Irreduzibilität von Polynomen

16.01.2015

#9

⓪ Definition

R nullteilerfrei, z.B. $R = \mathbb{Z}$ oder $R = K$. [{für diese R ist R[X] faktoriell, prim = irred.]

Def.: Sei $f \in R[X]$.

f ist irreduzibel in R[X] $\Leftrightarrow$ aus $f = gh$ folgt $g \in R^*$ oder $h \in R^*$

Bsp. 0: $f(X) = aX + b$ ist irred. in $K[X]$.

① Nullstellen-Suche

Lemma: $f(\lambda) = 0$ für ein $\lambda \in K \Leftrightarrow f(X) = \underbrace{(X-\lambda)}_{g(X)} \cdot h(X)$ $\exists\, h \in R[X]$

Kor. 1: $\deg f = 2$ oder 3.

f irreduzibel in $R[X]$ $\Leftrightarrow$ f hat keine Nullstellen in R.

$\deg f \geq 4$: f irred. $\Rightarrow$ "

[„$\Leftarrow$" für $\deg(f) = 2, 3$: f reduzibel $\Rightarrow f = g \cdot h$ mit $\deg g = 1$ oder $\deg h = 1$]

Bsp. 1: $x^2 + 1$ irred in $\mathbb{R}[X]$, aber $x^2 + 1 = (x+i)(x-i)$ in $\mathbb{C}[X]$

$x^2 + 1 = (x+1)^2$ in $\mathbb{Z}_2[X]$.

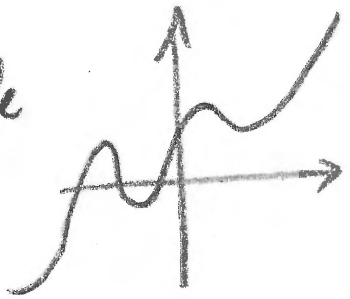
[$x^2 + 1 > 0$ $\forall x \in \mathbb{R}$]

Bsp. 2: $f(X) = x^{2n+1} + a_{2n} x^{2n} + \ldots + a_0 \in \mathbb{R}[X]$ reduzibel, $\forall n \geq 1$

denn $\lim\limits_{x \to -\infty} f(x) = -\infty$

$\lim\limits_{x \to \infty} f(x) = \infty$

[f stetig] ZWS $\Rightarrow$ f hat Nullstelle



Bsp. 3: $f(X) = x^3 - x - 1 \in \mathbb{Z}_3[X]$

$f(\bar{0}) = -1$ $f(\bar{1}) = -1$ $f(\bar{2}) = \bar{8} - \bar{2} - \bar{1} = \bar{5}$

$\Rightarrow f(\bar{m}) \neq 0$ $\forall \bar{m} \in \mathbb{Z}_3$ $\Rightarrow$ f irred

Bem.: • $f \in \mathbb{R}[X]$ mit $\deg f \geq 3 \Rightarrow$ f reduzibel]

[FSA]: • $f \in \mathbb{C}[X]$, $\deg f \geq 1$ $\Rightarrow f(X) = c \cdot \prod_{i=1}^{n} (X - \lambda_i)$ $\exists\, \lambda_1, \ldots, \lambda_n \in \mathbb{C}$. ①

Bsp. 4: $f(x) = x^3 + x^2 - 2x - 1 \in \mathbb{Z}[X]$. Beh.: f reduzibel

$\overset{K1}{\Rightarrow}$ $\exists m \in \mathbb{Z}$ mit $f(m) = 0$ $\Leftrightarrow$ $m(\dots) = 1$

$\| \quad m^3 + m^2 - 2m - 1$

$\Rightarrow m \mid 1 \quad \Rightarrow m \in \{-1, +1\}$

$f(-1) = -1 + 1 + 2 - 1 = 1$

$f(1) = 1 + 1 - 2 - 1 = -1$

$\Rightarrow f(m) \neq 0$ ↯ $\Rightarrow f$ irred.

② Eisenstein-Kriterium und Substitution

Satz [EK]: Sei $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \in \mathbb{Z}[X]$

Falls es Primzahl p gibt

mit $p \nmid a_n$, $p \mid a_i$ $\forall i \in \{1, \dots, n-1\}$, $p \mid a_0$

$p^2 \nmid a_0$

dann ist f irreduzibel (in $\mathbb{Z}[X]$).

Folgerung: Sei $n \in \mathbb{N}$ fest mit $n \geq 2$.

/Bsp. 5: Es gibt ∞-viele irreduzible $f \in \mathbb{Z}[X]$ mit $\deg(f) = n$.

z.B.: $f_m(x) = x^n + 2x + 2 \cdot (2m-1)$ $\Rightarrow f_m$ irred. $\forall m \in \mathbb{Z}$.

$2 \nmid a_n$ $2 \mid a_1$ $2 \mid a_0$, $4 \nmid a_0$

Gauß'Lemma: f irred. in $\mathbb{Z}[X] \Rightarrow f$ irred. in $\mathbb{Q}[X]$

$\|$ $\Leftarrow$ f irred. in $\mathbb{Q}[X]$, $f \in \mathbb{Z}[X]$, $\operatorname{ggT}(a_0, \dots, a_n) = 1$

Bsp.: $f(x) = 15x^2 + 6$ irred. in $\mathbb{Q}[X]$ $\|$ f primitiv

$= 3 \cdot (5x^2 + 2)$ reduzibel in $\mathbb{Z}[X]$

$\notin \mathbb{Z}^*$

Bsp. 6: $f(x) = 5x^3 + 63x^2 + 168 \in \mathbb{Q}[X]$

$3 \nmid 5$ $3 \mid 63$ $3 \mid 168$ $\frac{168}{3} = 56$

$3 \nmid 56 \Rightarrow 9 \nmid 168$ $\Rightarrow f$ irred. in $\mathbb{Z}[X]$ und $\mathbb{Q}[X]$.

Bsp. 7: $f(x) = x^3 - x^2 + x + 1 \in \mathbb{Z}[x]$

[EK] nicht anwendbar

aber Bem.: $\underset{\in R[x]}{f(x)}$ irred. $\Leftrightarrow$ $\underset{\in R[x]}{f(x+1)}$ irred.

[„$\Leftarrow$": Sei: $f(x) = g(x) \cdot h(x) \Rightarrow f(x+1) = g(x+1) \cdot h(x+1)$

$\Rightarrow$ $g(x+1)$ oder $h(x+1) = u$ für ein $u \in R^*$

$\Rightarrow$ $g(x)$ oder $h(x) \in R^*$.]

