mid q$

(2) $p \mid q$, $q \mid p \Rightarrow \exists c$ mit $p = c \cdot q$

(3) angen. $p = q_1 \cdot q_2$ mit q_1, q_2 keine Einheiten

$\Rightarrow \operatorname{grad} q_1 < \operatorname{grad} p$, $\operatorname{grad} q_2 < \operatorname{grad} p$

$0 = p(a) = q_1(a) \cdot q_2(a) \Rightarrow q_1(a) = 0$ oder $q_2(a) = 0$ ↯ WID

(4) sei p_1 Minimalpolynom von a $\overset{(1)}{\Rightarrow} p_1 \mid p \overset{p \text{ irred.}}{\Rightarrow} p = c \cdot p_1$.

(5) angen. $p = (x-a)^k \cdot q$ $k > 1$

$p' = k \cdot (x-a)^{k-1} \cdot q + (x-a)^k \cdot q' \Rightarrow p'(a) = 0$

$\operatorname{grad} p' = \operatorname{grad} p - 1$ ↯ WID □

Proposition

$K \subseteq L$ (1) L endliche Erweiterung $\Rightarrow L$ algebraisch

(2) $a \in L$ algebraisch $\Rightarrow K(a)$ endlich

Algebr. Zahlen sind: abzählbar, nicht vollständig

Beweis

(2) ✓

(1) sei $a \in L$, $\dim_K L := n$ $\{1, a, a^2, \dots, a^n\}$ linear abh.

$\Rightarrow \exists a_0, \dots, a_n \in K$ mit $a_0 + a_1 a + \dots + a_n a^n = 0$ □

Proposition

$K \subseteq L$, $a, b \in L$, $p \in K[x]$ $\varphi : K \to L$ injektiver Homomorphismus

p irreduzibel, $p(a) = p(b) = 0$

(1) $\exists \tilde{\varphi} : K(a) \to L$ Homomorphismus mit $\tilde{\varphi}|_K = \varphi$ und $\tilde{\varphi}(a) = b$

(2) falls $K \subseteq \hat{L} \subseteq L$, $\hat{L}$ endl. Erweiterung mit $a \in \hat{L}$

$\Rightarrow \exists \tilde{\varphi} : \hat{L} \to L$ Homomorphismus $\tilde{\varphi}|_K = \varphi$ und $\tilde{\varphi}(a) = b$

Beweis

(1) $K(a) = \left\{ \sum_{j=0}^{n-1} x_j a^j \right\}$

$\tilde{\varphi}\left(\sum_{j=0}^{n-1} x_j a^j\right) := \sum_{j=0}^{n-1} \varphi(x_j) b^j$ Homomorphismus

(2) Sei L_K konstruiert $(L_1 = K \subseteq L_1 \subseteq \dots \subseteq L_K \subseteq \tilde{L})$

$\tilde{\varphi}_K : L_K \to L$ konstruiert

falls $L_K = \tilde{L}$ ✓

sonst $\exists\ c \in \tilde{L} \setminus L_K$, betrachte Minimalpolynom von c

$L_{K+1} := L_K(c) \overset{(1)}{\Rightarrow} \exists \tilde{\varphi}_{K+1} : L_{K+1} \to L$ mit $\tilde{\varphi}_{K+1}|_{L_K} = \tilde{\varphi}_K$

und $\tilde{\varphi}_{K+1}(c) = c$ □

3) Galoisgruppen

$K \subseteq L$ $(\to \mathbb{Q} \subseteq K \subseteq L \subseteq \mathbb{C})$ Körpererweiterungen

Sei K Körper, p irreduzibel in $K[x]$ Dann hat p verschiedene Nullstellen $a_1, a_2, \dots, a_n \in \mathbb{C}$ $(n = \text{grad } p)$

Def: $K(p) := K(a_1, \dots, a_n)$ Körper mit allen Nst von p erweitern

Satz

Seien $p_1, \dots, p_n$ irreduzible Polynome über $\mathbb{Q}$. Sei q ein irreduzibles Polynom über $\mathbb{Q}$ $a_1, \dots, a_k$ die Nullstellen von q.

Falls $a_1 \in \mathbb{Q}(p_1, \dots, p_n)$, dann ist $a_j \in \mathbb{Q}(p_1, \dots, p_n)\ \forall j$

irred Polynom 1 Nst in Körper, dann alle Nst drinnen

(<u>separabel</u>)

<u>Beweis</u>

Sei $j \in \{1, 2, \dots, k\}$ $\exists$ inj. Homomorphismus $\varphi : K := \mathbb{Q}(p_1, \dots, p_n) \to \mathbb{C}$

mit $\varphi|_{\mathbb{Q}} = \text{id}_{\mathbb{Q}}$ und $\varphi(a_1) = a_j$

sei $r \in \{1, 2, \dots, n\}$ p_r hat die Nullstellen $b_1, \dots, b_s$

sei $t \in \{1, \dots, s\}$ $p_r(b_t) = 0$

$0 = \varphi(0) = \varphi(p_r(b_t)) = p_r(\varphi(b_t)) \Rightarrow \varphi(b_t) \in K$ (da Nullstelle)