$\rightsquigarrow f(x+1) = (x+1)^3 - (x+1)^2 + (x+1) + 1$

$= (x+1)^2 [x+1-1] + (x+1) + 1 = x^3 + 2x^2 + 2x + 2$

$2 \nmid 1 \quad 2 | 2 \quad 4 \nmid 2$

$\overset{[EK]}{\Rightarrow} f(x+1)$ irred. $\overset{Bem.}{\Rightarrow} f(x)$ irred.

Bem.: Sei $f(x) = x^2 + 4x + 8 \in \mathbb{Z}[x]$

[EK] nicht anwendbar auf $f(x+d)$ $\forall d \in \mathbb{Z}$!

3) Reduktion modulo p

Satz: $f \in \mathbb{Z}[x] \longrightarrow \mathbb{Z}_p[x]$ ($ggT(a_0, \dots, a_n) = 1$, p prim mit $p \nmid a_n$)

$= a_n x^n + \dots + a_1 x + a_0 \longmapsto \bar{f}(x) = \bar{a}_n x^n + \dots + \bar{a}_1 x + a_0$

$\bar{f}$ irreduzibel in $\mathbb{Z}_p[x]$ $\Rightarrow$ f irred. in $\mathbb{Z}[x]$

[Beweis: Sei $f = gh$ in $\mathbb{Z}[x]$ $\Rightarrow$ $\bar{f} = \bar{g} \cdot \bar{h}$ in $\mathbb{Z}_p[x]$

mit $g(x) = b_k \cdot x^k + \dots$ mit $k, l \geq 1$ $\quad p \nmid a_n = b_k \cdot c_l$

f red. $\nearrow$ $h(x) = c_l \cdot x^l + \dots$ $\quad \Rightarrow p \nmid b_k,\ p \nmid c_l$

$\Rightarrow \deg(\bar{g}), \deg(\bar{h}) \geq 1 \Rightarrow \bar{f}$ red. □]

Bsp. 8: $f(x) = x^2 + 4x + 8 \in \mathbb{Z}[x]$

$\rightsquigarrow \bar{f}(x) = x^2 + x + 2 \in \mathbb{Z}_3[x]$

$\left.\begin{array}{l} \bar{f}(0) = 2 \\ \bar{f}(1) = 4 = 1 \\ \bar{f}(2) = 8 = 2 \end{array}\right\}$ $\bar{f}$ irred. in $\mathbb{Z}_3[x]$ $\Rightarrow$ f irred. in $\mathbb{Z}[x]$

Bsp. 9:

$f(x) = x^3 + 3x^2 + 2x + 2 \in \mathbb{Z}[x]$

$f(x)$ in $\mathbb{Z}_2[x]$: $x^3 + x^2 = x^2(x+1)$ ...

$f(x)$ in $\mathbb{Z}_3[x]$: $x^3 + \bar{2}x + \bar{2} = x^3 - x - 1$ ist irred. nach Bsp. 3.

$\Rightarrow f$ irred.

④ Noch weitere Beispiele.

Bsp. 10: $f(x) = x^4 + x^3 + x^2 + x + 1$ in $\mathbb{Z}[x]$

in $\mathbb{Z}_2[x]$: Ang.: f reduzibel $\Rightarrow f = \bar{g} \cdot \bar{h}$ mit a) $\deg(\bar{g}) = 1, \deg(\bar{h}) =$ oder b) $\deg(\bar{g}) = 2 = \deg(\bar{h})$

Ang a) gilt $\Rightarrow f$ hat Nullstelle in $\mathbb{Z}_2$

$f(\bar{0}) = \bar{1}$ $f(\bar{1}) = \bar{5} = \bar{1}$ ↯

$\Rightarrow$ Fall b): $f = \bar{g} \cdot \bar{h}$ mit $\bar{g}, \bar{h}$ irred. vom Grad 2

$\Rightarrow \bar{g}, \bar{h} \in \{x^2 + x + 1\}$ $\Rightarrow f = (x^2+x+1)^2 = x^4 + x^2 + 1$ ↯

$x^2 + x = x(x+1)$
$x^2 + \quad + \bar{1} = (x+1)^2$
$x^2 = x \cdot x$
} reduzibel in $\mathbb{Z}_2[x]$ $\Rightarrow f$ irreduzibel.

Bsp 11: Zerlege $f(x) = x^5 + x + 1$ in $\mathbb{Z}_2[x]$ Ang.: f reduzibel

- $f(0) = 1 \neq 0$, $f(1) = 1 \neq 0$ $\Rightarrow f(x) = \underbrace{(x^3 + a_2x^2 + a_1x + a_0)}_{g}\ \underbrace{(x^2 + b_1x + b_0)}_{h}$

irred. irred.

$a_0 = 1 \Rightarrow b_1 = b_0 = 1$

$g(x) = x^3 + a_2x^2 + a_1x + 1$ $= x^5 + (a_2 + b_1)x^4 + \ldots$ Bsp. 10.

$g(1) \neq 0 \Rightarrow a_2 \neq a_1 \Rightarrow a_1 = 1, a_2 = 0$ oder $a_2 = 1, a_1 = 0$

$a_2 + a_1$ $\qquad$ $a_2 + b_1 = 0 \Rightarrow a_2 = 1$

$\Rightarrow f(x) = (x^3 + x^2 + 1)(x^2 + x + 1)$

[nachgerechnet]

5) [Schubert (1793) - Kronecker (1882) - Algorithmus]

Sei $f \in \mathbb{Z}[x]$ mit $\deg f = n$.

Wie zerlegt man f in irred. Faktoren?

z.B. [Bsp. 12].

$f(x) = x^5 - x^4 - 2x^3 - 8x^2 + 6x - 1$

Angenommen, $f(x) = g(x) \cdot h(x)$

mit $\deg g \leq \deg h \rightsquigarrow \deg g \leq \left\lfloor \frac{n}{2} \right\rfloor =: k$ $\quad \deg g \leq 2 = k$

Ziel: Finde g.

① Wähle $k+1$ Stellen $m_0, \dots, m_k \in \mathbb{Z}$,

berechne $f(m_i) \; \forall i \in \{0, \dots, k\}$

$f(0) = -1$, $f(1) = -5$, $f(2) = -21$

$\rightsquigarrow f(m_i) = g(m_i) \cdot h(m_i)$

$\Rightarrow g(m_i) \mid f(m_i) =: y_i$

② Berechne alle Teiler d_{ij} von y_i $\Rightarrow g(0) \in \{\pm 1\}$ #2

- das Polynom g vom Grad k $\quad g(1) \in \{\pm 1, \pm 5\}$ #4

ist eindeutig durch $k+1$ Werte bestimmt $\quad g(2) \in \{\pm 1, \pm 3, \pm 7, \pm 21\}$ #8

③ Wähle Teiler $d_{0j}, d_{1j}, \dots, d_{kj}$ von $y_0, y_1, \dots, y_k$ $\Rightarrow 2 \cdot 4 \cdot 8 = 64$ Möglichkeiten

↳ bestimme Polynom g mit $g(m_0) = d_{0j}$; $g(m_k) = d_{kj}$ (viele ... durch Lagrange-Interpolation)

z.B. $g(0) = +1$, $g(1) = -5$, $g(2) = +7$ ...

- Teste ob $g \mid f$ mit Euklid. Algorithmus ... • OBdA $g(0) = +1$ ↝ 32 Möglichkeiten

④ Wiederhole ③ für jede Kombination von Teilern.

bis g ein Faktor von f ist ... $\Rightarrow f(x) = \overbrace{(x^2 - 3x + 1)}^{g(x)} \cdot (x^3 + 2x^2 + 3x - 1)$

Tutorium #10: 23.01.2015

Endlich erzeugte abelsche Gruppen

① Hauptsatz über EEAG

Satz [Frobenius-Stickelberger '1878]:
Sei G endlich erzeugte abelsche Gruppe. Dann gibt es

v1) $r \in \mathbb{N}_0$ und $m_{p,i} \in \mathbb{N}_0$ für p prim, $i \in \mathbb{N}$, so dass

$$G \cong \mathbb{Z}^r \times \overbrace{\prod_{p \text{ prim}} \prod_{i \in \mathbb{N}} (\mathbb{Z}_{p^i})^{m_{p,i}}}^{\mathrm{Tor}(G)} \quad \text{wobei}$$

$\underbrace{\quad\quad}_{\mathrm{Tor}_p(G) =: G_p}$

- r und $m_{p,i}$ eindeutig
- nur endlich viele $m_{p,i} \neq 0$

v2) $r \in \mathbb{N}_0$ und Primzahlpotenzen $q_1, \dots, q_t \in \mathbb{N}^+$ [$q_k = p_k^{i_{p_k}}$ mit p_k prim, $i_{p_k} \in \mathbb{N}$]

s.d. $G \cong \mathbb{Z}^r \times \mathbb{Z}_{q_1} \times \mathbb{Z}_{q_2} \times \dots \times \mathbb{Z}_{q_t}$ wobei

$q_1 \leq q_2 \leq \dots \leq q_t$

- r und $q_1, \dots, q_t$ eindeutig.

$\overline{\mathrm{rk}}(G)$

Bem.: a) $G_1, \dots, G_n$ Gruppen $\Rightarrow \prod_{i=1}^n G_i = \bigoplus_{i=1}^n G_i$ [$n < \infty$].

(b) G ist direkte Summe zyklischer Gruppen)

Anwendung: Bestimme alle abelschen Gruppen G mit $|G| = 360$.

Satz $\Rightarrow$ $r = 0$, $G \cong \prod_{p \text{ prim}} G_p$ $\quad |G_p| = \prod_{i \in \mathbb{N}} (p^i)^{m_{p,i}} = p^{n_p}$ für ein $n_p \in \mathbb{N}_0$.

$|G| < \infty$

$$\Rightarrow |G| = \prod_{p \text{ prim}} p^{n_p}$$

$|G| = 360 = 8 \cdot 9 \cdot 5 = 2^3 \cdot 3^2 \cdot 5 \Rightarrow m_{p,i} = 0 \quad \forall i \in \mathbb{N} \; \forall p \notin \{2,3,5\}$

$n_p = 0 \quad \forall p \notin \{2,3,5\}$

$\Rightarrow G \cong \underbrace{G_2}_{\text{endlich, abelsch}} \times G_3 \times G_5$ mit $|G_2| = 2^3$, $|G_3| = 3^2$, $|G_5| = 5$

$n_2 = 3 = 2+1 = 1+1+1$ $\quad n_3 = 2 = 1+1$ $\quad n_5 = 1$ $\quad \Rightarrow \underbrace{3 \cdot 2 \cdot 1}_{\text{6 mögliche Gruppen}}$

$\Rightarrow G_5 \cong \mathbb{Z}_5$

$G_3 \cong \mathbb{Z}_9$ oder $\mathbb{Z}_3 \times \mathbb{Z}_3$

$G_2 \cong \mathbb{Z}_8$ oder $\mathbb{Z}_2 \times \mathbb{Z}_4$ oder $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$

Bem.: a) $|G|$ beliebig endlich.

b) G abelsch, $|G| = p^k \cdot m < \infty$

$\Rightarrow \mathrm{Tor}_p(G)$ ist p-Sylow-UG

② EEAG via „Lineare Algebra über $\mathbb{Z}$"

ideen.: abelsche Gruppen = „Vektorräume über $\mathbb{Z}$" = $\mathbb{Z}$-Modulen

$(G,+) \rightsquigarrow \mathbb{Z} \times G \longrightarrow G$

$\cdot n \cdot g = \underbrace{(g + \dots + g)}_{n\text{-mal}} \quad \forall n \in \mathbb{N}_0$

$\cdot (-n) \cdot g = n \cdot (-g) \dots$

Aufg. 1:

Sei $\Gamma = \left\langle \begin{pmatrix}6\\7\\5\end{pmatrix}, \begin{pmatrix}8\\11\\7\end{pmatrix}, \begin{pmatrix}-6\\-11\\-5\end{pmatrix} \right\rangle_{\mathbb{Z}} \subset \mathbb{Z}^3$

Zerlege $\mathbb{Z}^3/\Gamma$ in direkte Summe von zyklischen Gruppen.

Ansatz: bringe $A = \begin{pmatrix}6 & 8 & -6\\7 & 11 & -11\\5 & 7 & -5\end{pmatrix}$ durch „ZT oder ST aus $GL_3(\mathbb{Z})$" auf Diagonalform

$m \in \mathbb{Z}$

- $m \cdot$ Zeile i zu Zeile j addieren / Spalte / Spalte $i \neq j$
- $(-1) \cdot$ Zeile i / Spalte i
- vertauschen von Zeilen / Spalten

Idee:

$$\begin{array}{ccccc} \mathbb{Z}^3 & \xrightarrow{A} & \mathbb{Z}^3 & \twoheadrightarrow & \operatorname{coker}(A) = \mathbb{Z}^3/\Gamma \\ \downarrow S\,|\,T & & \downarrow S & & \downarrow S\,|\,[VL] \\ \mathbb{Z}^3 & \dashrightarrow & \mathbb{Z}^3 & \twoheadrightarrow & \operatorname{coker}(SAT^{-1}) \\ & SAT^{-1} & & & \end{array}$$