somit ist $\varphi : K \to K$

insbesondere ist $a_j = \varphi(\underbrace{a_1}_{\in K}) \in K$ □

Def: $K \subseteq L$ endlich. Dann heißt $\underline{Gal(L,K)} = \{\varphi : L \to L$ Automorphismus mit $\varphi|_K = id_K\}$ Galoisgruppe von L über K

falls G Untergruppe von $Gal(L,K)$, dann heißt

$\underline{Fix(G)} := \{x \in L : \varphi(x) = x \ \forall \varphi \in G\}$ der Fixkörper von G

p Polynom (irreduzibel) $Gal(p) = Gal(\mathbb{Q}(p), \mathbb{Q})$

p hat Nullstellen $a_1, \dots, a_n$

$\varphi \in Gal(p)$ $\varphi(a_j) \in \{a_1, \dots, a_n\}$

erhalten Permutation von $\{a_1, \dots, a_n\}$ $Gal(p) \subseteq S_n$

Proposition

$L := \mathbb{Q}(\underbrace{p_1, \dots, p_n}_{\text{irreduzibel}})$ $K \subseteq L$ $Fix(Gal(L,K)) = K$

falls $Gal(L,K) = \{id\} \Rightarrow L = K$

Beweis

$\tilde{K} := Fix(Gal(L,K)) \supseteq K$

angen: $\tilde{K} \neq K \Rightarrow \exists\, a \in \tilde{K} \setminus K$ p Minimalpolynom von a über K (grad ≥ 2) $\Rightarrow \exists\, b \neq a$ mit $p(b) = 0$

Satz $\Rightarrow b \in L$

$\exists\, \varphi : \tilde{K} \xrightarrow{L} L$ mit $\varphi(a) = b$ und $\varphi|_K = id_K$

$\Rightarrow \varphi \in Gal(L,K)$ $\varphi(a) = b \neq a$ ↯ WID (da a im Fix. der Galgruppe also $\varphi(a) = a$ müsste)

also $\tilde{K} = K$

analog $Gal(\tilde{L},K) = \{id\} \Rightarrow \tilde{L} = K$ □

Algebraische Formel: $p = a_n x^n + \dots + a_0$

darf vorkommen: $+, -, \times, \div$, $\underbrace{\sqrt[n]{a}}_{\text{Nullstellen von } x^n - a}$, n-te Einheitswurzeln $(e^{\frac{2\pi i}{n}})$

Def: p heißt auflösbar (durch algebraische Formel der Koeffizienten beschreibbar) falls $\exists\, K_1 = \mathbb{Q} \subseteq K_2 \subseteq \dots \subseteq K_n$, alle Nullstellen von p

liegen in K_n und $\forall j \in \{2,\dots,n\}$ ist $K_j = K_{j-1}(e^{\frac{2\pi i}{n}})$ oder $K_j = K_{j-1}(a)$, wobei a Nullstelle von $x^n - a$ ist.

Lemma

$K \subseteq \underbrace{L_1}_{\text{separabel}} \subseteq L_2$

(1) $Gal(L_2, K)$ auflösbar $\Rightarrow Gal(L_1, K)$ auflösbar

(2) $Gal(L_1, K)$ auflösbar, $Gal(L_2, L_1)$ Abel'sch $\Rightarrow Gal(L_2, K)$ auflösbar

Beweis

$\Psi: Gal(L_2, K) \to Gal(L_1, K)$, $\Psi(\varphi) := \varphi|_{L_1}$

$\varphi|_{L_1}: L_1 \to L_2$, weil L_1 separabel ist $\varphi|_{L_1}: L_1 \to L_1$

$\Psi(\varphi_1 \circ \varphi_2) = \varphi_1|_{L_1} \circ \varphi_2|_{L_1}$

Ψ ist surjektiver Homomorphismus (Erweiterungseigenschaft)

$Gal(L_2, K)/\ker\Psi \underset{\text{isomorph}}{\cong} Gal(L_1, K)$

$\ker\Psi = \{\varphi : \varphi|_{L_1} = id|_{L_1}\} = Gal(L_2, L_1)$

haben gezeigt: $Gal(L_2, K)/_{Gal(L_2, L_1)} \cong Gal(L_1, K)$

$H \underset{\text{untergruppe}}{\leq} Gal(L_2, K)$

$D(\Psi(H)) = \langle \{\underbrace{\Psi(a)\cdot\Psi(b)\cdot\Psi(a)^{-1}\cdot\Psi(b)^{-1}}_{= \Psi(a\cdot b\cdot a^{-1}\cdot b^{-1})}\} \rangle = \Psi(D(H))$

$\forall k: \Psi(D^{(k)}(Gal(L_2, K))) = D^{(k)}(Gal(L_1, K))$

(1) $\exists k: D^{(k)}(Gal(L_2, K)) = \{id\} \Rightarrow$

$\Rightarrow D^{(k)}(Gal(L_1, K)) = \{id\} \Rightarrow Gal(L_1, K)$ auflösbar

(2) $\exists k: D^{(k)}(Gal(L_1, K)) = \{id\}$

$\Rightarrow \Psi(D^{(k)}(Gal(L_2, K))) = \{id\}$

$\Rightarrow D^{(k)}(Gal(L_2, K)) \subseteq Gal(L_2, L_1) \Rightarrow$

$\Rightarrow D^{(k+1)}(Gal(L_2, K)) = \{id\} \Rightarrow Gal(L_2, K)$ auflösbar

Satz

Sei p ein irreduzibles Polynom über $\mathbb{Q}$. Falls p auflösbar ist, dann ist $Gal(\mathbb{Q}(p), \mathbb{Q})$ auflösbar.