Bsp.:

$$A = \begin{pmatrix}6 & 8 & -6\\7 & 11 & -11\\5 & 7 & -5\end{pmatrix} \Rightarrow \begin{pmatrix}6 & 2 & 0\\7 & 4 & -4\\5 & 2 & 0\end{pmatrix} \overset{1-2\cdot3}{\Rightarrow} \begin{pmatrix}1 & 0 & 0\\7 & 4 & -4\\5 & 2 & 0\end{pmatrix} \overset{1-7\cdot1}{\underset{1-5\cdot1}{}}$$

$-5\cdot1 \quad +5\cdot1$ (in A)

$+5\cdot3$ (in der letzten Matrix)

$$\Rightarrow \begin{pmatrix}1 & 0 & 0\\0 & 0 & -4\\0 & 2 & 0\end{pmatrix} \overset{\cdot(-1)}{\Rightarrow} \begin{pmatrix}1 & & \\ & 2 & \\ & & -4\end{pmatrix} \overset{\cdot(-1)}{\Rightarrow} \begin{pmatrix}1 & & \\ & 2 & \\ & & 4\end{pmatrix} = SAT^{-1}$$

$$\Rightarrow \mathbb{Z}^3/\Gamma \cong \operatorname{coker}(SAT^{-1}) = \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z} \Big/ \left\langle \begin{pmatrix}1\\0\\0\end{pmatrix}, \begin{pmatrix}0\\2\\0\end{pmatrix}, \begin{pmatrix}0\\0\\4\end{pmatrix} \right\rangle \cong \mathbb{Z}_1 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_4$$

$\mathbb{Z}_1 \cong 0$

$$\cong \mathbb{Z}_2 \oplus \mathbb{Z}_4$$

Aufg. 2

a) $G = \mathbb{Z}_3 / \Gamma$ mit $\Gamma = \left\langle \underbrace{\begin{pmatrix}2\\5\\14\end{pmatrix}}_{v_1}, \underbrace{\begin{pmatrix}3\\9\\24\end{pmatrix}}_{v_2} \right\rangle_{\mathbb{Z}}$

$\bar{g} = \begin{pmatrix}\bar{1}\\\bar{0}\\\bar{2}\end{pmatrix}$. Was ist $\operatorname{ord}(\bar{g})$?

$\operatorname{ord}(\bar{g}) = |\underbrace{\langle \bar{g} \rangle}_{\text{UG in } G}| = \min\{n \in \mathbb{N}^+ \mid \underbrace{(\bar{g} + \bar{g} + \dots + \bar{g})}_{n\text{-mal}} = \bar{0}\}$

$= \min\{n \in \mathbb{N}^+ \mid n \cdot g \in \Gamma\}$

$= \min\{n \in \mathbb{N}^+ \mid \exists m_1, m_2 \in \mathbb{Z}: \underbrace{m_1 v_1 + m_2 v_2 = ng}_{\text{inhom. LGS}}\}$

Ansatz:

finde minimales $n \in \mathbb{N}^+$ so dass $\left(\begin{array}{cc|c}2 & 3 & n\\5 & 9 & 0\\14 & 24 & 2n\end{array}\right)$ lösbar über $\mathbb{Z}$ ist.

$\quad$ "$(A \mid ng)$"

- ST bzgl. $\mathbb{Z}$ sind erlaubt, denn

$$ng \in \langle v_1, v_2 \rangle_{\mathbb{Z}} \Leftrightarrow ng \in \langle \underbrace{v_1, v_2 + m \cdot v_1}_{\text{ST von } A} \rangle_{\mathbb{Z}} = \langle v_1, v_2 \rangle_{\mathbb{Z}}$$

- ZT bzgl. $\mathbb{Z}$ auch erlaubt, denn

$$ng \in \langle v_1, v_2 \rangle_{\mathbb{Z}} \Leftrightarrow \underbrace{S \cdot ng \in \langle S \cdot v_1, S \cdot v_2 \rangle_{\mathbb{Z}}}_{\text{ZT von } (A \mid ng)} \quad \forall S \in Gl_n(\mathbb{Z})$$

$\Rightarrow$ · Vertauschen von Zeilen oder Spalten erlaubt

$$\left(\begin{array}{cc|c}2 & 3 & n\\5 & 9 & 0\\14 & 24 & 2n\end{array}\right) \Rightarrow \left(\begin{array}{cc|c}2 & 1 & n\\5 & 4 & 0\\14 & 10 & 2n\end{array}\right) \Rightarrow \left(\begin{array}{cc|c}0 & 1 & n\\-3 & 4 & 0\\-6 & 10 & 2n\end{array}\right)_{|-2 \cdot 2}$$

$-S2$ $\quad$ $-2 \cdot S1$

$$\Rightarrow \left(\begin{array}{cc|c}0 & 1 & n\\-3 & 4 & 0\\0 & 2 & 2n\end{array}\right) \Rightarrow \begin{array}{c} m_2 = n \\ -3m_1 + 4m_2 = 0 \Leftrightarrow +3m_1 = 4n \\ 2m_2 = 2n \end{array}$$

$\Rightarrow (A \mid ng)$ lösbar für $n \in 3\mathbb{Z} \Rightarrow \operatorname{ord}(\bar{g}) = 3$.

b)

$G = \mathbb{Z}^3/\Gamma \qquad \Gamma = \langle \underbrace{\begin{pmatrix}2\\1\\-50\end{pmatrix}}_{v_1}, \underbrace{\begin{pmatrix}4\\5\\60\end{pmatrix}}_{v_2} \rangle$

$\bar{g} = \begin{pmatrix}32\\31\\0\end{pmatrix} \qquad \text{ord}(\bar{g})?$

$$\rightsquigarrow \left(\begin{array}{cc|c}2 & 4 & 32n\\1 & 5 & 31n\\-50 & 60 & 0\end{array}\right) \Rightarrow \left(\begin{array}{cc|c}1 & -1 & n\\1 & 5 & 31n\\-50 & 60 & 0\end{array}\right) \; 1-Z1$$

$$\Rightarrow \left(\begin{array}{cc|c}1 & -1 & n\\0 & 6 & 30n\\-50 & 60 & 0\end{array}\right)_{1+50Z1} \Rightarrow \left(\begin{array}{cc|c}1 & -1 & n\\0 & 6 & 30n\\0 & 10 & 50n\end{array}\right) \Rightarrow \begin{array}{l} m_1 - m_2 = n \\ m_2 = 5n \end{array}$$

$$\Rightarrow m_1 = 6n$$

$\Rightarrow$ lösbar $\forall n \in \mathbb{N}^+ \Rightarrow \text{ord}(\bar{g}) = 1 \Leftrightarrow g \in \Gamma$

$[6v_1 + 5v_2 = g]$

c)

$G = \mathbb{Z}^3/\Gamma \qquad \Gamma = \langle \begin{pmatrix}2\\6\\-2\end{pmatrix}, \begin{pmatrix}2\\8\\-4\end{pmatrix}, \begin{pmatrix}6\\20\\-8\end{pmatrix} \rangle_{\mathbb{Z}}$

$\bar{g} = \begin{pmatrix}2\\7\\-1\end{pmatrix} \qquad \text{ord}(\bar{g})?$

$$\rightsquigarrow \left(\begin{array}{ccc|c}2 & 2 & 6 & 2n\\6 & 8 & 20 & 7n\\-2 & -4 & -8 & -1n\end{array}\right)_{1-3Z1} \Rightarrow \left(\begin{array}{ccc|c}2 & 2 & 6 & 2n\\0 & 2 & 2 & n\\0 & -2 & -2 & n\end{array}\right)_{1+Z1} \Rightarrow \begin{array}{l} 2m_2 + 2m_3 = n \\ -2m_2 - 2m_3 = n \end{array}$$

$\Rightarrow m_2 = m_3 = 0 = n \qquad \rightsquigarrow$ was ist also $\text{ord}(\bar{g})$?

$n \cdot \bar{g} \neq \bar{0} \; \forall n \in \mathbb{N}^+ \Leftrightarrow \langle \bar{g} \rangle \cong \mathbb{Z}$

$$\left(\begin{array}{ccc}2 & 2 & 6\\0 & 2 & 2\\0 & -2 & -2\end{array}\right)_{1+Z2} \Rightarrow \left(\begin{array}{ccc}2 & 0 & 0\\0 & 2 & 2\\0 & 0 & 0\end{array}\right) \Rightarrow \begin{pmatrix}2 & & \\ & 2 & \\ & & 0\end{pmatrix}$$

$-S1 \quad -3S1 \qquad\qquad -S2$

$\Rightarrow \mathbb{Z}^3/\Gamma \cong \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z} / \langle \begin{pmatrix}2\\0\\0\end{pmatrix}, \begin{pmatrix}0\\2\\0\end{pmatrix} \rangle \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \underbrace{\mathbb{Z}_0}_{\mathbb{Z} \cong \langle \begin{pmatrix}0\\7\\1\end{pmatrix} \rangle}$

3)

Aufg. 3: $G = \mathbb{Z}_4 \oplus \mathbb{Z}_8$ Zerlege G/H.

$H = \langle(\bar{2},\bar{4})\rangle = \{(\bar{2},\bar{4}), (\bar{2},\bar{4})+(\bar{2},\bar{4}) = (\bar{0},\bar{0})\}$

- $|H| = 2$, $|G| = 32 \Rightarrow |G/H| = 16$.

Hauptsatz $\Rightarrow G/H \cong \begin{cases} \mathbb{Z}_{16} & \mathbb{Z}_4 \times \mathbb{Z}_4 \\ \mathbb{Z}_8 \times \mathbb{Z}_2 & \mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2, \text{ oder} \\ & \underbrace{\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2}_{\text{haben kein Element der Ordnung 8.}} \end{cases}$

Ansatz: Untersuche $\text{ord}(\bar{g})$ für bestimmte $\bar{g} \in G/H$

Lemma: a) $\varphi : (G_1,+) \to (G_2,+)$ Gruppen-Hom. $\Rightarrow \text{ord}(\varphi(g)) \leq \text{ord}(g)$ $\forall g \in G_1$

[sei $\text{ord}(g) = n \Rightarrow n \cdot \varphi(g) = \varphi(n \cdot g) = \varphi(e) = e$]

b) φ isom. $\Rightarrow \text{ord}(\varphi(g)) = \text{ord}(g)$ $\forall g \in G_1$

[$G \xrightarrow{\varphi}_{\sim} G \xrightarrow{\varphi^{-1}}_{\sim} G$ $\text{ord}(g) = \text{ord}(\varphi^{-1}(\varphi(g))) \leq \text{ord}(\varphi(g)) \leq \text{ord}(g)$]

c) $g \in \mathbb{Z}_{q_1} \times \mathbb{Z}_{q_2} \times \ldots \times \mathbb{Z}_{q_4} \Rightarrow \text{ord}(g) \leq \text{kgV}(q_1,\ldots,q_4) =: q$

[$q \cdot g = (qg_1, qg_2, \ldots, qg_4)$ $q_k \mid q \Rightarrow q_k \mid q g_k$ $\forall k \in \{1,\ldots,4\}$

$\Rightarrow q \cdot g = (0,\ldots,0)$]

Anwendung:

- $G \twoheadrightarrow G/H \ni \bar{g}$ $\overset{a)}{\Rightarrow}$ $\text{ord}(\bar{g}) \leq 8 = \max\{\text{ord}(g) \mid g \in \underbrace{\mathbb{Z}_4 \oplus \mathbb{Z}_8}_{G}\}$

$\overset{b)}{\Rightarrow}$ $G/H \not\cong \mathbb{Z}_{16}$

- Betrachte $\bar{g} = (\bar{0},\bar{1}) \in G/H \Rightarrow \langle\bar{g}\rangle = \{(\bar{0},\bar{m}) \mid m \in \mathbb{Z}_8\}$ $\not\ni H$

$\Rightarrow \text{ord}(\bar{g}) = 8 \overset{b)}{\Rightarrow} G/H \cong \mathbb{Z}_8 \times \mathbb{Z}_2$ □

Tutorium #10: 30.10.2015

Algebraische Körpererweiterungen

① Adjunktion einer Nullstelle

Bsp.: $g(x) = x^4 - 4$ hat keine Nullstelle in $\mathbb{Q}$

Ziel: Beschreibe „kleinsten" Körper der $\mathbb{Q}$ und $\sqrt{2}$ enthält.

Seien $K \subset L$ Körper,
sei $a \in L$ algebraisch
(d.h. $\exists\, g \in K[X] \setminus \{0\} : g(a) = 0$)

Betrachte

$$\begin{array}{ccc} K[X] & \xrightarrow{ev_a} & L \\ \cup & & \\ p(X) & \longmapsto & p(a) \end{array}$$

$$0 \neq \ker(ev_a) = (f)$$

Bsp:
$\mathbb{Q} \subset \mathbb{R}$
$\sqrt{2} \in \mathbb{R}$
$(g(x) = x^4 - 4)$

$$\begin{array}{ccc} \mathbb{Q}[X] & \xrightarrow{ev_{\sqrt{2}}} & \mathbb{R} \\ \cup & & \\ p(X) & \longmapsto & p(\sqrt{2}) \end{array}$$

$$\ker(ev_{\sqrt{2}}) = (x^2 - 2)$$

Def. 1: Sei $f \in K[X]$. f ist Minimal-Polynom von a (über K) $\quad [f \neq 0]$.