(es gilt sogar: p auflösbar $\Leftrightarrow$ $Gal(\mathbb{Q}(p), \mathbb{Q})$ auflösbar)

Beweis

$\exists\ K_0 = \mathbb{Q} \subseteq K_1 \subseteq \dots \subseteq K_n$ mit $\mathbb{Q}(p) \subseteq K_n$

$K_{j+1} = K_j(a)$ mit a Nullstelle von $x^n - 1$ oder $x^n - b$

Wir konstruieren: $L_0 = \mathbb{Q} \subseteq L_1 \subseteq \dots \subseteq L_r$, L_j separabel, $Gal(L_j, \mathbb{Q})$ auflösbar

$K_n \subseteq L_r$ wie folgt $K_j \subseteq L_k$ konstruiert

1. Fall $K_{j+1} = K_j(a)$ mit a Nullstelle von $x^n - 1$

Sei q Minimalpolynom von a

$\langle a \rangle$ zyklisch und enthält alle Nullstellen von q

$\varphi \in Gal(L_k(a), L_k)$

$\varphi(a) = a^s \Rightarrow \varphi(a^u) = a^{s \cdot u}$

$|\langle a \rangle| = \ell$ Wähle t so, dass $ggT(t, \ell) = 1$

$\varphi_0(a) = a^t$ $\quad \varphi(a) = a^s = \underbrace{\varphi_0^{\tilde{t}}(a)}_{= a^{t\tilde{t}}}$

$Gal(L_k(a), L_k)$ zyklisch, Abel'sch $\overset{\text{Lemma}}{\Longrightarrow}$

$Gal(\underbrace{L_k(a)}_{= L_{k+1}}, \mathbb{Q})$ auflösbar $\quad L_{k+1} \supseteq K_{j+1} = K_j(a)$

2. Fall

$K_{j+1} = K_j(a)$, wobei a Nullstelle von $x^n - b$

$L_{k+1} := L_k(e^{\frac{2\pi i}{n}}) \overset{\text{gerade gezeigt}}{\Longrightarrow} Gal(L_{k+1}, \mathbb{Q})$ auflösbar

$L_{k+2} := L_{k+1}(a) \supseteq K_j(a) = K_{j+1}$

$\varphi \in Gal(L_{k+2}, L_{k+1})$: Nullstellen von $x^n - b$:

$a,\ a \cdot \underbrace{e^{\frac{2\pi i}{n}}}_{\omega \in L_{k+1}},\ a \cdot \underbrace{e^{\frac{2\pi i}{n} \cdot 2}}_{\omega^2 \in L_{k+1}},\ \dots,\ a \cdot \underbrace{e^{\frac{2\pi i}{n}(n-1)}}_{\omega^{n-1} \in L_{k+1}} \in L_{k+2}$ separabel

$\varphi(a) = \omega^l \cdot a$

$\varphi(\omega^u \cdot a) = \underbrace{\varphi(\omega^u)}_{=\omega^u} \cdot \underbrace{\varphi(a)}_{=\omega^l \cdot a} = \omega^l \cdot (\omega^u \cdot a)$

$\varphi_0(a) = \omega \cdot a$

$\varphi(a) = \varphi_0^l(a) \Rightarrow Gal(L_{k+2}, L_{k+1})$ zyklisch, Abel'sch

$\overset{\text{Lemma}}{\Rightarrow} Gal(L_{k+2}, \mathbb{Q})$ auflösbar

$\mathbb{Q}(p) \subseteq L_r$ $\quad Gal(L_p, \mathbb{Q})$ auflösbar $\overset{\text{Lemma}}{\Rightarrow}$

separabel separabel

$\Rightarrow Gal(\mathbb{Q}(p), \mathbb{Q})$ auflösbar $\square$

Satz

Falls $n \geq 5$ ist das allgemeine Polynom n-ten Grades nicht auflösbar

Beweis

o.B.d.A p irreduzibel hat n verschiedene Nullstellen $a_1, \dots, a_n$

man kann $\varphi: \mathbb{Q}(p) \to \mathbb{Q}(p)$ sodass $\varphi(a_j) = a_{\sigma(j)}$ für eine beliebige Permutation $\sigma \in S_n$ (Homomorphismus)

$\Rightarrow Gal(\mathbb{Q}(p), \mathbb{Q}(p)) \cong S_n$

S_n ist nicht auflösbar $\overset{\text{Satz}}{\Rightarrow}$ p ist nicht auflösbar $\square$

Satz

Sei n eine Primzahl, p ein irreduzibles Polynom über $\mathbb{Q}$ vom grad n, a_1, a_2 verschiedene Nullstellen von p. Falls $Gal(\mathbb{Q}(p), \mathbb{Q})$ auflösbar ist, dann ist $\mathbb{Q}(p) = \mathbb{Q}(a_1, a_2)$

Beweis

1. Schritt Setze $G := Gal(\mathbb{Q}(p), \mathbb{Q})$

Behauptung G enthält einen Normalteiler G_0 mit n Elementen.