$\Leftrightarrow$ $\begin{cases} \cdot\,(f) = \ker(ev_a) \\ \cdot\, f \text{ ist normiert, d.h. } f(X) = \sum_{j=0}^{n} c_n X^n \text{ mit } c_n = 1. \end{cases}$

Bem. 1: $a \in L$ alg. über $K \Rightarrow \exists!$ Min.-Polynom m_a, wobei $m_a \neq 0$.
$(m_a) = \ker ev_a \neq 0$

[Char. von Min.-Polynom]

Satz 1: Sei $f \in K[X]$. $[f \neq 0]$.

(i) f ist Min. Polynom von a
$\Leftrightarrow$ (ii) f ist normiertes Polynom kleinsten Grades mit $f(a) = 0$
$\Leftrightarrow$ (iii) f ist normiertes, irreduzibles Polynom mit $f(a) = 0$.

Beweis: (i) $\Rightarrow$ (ii): $f = m_a$. [siehe Bsp.]

Sei g normiert mit $g(a) = 0 \Rightarrow g \in \ker(ev_a) = (f)$

$\Rightarrow \exists\, h \in K[X]: g = h \cdot f$ und $\deg(g) = \deg(h) + \deg(f)$

$\Rightarrow \deg(g) \geq \deg(f)$

ii) $\Rightarrow$ iii): Sei f wie in ii). Beh.: f irred.

$f = g \cdot h \Rightarrow f(a) = 0 = g(a)\,h(a)$

OBdA $g(a) = 0$. Sei $g(x) = c_m \cdot x^m + \dots$

$\Rightarrow \deg(g) = \deg(\underbrace{\frac{1}{c_m} \cdot g}_{\tilde{g}}) \leq \deg(f)$, $\tilde{g}(a) = 0$, $\tilde{g}$ normiert

$\overset{ii)}{\Rightarrow} \deg(f) = \deg(\tilde{g}) = \deg(g)$

$\Rightarrow \deg(h) = 0 \overset{(h \neq 0)}{\Leftrightarrow} f$ irred*

iii) $\Rightarrow$ (i): f irred.... $f(a) = 0 \Rightarrow f \in \ker ev \overset{\text{Bem. 1}}{=} \underbrace{(m_a)}_{*\text{ Min. Pol.}}$

$\Rightarrow \exists h \in K[x]: f = h \cdot m_a \Rightarrow \deg(h) = 0$ ($\deg(m_a) \geq 1$)

f, h normiert $\Rightarrow h(x) = 1 \Rightarrow f = m_a$. $\square$

Def. 2:

i) $K[a] := \operatorname{im} ev_a = \{ \sum_{j=0}^{n} c_j a^j \mid c_j \in K \} = \{ f(a) \mid f \in K[x] \}$

Bem.: $K[x]/\ker ev_a \cong \operatorname{im} ev_a$ Bsp.: $\mathbb{Q}[x]/(x^2-2) \cong \mathbb{Q}[\sqrt{2}]$

$\| \qquad \|$

$K[x]/(m_a) \cong K[a]$ ein Ring mit $K \subset K[a] \subset L$

Def. 2 ii) $K(a) := Q(K[a]) =$ Quot.-Körper von $K[a]$

$[= \{ \frac{f(a)}{g(a)} \mid f, g \in K[x], g(a) \neq 0 \}]$

Bem.: $K[a] =$ „kleinster" Ring der K und a enthält

$K(a) =$ " Körper "

Satz 2: $a \in L$ algebraisch $\Rightarrow$ $\boxed{K[a] = K(a) \text{ ein Körper}}$ Bsp.: $\mathbb{Q}[\sqrt{2}] = \mathbb{Q}(\sqrt{2})$

Def. 3: $K \subset E$ Körper. $[E:K] := \dim_K E =$ Grad von E über K

Satz 3: $[K(a) : K] = \dim_K K[x]/(m_a) = \deg(m_a)$

Bsp.: $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ $\mathbb{Q}(\sqrt{2}) = \langle 1, \sqrt{2} \rangle_{\mathbb{Q}}$. $\mathbb{Q}[x]/(x^4+16) \| \mathbb{Q}(\sqrt{2}+\sqrt{2}i)$

Bem.: $\mathbb{Q}[x]/(x^4-4) \not\cong \mathbb{Q}(\underbrace{\sqrt{2}, \sqrt{2}i}_{\text{Nullstellen von } x^2-4}) \cong \mathbb{Q}(\sqrt{2})[x]/(x^2+2)$

② Aufg. 1:

i) Beh.: $\underbrace{\mathbb{Q}(\sqrt[5]{3}, \sqrt{7})}_{L} = \mathbb{Q}(\underbrace{\sqrt[5]{3} \cdot \sqrt{7}}_{a})$

„$\supseteq$": ✓

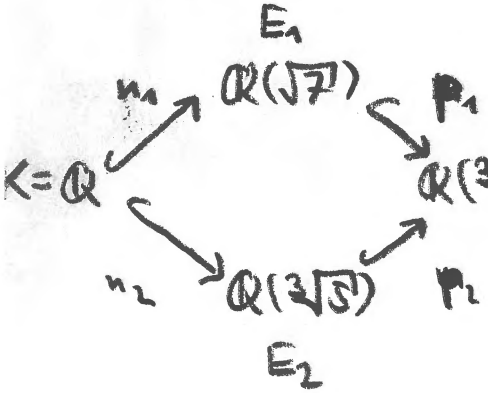
„$\subseteq$": Beh.: $\sqrt[5]{3}$ und $\sqrt{7} \in \mathbb{Q}(a)$.

$a^5 = 3 \cdot \sqrt{7} \cdot 7^2 \Rightarrow \sqrt{7} = \frac{1}{3 \cdot 7^2} a^5 \in \mathbb{Q}(a)$

$\Rightarrow \frac{1}{\sqrt{7}} \in \mathbb{Q}(a) \Rightarrow \sqrt[5]{3} = \frac{1}{\sqrt{7}} \cdot a \in \mathbb{Q}(a)$.

ii) bestimme $[L : \mathbb{Q}]$.

Gradsatz: $K \subset E \subset L$ Körper $\Rightarrow [L:K] = [L:E] \cdot [E:K]$.



$\Rightarrow [L:\mathbb{Q}] \overset{?}{=} [L:\mathbb{Q}(\sqrt{7})]_{P_1} \cdot [\mathbb{Q}(\sqrt{7}):\mathbb{Q}]_{n_1}$

$= [L:\mathbb{Q}(\sqrt[3]{5})]_{P_2} \cdot [\mathbb{Q}(\sqrt[3]{5}):\mathbb{Q}]_{n_2}$

$\cdot n_1 = \deg(\underbrace{m_{\sqrt{7}}(x)}_{\in})$

$x^2 - 7$ ist irred. über $\mathbb{Q}[x]$

$\Rightarrow$ Min. Pol. $\Rightarrow n_1 = 2$

$\cdot n_2 = \deg(m_{\sqrt[3]{5}}(x)) \quad m_{\sqrt[3]{5}}(x) = x^5 - 3$ irred.