Dieser ist zyklisch, also $G_0 = \{\sigma^k : k \in \mathbb{N}\}$

Beweis der Behauptung

$$D^0(a) = a \geq D^{(1)}(a) \geq \ldots \geq \underbrace{D^{(k)}(a)}_{\neq \{id\}} \geq D^{(k+1)}(a) = \{id\}$$

Seien $a_1, \ldots, a_n$ alle Nullstellen von p

V_j: $\exists \varphi \in a$ mit $\varphi_j(a_1) = a_j$

angenommen l erfüllt: V_j $\exists \varphi_j \in D^{(l)}(a)$ mit $\varphi_j(a_1) = a_j$

für $j \in \{1, 2, \ldots, n\}$ setze $B_j := \{\varphi(a_j) : \varphi \in D^{(l+1)}(a)\}$

$\{B_1, \ldots, B_n\}$ Klasseneinteilung z.B. r Klassen

$\underbrace{\varphi_j(B_1)}_{\varphi_j(a_1) \in a_j} = B_j$ jede Klasse hat z.B. s Elemente (gleich viele)

$n = r \cdot s \overset{n \text{ prim}}{\Rightarrow} r = 1$ oder $s = 1$

sei $s = 1$ $a_j \in B_j = B_j = \{a_j\}$

für $\varphi \in D^{(l+1)}(a)$ muss $\varphi(a_j) = a_j$ $\forall j$ gelten $\Rightarrow \varphi = id$

$\Rightarrow D^{(l+1)}(a) = \{id\}$

für $l < k$ ist $r = 1$ $B_1 = \{a_1, \ldots, a_n\}$

$\Rightarrow V_j$ $\exists \tilde{\varphi}_j \in D^{(l+1)}(a)$ mit $\tilde{\varphi}_j(a_1) = a_j$

insbesondere card $(D^{(k)}(a)) \geq n$

Sei $\varphi \in D^{(k)}(a)$, $\varphi \neq id$ $\Rightarrow s := \text{ord}(\varphi) > 1$

$D^{(k)}(a)$ Abelsch, $\{\varphi^l : l \in \mathbb{Z}\}$ Untergruppe von $D^{(k)}(a)$ Normalteiler

Argument von vorher: $\forall j$ $\exists \varphi_j \in \{\varphi^l : l \in \mathbb{Z}\}$ mit $\varphi_j(a_1) = a_j$

$\Rightarrow s \geq n$

angen. $\exists \varphi \in D^{(k)}(a)$ mit $\varphi \neq id$ und $\text{ord}(\varphi) \neq n$

$s \mid n!$, da $a \leq S_n$ $\Rightarrow \exists t \in \{2, \ldots, n-1\}$ mit $t \mid s$

$\text{ord}(\varphi^{\frac{s}{t}}) = t \geq n$ ↯ WID

daher ist $D^{(k)}(a)$ zyklisch mit n Elementen

Sei $\varphi \in G$ $\{\varphi^{-1} \cdot \tau \cdot \varphi : \tau \in D^{(k)}(a)\}$

$(\varphi^{-1} \tau_1 \varphi) \cdot (\varphi^{-1} \tau_2 \varphi)^{-1} = \varphi^{-1} \tau_1 \tau_2^{-1} \varphi \in$ ↖

ist Untergruppe mit n Elementen.

Falls $\{\varphi^{-1}\tau\varphi : \tau \in D^{(k)}(a)\} \neq D^{(k)}(a)$

$G/D^{(k)}(a)$ hat $\cong \{\varphi^{-1}\tau\varphi : \tau \in D^{(k)}(a)\}$ als Untergruppe

$\Rightarrow n \mid \text{card } G/D^{(k)}(a) \Rightarrow n^2 / \text{card } G \mid n!$ ↯ WID

also $\forall \tau : \varphi^{-1}\tau\varphi = \tau^r$

$\Rightarrow \tau^{-1}\varphi^{-1}\tau\varphi = \tau^{r-1} \in D^{(k)}(a)$ Normalteiler ◇

2. Schritt

Behauptung: Sei $\varphi \in G$ mit $\varphi(a_1) = a_1$ und $\varphi(a_2) = a_2$.

Dann ist $\varphi = id$

Beweis der Behauptung: $G_0 = \{\sigma^l : l \in \mathbb{Z}\}$

σ kann als Permutation auf $\{1,\dots,n\}$ aufgefasst werden

$\text{ord}\,\sigma = n \Rightarrow \sigma$ ist n-Zyklus

o.B.d.A $\sigma = (1\ 2\ \dots\ n)$

φ kann auch als Permutation auf $\{1,2,\dots n\}$ aufgefasst werden

$\Rightarrow \exists j \neq k$ mit $\varphi(j) = j$ und $\varphi(k) = k$

(Rechnungen immer modulo n (n statt 0 schreiben))

G_0 ist Normalteiler $\exists r$ mit $\varphi\sigma = \sigma^r\varphi$

Sei $s \in \{1,\dots,n\}$

$$\varphi(s+1) = \varphi(\underbrace{\sigma(s)}_{s+1}) = \sigma^r\varphi(s) = \varphi(s) + r$$

Behauptung: $\varphi(s) = \varphi(1) + r\cdot(s-1)$

Beweis der Behauptung: $\varphi(1) + r\cdot(1-1) = \varphi(1)$ damit für s=1 gezeigt

Sei $s>1$ $\varphi(s) = \varphi(s-1+1) = \underbrace{\varphi(s-1)}_{=\varphi(1)+r\cdot(s-2)} + r = \varphi(1) + r\cdot(s-1)$ ◇

$\int = \varphi(j) = \varphi(1) + r\cdot(j-1)$

$k = \varphi(k) = \varphi(1) + r\cdot(k-1)$

$\Rightarrow \underbrace{j-k}_{1\dots<n} = r\cdot(j-k)$

$\Rightarrow r = 1$

$\Rightarrow \quad s = \varphi(1) + s - 1 \quad \Rightarrow \quad \varphi(1) = 1$

$\varphi(s) = \underbrace{\varphi(1)}_{=1} + \underbrace{r}_{=1}(s-1) = s \quad \Rightarrow \varphi = id$ ◇

3 Schritt

Sei $\varphi \in Gal(\mathbb{Q}(p), \mathbb{Q}(a_1, a_2))$

Insbesondere $\varphi(a_1) = a_1$ und $\varphi(a_2) = a_2$

$\overset{4.\text{Schritt}}{\Rightarrow} \varphi = id$

$\Rightarrow Gal(\underset{\text{separabel}}{\mathbb{Q}(p)}, \mathbb{Q}(a_1, a_2)) = \{id\}$

$\Rightarrow \mathbb{Q}(p) = \mathbb{Q}(a_1, a_2)$ | □

Korollar

Sei n eine Primzahl, p ein irreduzibles Polynom über $\mathbb{Q}$ vom Grad n, das mindestens zwei verschiedene reelle und mind. eine nicht-reelle Nullstelle hat. Dann ist p nicht auflösbar.

Bsp $p = x^5 - 6x + 3$

$5 \in \mathbb{P} \quad 3 \nmid 1, \; 3 \nmid 0, \; 3 \nmid -6, \; 3 \nmid 3 \quad 3^2 \nmid 3$

$\overset{\text{Eisenstein}}{\Rightarrow}$ p irreduzibel über $\mathbb{Q}$

$p'(x) = 5x^4 - 6$

$p'(x) > 0$ auf $(-\infty, -\sqrt[4]{\frac{6}{5}})$ $\Rightarrow$ p ist streng monoton steigend auf $(-\infty, \sqrt[4]{\frac{6}{5}}]$

$p'(x) < 0$ auf $(-\sqrt[4]{\frac{6}{5}}, \sqrt[4]{\frac{6}{5}})$ $\Rightarrow$ p streng monoton fallend auf $[-\sqrt[4]{\frac{6}{5}}, \sqrt[4]{\frac{6}{5}}]$

$p'(x) > 0$ auf $(\sqrt[4]{\frac{6}{5}}, +\infty)$ $\Rightarrow$ p streng monoton wachsend auf $[\sqrt[4]{\frac{6}{5}}, +\infty)$

also ≤ 3 reelle NSt, also ≥ 1 nicht reelle NSt

$p(0) = 3$, $p(1) = -2$ $\overset{\text{Zwischenwertsatz}}{\Rightarrow}$ $\exists$ NSt $\in (0,1)$

$p(2) = 23$ $\overset{\text{Zwischenwertsatz}}{\Rightarrow}$ $\exists$ NSt $\in (1,2)$

$\Rightarrow$ mind 2 reelle NSt

Korollar $\Rightarrow$ p ist nicht auflösbar

Nachtrag (zu Beweis vorher!?)

$L_K(e^{\frac{2\pi i}{n}})$ $G := Gal(L_K(\underbrace{e^{\frac{2\pi i}{n}}}_{:=\omega}), L_K)$

$\varphi \in G$: $\varphi(\omega) = \omega^r \Rightarrow \varphi(\omega^k) = \omega^{r \cdot k}$

Seien $\varphi_1, \varphi_2 \in G$ $\Rightarrow \exists$ r,s mit $\varphi_1(\omega) = \omega^r$ und $\varphi_2(\omega) = \omega^s$

$(\varphi_1 \circ \varphi_2)(\omega) = \varphi_1(\underbrace{\varphi_2(\omega)}_{=\omega^s}) = \omega^{r \cdot s}$

$(\varphi_2 \circ \varphi_1)(\omega) = \varphi_2(\underbrace{\varphi_1(\omega)}_{=\omega^r}) = \omega^{s \cdot r} = \omega^{r \cdot s} = (\varphi_1 \circ \varphi_2)(\omega)$

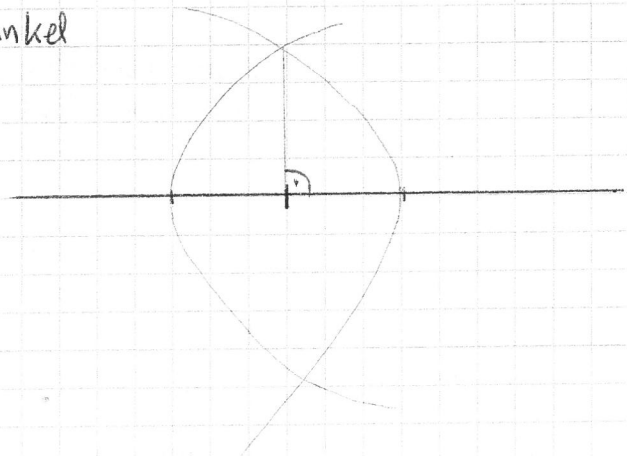
$\Rightarrow \varphi_1 \circ \varphi_2 = \varphi_2 \circ \varphi_1$ $\Rightarrow$ G Abel'sch.