$= 5 \qquad \in \mathbb{Q}[x]$

$\Rightarrow 2 | q \,,\, 5 | q \Rightarrow 10 | q$

$\cdot P_2 = \deg(\tilde{m}_{\sqrt{7}}(x))$ wobei $\tilde{m}_{\sqrt{7}}(x) \in \mathbb{Q}(\sqrt[3]{5})[x]$.

$\Rightarrow P_2 \leq \deg((x^2 - 7)) = 2$ [denn $x^2 - 7 \in (\tilde{m}_{\sqrt{7}})$]

analog: $P_1 \leq 5 \Rightarrow q \leq 10 \Rightarrow q = 10$.

iii) bestimme Min.-Polynom von a über $\mathbb{Q}$

$\rightsquigarrow$ suche $f \in \mathbb{Q}[x]$ mit $\deg f = 10$ so dass $f(a) = a^{10} + \sum_{j=0}^{9} c_j a^j = 0$ [nach Satz 1 (ii)]

$\rightsquigarrow$ betrachte $a^j \rightsquigarrow \begin{matrix} a^5 = 3 \cdot 7^2 \cdot \sqrt{7} \\ \vdots \\ a^{10} = 3^2 7^5 \end{matrix} \Rightarrow m_a(x) = f(x) = x^{10} - 3^2 \cdot 7^5$

Aufg. 3: Erweiterung eines endlichen Körpers.

Sei p prim, $K = \mathbb{F}_p$, $n \in \mathbb{F}_p$.

$$L_n := \left\{ \begin{pmatrix} a & nb \\ b & a \end{pmatrix} \mid a, b \in \mathbb{F}_p \right\} \subset \mathrm{Mat}_{2\times 2}(\mathbb{F}_p) =: \mathcal{M}$$

Beh.: L_n ein Körper $\Leftrightarrow$ n kein Quadrat, d.h. $n \neq c^2 \ \forall c \in \mathbb{F}_p$.

✓1) „konkret":

- $M_1, M_2 \Rightarrow M_1 + M_2 \in L_n$

$$M_1 \cdot M_2 = \begin{pmatrix} a_1 & nb_1 \\ b_1 & a_1 \end{pmatrix}\begin{pmatrix} a_2 & nb_2 \\ b_2 & a_2 \end{pmatrix} = \begin{pmatrix} a_1a_2 + nb_1b_2 & n(b_1a_2 + a_1b_2) \\ b_1a_2 + a_1b_2 & a_1a_2 + nb_1b_2 \end{pmatrix}$$

$\Rightarrow M_1 \cdot M_2 \in L_n$ $\quad M_1 \cdot M_2 = M_2 \cdot M_1$.

$\Rightarrow L_n$ kommut. UR von $\mathrm{Mat}_{2\times 2}(\mathbb{F}_p)$.

- sei $M = \begin{pmatrix} a & nb \\ b & a \end{pmatrix} \in L_n$

$\exists M^{-1} \Leftrightarrow \det(M) = a^2 - nb^2 \neq 0$

L_n ein Körper $\Leftrightarrow \forall M \in L_n \setminus \{0\} \ \exists M^{-1} \in \Leftrightarrow n \neq \underbrace{\frac{b^2}{a^2}}_{c^2} \ \forall a, b \in \mathbb{F}_p$

[$M \in L_n$ mit $a = 0$: $\exists M^{-1}$.

ist $M^{-1} \in L_n$? $\quad M^{-1} = \begin{pmatrix} a & -nb \\ -b & b \end{pmatrix} \frac{1}{\det(M)} \in L_n$ ✓

✓2) „abstrakt":

$$K = \mathbb{F}_p \hookrightarrow L_n = \left\langle \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \underbrace{\begin{pmatrix} 0 & n \\ 1 & 0 \end{pmatrix}}_{\gamma} \right\rangle_{\mathbb{F}_p} = \left\{ a \cdot \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + b \cdot \begin{pmatrix} 0 & n \\ 1 & 0 \end{pmatrix} \mid a, b \in \mathbb{F}_p \right\}$$

$$q \longmapsto \begin{pmatrix} q & 0 \\ 0 & q \end{pmatrix} = q \cdot \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$\dim_{\mathbb{F}_p} L_n = 2$.

- $\gamma^2 = \begin{pmatrix} 0 & n \\ 1 & 0 \end{pmatrix}^2 = \begin{pmatrix} n & 0 \\ 0 & n \end{pmatrix} = n \cdot \mathbb{1} \Rightarrow$ Ring-Isom. $\mathbb{F}_p[X]/(X^2 - n) \xrightarrow{\sim} L_n$

$$a \cdot 1 + bX \longmapsto a \cdot \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + b \cdot \begin{pmatrix} 0 & n \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} a & nb \\ b & a \end{pmatrix}$$

- $\mathbb{F}_p[X]/(X^2 - n)$ ein Körper $\Leftrightarrow f(X) = X^2 - n$ irred. $\Leftrightarrow f(x) \neq 0 \ \forall x \in \mathbb{F}_p$

$\cong L_n$

$\Leftrightarrow n \neq x^2 \ \forall x \in \mathbb{F}_p$.

⑤ Min. Polynom via lineare Algebra

Aufg.: Bestimme Min. Polynom von $a = \sqrt{5} - \sqrt{3}$ über $\mathbb{Q}$.

i) Abschätzung von $[\mathbb{Q}(a):\mathbb{Q}]$

$\mathbb{Q} \subset \mathbb{Q}(\sqrt{5}+\sqrt{3}) \subset \mathbb{Q}(\sqrt{5},\sqrt{3}) \Rightarrow [\mathbb{Q}(a):\mathbb{Q}] \le [\mathbb{Q}(\sqrt{5},\sqrt{3}):\mathbb{Q}]$

$[\mathbb{Q}(\sqrt{5},\sqrt{3}):\mathbb{Q}] = [\mathbb{Q}(\sqrt{5},\sqrt{3}):\mathbb{Q}(\sqrt{3})] \cdot \underbrace{[\mathbb{Q}(\sqrt{3}):\mathbb{Q}]}_{=2 \text{ wegen } x^2-3 \in \mathbb{Q}[x]} \le 4$