---

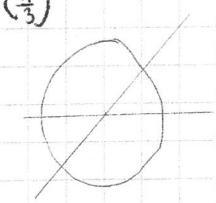
4) Konstruktionen mit Zirkel und Lineal

$\mathbb{R}^2$, Einheitsstrecke $\begin{pmatrix}0\\0\end{pmatrix}$ $\begin{pmatrix}1\\0\end{pmatrix}$

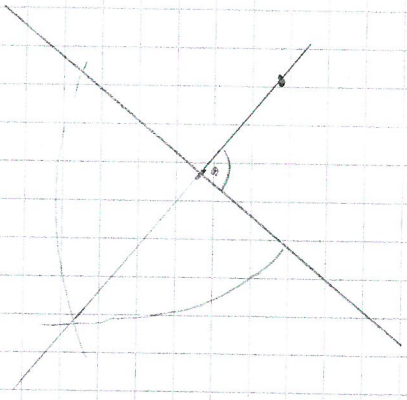
rechte Winkel



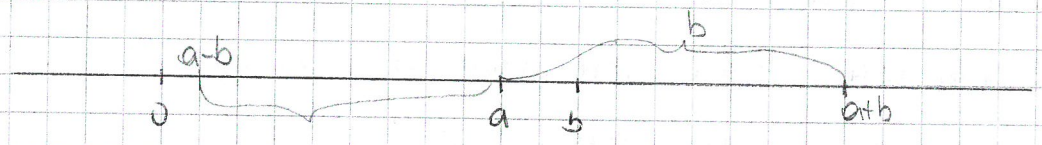
60° ($\frac{\pi}{3}$)



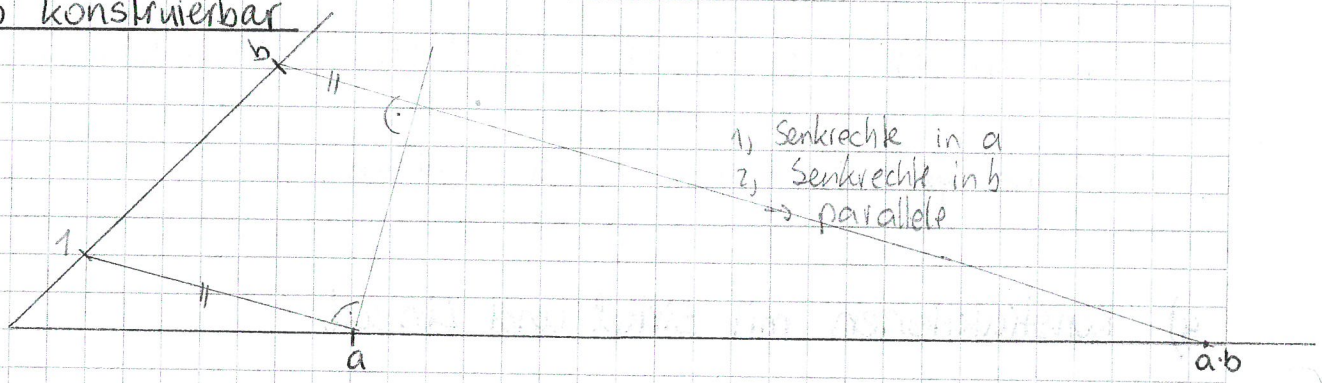
von Punkt senkrechte auf Gerade



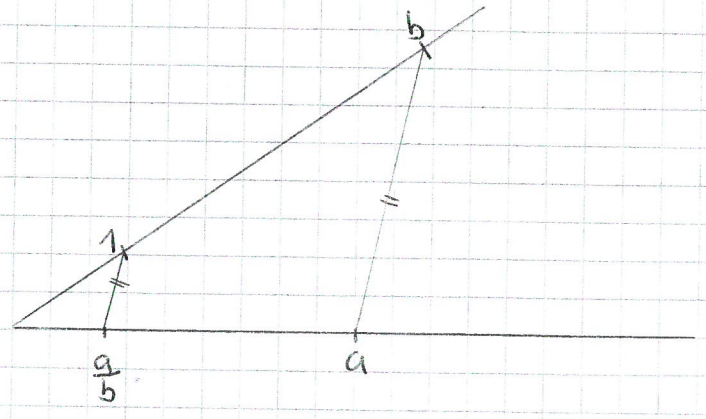
a, b konstruierbar ⇒ a+b, a-b konstruierbar



a·b konstruierbar



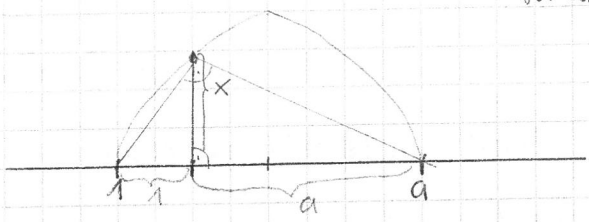
falls b ≠ 0, $\frac{a}{b}$ konstruierbar



b·a verbinden
parallele dazu durch 1

falls a konstruierbar $\Rightarrow$ $\sqrt{a}$ konstruierbar

verwende Höhensatz v. Pythagoras



$x^2 = 1 \cdot a$

$\Rightarrow x = \sqrt{a}$

Menge der konstruierbaren Zahlen ist ein Körper und mit a ist $\sqrt{a}$ konstruierbar.

Alle Zahlen, die sich durch $\mathbb{Q} \subseteq \mathbb{Q}(a_1) \subseteq \mathbb{Q}(a_1, a_2) \subseteq \dots \subseteq \mathbb{Q}(a_1, \dots, a_n)$

(Körpererweiterungen vom grad 2: grad 2, grad 2, grad 2)

mit $x \in \mathbb{Q}(a_1, \dots, a_n)$ sind konstruierbar.

Umkehrung:

dann nur Körpererweiterung vom grad höchstens 2

erlaubt: 2 Geraden, schneiden, Kreis mit Gerade schneiden, 2 Kreise schneiden

1. Fall 2 Geraden schneiden

$a_1 x_1 + a_2 x_2 = b_1$
$c_1 x_1 + c_2 x_2 = d_1$ lin gls bleiben im Körper

keine „echte" Körpererweiterung

2. Fall Gerade mit Kreis

$a_1 x_1 + a_2 x_2 = b_1$
$(x_1 - m_1)^2 + (x_2 - m_2)^2 = r^2$

x_2 durch x_1 ausdrücken und in $(x_2 - m_2)$ einsetzen,

erhalten quadratische Gleichung

$x_1 = -\frac{p}{2} \pm \sqrt{\frac{p^2}{4} - q}$

also Körpererweiterung vom Grad 1 oder 2

3. Fall 2 Kreise schneiden

$$(x_1 - m_1)^2 + (x_2 - m_2)^2 = r^2$$
$$(x_1 - k_1)^2 + (x_2 - k_2)^2 = s^2$$

ausmultiplizieren, Differenz ⇒ lineare Gl., erhalte Gerade

diese muss mit einem der Kreise geschnitten werden

2. Fall ⇒ Körpererweiterung vom Grad 1 oder 2

Satz

Eine Zahl $x \in \mathbb{R}$ ist genau dann konstruierbar, wenn es eine Körperkette (Kette v. Erweiterungen)

$$\underbrace{\mathbb{Q}}_{=K_0} \subseteq \underbrace{\mathbb{Q}(a)}_{=K_1} \subseteq K_2 \subseteq \dots \subseteq K_n \quad \text{mit } \dim_{K_{j-1}} K_j = 2$$

$\forall j \in \{1, 2, \dots, n\}$ mit $x \in K_n$

Beweis siehe oben

Korollar

x konstruierbar ⇒ Grad des Minimalpolynoms von x ist 2^k

Beweis

angen. nicht ⇒ $\exists p \neq 2$ Primzahl mit p | Grad vom Minimalpolynom

$x \in \mathbb{Q} \subset K_1 \subseteq \dots K_n$ ⇒ $p \mid \dim_{\mathbb{Q}} K_n$ ↯ WID □

es gilt sogar ⇔ im Korollar (ohne Beweis, da schwierig)

---

klassische Probleme

Würfelverdoppelung

kann man mit Zirkel und Lineal einen Würfel mit doppeltem Volumen konstruieren?

NEIN

Würfel mit Volumen 2 hätte Seitenlänge $\sqrt[3]{2}$ (Minimalpolynom $x^3 - 2$)

hat Grad 3, 3 ist keine Zweierpotenz $\overset{\text{Korollar}}{\Rightarrow}$ nicht konstruierbar

Quadratur des Kreises

Kann man Zirkel und Lineal zu einem gegebenen Kreis ein flächen gleiches Quadrat konstruieren?

NEIN

Fläche des Einheitskreises $= \pi$ $\Rightarrow$ Seitenlänge des Quadrats müsste $\sqrt{\pi}$ sein, $\sqrt{\pi}$ ist transzendent (nicht Nullstelle eines Polynoms)

$\overset{\text{Korollar}}{\Rightarrow}$ nicht konstruierbar.

Winkeldreiteilung

Kann jeder! Winkel mit Zirkel und Lineal dreigeteilt werden?

NEIN

z.B. $60° = \frac{\pi}{3}$ kann nicht dreigeteilt werden

z.z. $\underbrace{\cos \frac{\pi}{9}}_{:= y}$ nicht konstruierbar

$$\cos(\underbrace{3x}_{=2x+x}) = \underbrace{\cos 2x}_{=\cos^2 x - \sin^2 x} \cdot \cos x - \underbrace{\sin 2x}_{=2 \cdot \sin x \cdot \cos x} \cdot \sin x =$$

$$= \cos^3 x - 3 \cos x \cdot \underbrace{\sin^2 x}_{=1-\cos^2 x} =$$

$$= 4 \cos^3 x - 3 \cos x$$

$$4y^3 - 3y = \underbrace{\cos \frac{\pi}{3}}_{=\frac{1}{2}} \Rightarrow 8y^3 - 6y - 1 = 0$$

$y = z+1$ $\quad 8z^3 + 24z^2 + 18z \ldots\ldots$ error

zeigt: irreduzibel $\overset{\text{Korollar}}{\Rightarrow}$ nicht konstruierbar

$8y^3 - 6y - 1$

$y = z - 1 \Rightarrow 8z^3 - 24z^2 + 18z - 3$

Eisenstein mit 3 $\quad 3 \in P \quad 3 \nmid 8, \; 3 \mid 24, \; 3 \mid 18, \; 3 \mid 3 \quad 3^2 \nmid 3$

$\Rightarrow$ irreduzibel

regelmäßige n-Ecke $n \in \mathbb{P}$

$e^{\frac{2\pi i}{n}}$ konstruier

$n \in \mathbb{P}$ Minimalpolynom: $x^{n-1} + x^{n-2} + \ldots + 1$ grad $n-1$

$\Rightarrow n-1 = 2^k \quad \Rightarrow n = 2^k + 1$ Zahlentheorie, Fermat'sche Primzahlen

$\Rightarrow n = 2^{2^\alpha} + 1$

7-Eck nicht konstruierbar (Minimalpolynom grad 6)

Konstruierbar: 3-Eck

5-Eck ($\alpha = 1$)

17-Eck ($\alpha = 2$)

257-Eck ($\alpha = 3$)

IV Anwendungen

asymetrische Verschlüsselungen
z.B. online-banking

1) RSA-Verfahren

Wählt Primzahlen $p, q \in \mathbb{P}$ $(p \neq q)$ $n = p \cdot q$

wähle c, die $\gcd(c, n) = 1$

wähle $c \cdot d \equiv 1 \pmod{\underbrace{\varphi(n)}_{(p-1)\cdot(q-1)}}$

öffentlicher Schlüssel: (n, c)

mein persönlicher dekodier-Schlüssel: d

Information x: $y = x^c \pmod n$ wird verschickt

ich berechne $y^d = (x^c)^d = x^{cd} = x^{1+s\cdot\varphi(n)} =$

$\gcd(y, n) = 1$

$= x \cdot (\underbrace{x^{\varphi(n)}}_{=1})^s = x$ → dekodiert!

Bsp $p=11,\ q=5$

$n=55 \qquad \varphi(n)=40$

wähle $c=7 \Rightarrow d=23$ $(7\cdot d \equiv 1 \pmod{40})$

Geheimschlüssel

öffentlicher Schlüssel: $(55, 7)$

$x=9$ verschlüsseln: $x^7 \pmod{55}$

$9^2 = 81 = 26 \pmod{55}$

$9^4 = 26^2 = \ldots = 16 \pmod{55}$

$\Big\} 9^6 = 26\cdot 16 = 31$

$9^7 = 9^6 \cdot 9 = 31\cdot 9 = 4 \pmod{55}$ 4 wird mit gesendet

Rechnung siehe oben

Wir berechnen $4^{23} = 9 \pmod{55}$

2) El Gamal Verschlüsselung

$n \in \mathbb{P}$ $\mathbb{Z}_n^*$ zyklisch suche Erzeuger z.B α erzeugt $\mathbb{Z}_n^*$

$a \in \{2, 3, \ldots, n-2\}$

$\beta = \alpha^a$

öffentlicher Schlüssel: (n, α, β)

geheim Schlüssel: a

alle Rechnungen mod n

Information x verschicken: k zufällig in $\{2, \ldots, n-2\}$ gewählt

verschicke $(\alpha^k, x\cdot\beta^k)$ Paar k,a keine Primzahlen

ich berechne: $(x\cdot\beta^k)\cdot \underbrace{(\alpha^k)^{-a}}_{=(\alpha^a)^{-k}=\beta} = x\cdot \underbrace{\beta^k\cdot\beta^{-k}}_{=1} = x$

Bsp $n=29 \qquad \alpha=3, \quad a=11$

$\Rightarrow \beta = 3^{11} = 15 \pmod{29}$

öffentlicher Schlüssel: $(29, 3, 15)$

Geheimschlüssel: 11

Information $x = 9$ verschlüsseln : $k = 5$

$\alpha^5 \cdot x \cdot \beta^5$

$\alpha^5 = 3^5 = 11 \pmod{29}$

$x = 9$

$\beta^5 = 15^5 = 10 \pmod{29}$

$11 \cdot 9 \cdot 10 = 3 \pmod{29}$

wir erhalten : (11, 3)

$\mathbb{Z}_{29}^*$ hat 28 Elemente

$3 \cdot \underbrace{11^{-11}}_{= 11^{17} \pmod{28}} = \ldots = 9 \pmod{28}$

Computer: Passwort darf nicht direkt abgespeichert werden

↳ 30. codiert, codiertes PW gespeichert

dann verglichen (kein Schlüssel notwendig)

! darf an 1. Position eines PW nicht vorkommen