$\| \qquad \le 2$ wegen $x^2-5 \in \mathbb{Q}(\sqrt{3})[x]$

$\dim_{\mathbb{Q}} \mathbb{Q}(\sqrt{5},\sqrt{3})$

$\mathbb{Q}(\sqrt{5},\sqrt{3}) = \langle \underbrace{1, \sqrt{3}, \sqrt{5}, \sqrt{15}}_{\text{lin. unabh.}} \rangle_{\mathbb{Q}} =: V \Rightarrow [\mathbb{Q}(\sqrt{5},\sqrt{3}):\mathbb{Q}] = 4.$

ii) $[\mathbb{Q}(a):\mathbb{Q}] = \deg m_a \le 4$ [o.B.d.A. $\sqrt{5} \notin \mathbb{Q}(\sqrt{3})$ (*)]

$\rightsquigarrow$ suche $f(X) = \sum_{j=0}^{4} c_j X^j$ mit $f(a) = 0$ (und $c_j \in \mathbb{Q}$)

$$0 = f(a) = c_0 + c_1 \underbrace{a}_{(\sqrt{5}-\sqrt{3})} + c_2 \underbrace{(8 - 2\sqrt{15})}_{a^2} + c_3 \underbrace{(-18\sqrt{3} + 14\sqrt{5})}_{a^3} + c_4 \underbrace{(124 - 32\sqrt{15})}_{a^4}$$

{ eine Gleichung in V"

$$= (c_0 + 8c_2 + 124c_4) \cdot 1 + (-c_1 - 18c_3)\sqrt{3} + (c_1 + 14c_3)\cdot\sqrt{5} + (-2c_2 - 32c_4)\sqrt{15}$$

$\rightsquigarrow$

$$\begin{array}{c} 1 \\ \sqrt{3} \\ \sqrt{5} \\ \sqrt{15} \end{array} \begin{pmatrix} 1 & 0 & 8 & 0 & 124 \\ 0 & -1 & 0 & -18 & 0 \\ 0 & 1 & 0 & 14 & 0 \\ 0 & 0 & -2 & 0 & -32 \end{pmatrix} \begin{pmatrix} c_0 \\ c_1 \\ c_2 \\ c_3 \\ c_4 \end{pmatrix} = 0$$

$\downarrow$

$$\begin{pmatrix} 1 & 0 & 0 & 0 & -4 \\ 0 & 0 & 0 & 4 & 0 \\ 0 & 1 & 0 & 14 & 0 \\ 0 & 0 & 1 & 0 & 16 \end{pmatrix} \Rightarrow \begin{aligned} c_0 &= 4c_4 \\ c_1 &= c_3 = 0 \\ c_2 &= -16c_4 \end{aligned}$$

falls $\deg f \le 3$

$\Rightarrow c_4 = 0$

$\Rightarrow f = 0$ ↯

$\Rightarrow c_4 = 1 \Rightarrow f(X) = X^4 - 16X^2 + 4 = m_a(X).$

iii) Bestimme a^{-1} in $\mathbb{Q}(a)$. $a^4 - 16a^2 + 4 = 0 \quad | \cdot a^{-1} \; | -4a^{-1} \; | \cdot -\frac{1}{4}$

[Berechnung von a^{-1} in $\mathbb{Q}[a]$]

$\Rightarrow \frac{1}{2} a^{-1} = \frac{1}{4} a^3 - \frac{1}{4} a^3$

(*) Ang.: $\sqrt{5} = a + \sqrt{3}b$ mit $a,b \in \mathbb{Q}$

$\Rightarrow 5 = (a^2 + 3b^2) + \sqrt{3}(2ab)$

$\Rightarrow a = 0 \vee b = 0$

$\Rightarrow 5 = a^2$ oder $\frac{5}{3} = b^2$ ↯

Zusatzaufgaben

c) Min. Polynom von $\underbrace{1+\sqrt{2}}_{a}$ über $\mathbb{Q}(\sqrt{2}+\sqrt{3})$?

· [VL]: $\mathbb{Q}(\sqrt{2}+\sqrt{3}) = \mathbb{Q}(\sqrt{2},\sqrt{3})$

$\Rightarrow 1+\sqrt{2} \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$! $\Rightarrow m_{1+\sqrt{2}}(x) = x - c_0$

mit $c_0 \in \mathbb{Q}(\underbrace{\sqrt{2}+\sqrt{3}}_{\gamma})$

Was ist c_0?

$\gamma = \sqrt{2}+\sqrt{3}$

$\gamma^2 = 5 + 2\cdot\sqrt{6}$

$\gamma^3 = 11\sqrt{2} + 9\sqrt{3} \quad \Rightarrow \gamma^3 - 9\gamma = 2\sqrt{2}$

$\Rightarrow \underbrace{\frac{\gamma^3 - 9\gamma}{2} + 1}_{c_0} = \sqrt{2} + 1$

ii) Min. Polynom von $\underbrace{\sqrt{2}+\sqrt{5}}_{a}$ über $\mathbb{Q}(\underbrace{\sqrt{2}+\sqrt{3}}_{\gamma})$?

Beh.: · $[\mathbb{Q}(a) : \mathbb{Q}(\gamma)] \neq 1 \Leftrightarrow a \notin \mathbb{Q}(\sqrt{2}+\sqrt{3}) = \mathbb{Q}(\sqrt{2},\sqrt{3})$

$\mathbb{Q} \subset \mathbb{Q}(\sqrt{2})$

$\Leftrightarrow \sqrt{5} \notin \mathbb{Q}(\sqrt{2},\sqrt{3}) = \langle 1, \sqrt{2}, \sqrt{3}, \sqrt{6} \rangle_{\mathbb{Q}}$

Ang.: $\sqrt{5} = a + \sqrt{2}b + \sqrt{3}c + \sqrt{6}d$ mit $a,b,c,d \in \mathbb{Q}$

$\Rightarrow 5 = (a^2+2b^2+3c^2+6d^2) + \sqrt{2}(2ab+6cd) + \sqrt{3}(4bd+2ac) + \sqrt{6}(2bc+2ad)$

$\Rightarrow d=0 \Rightarrow \begin{matrix} a \vee b = 0 \\ b \vee c = 0 \\ a \vee c = 0 \end{matrix} \Rightarrow \begin{matrix} 5 = 3c^2 \text{ oder} \\ 5 = a^2 \text{ oder} \\ 5 = 2b^2 \end{matrix}$ ↯.

· $a = \sqrt{2}+\sqrt{5}$

$a^2 = 7 + 2\sqrt{10} = 7 + 2\cdot\underbrace{\sqrt{2}\cdot\sqrt{5}}_{\in \mathbb{Q}(\sqrt{2}+\sqrt{3})}$ $\Rightarrow a^2 - 2\sqrt{2}a = 7 - 4 = 3$

$\Rightarrow m_{\sqrt{2}+\sqrt{5}}(x) = x^2 - \underbrace{2\cdot\frac{\gamma^3-9\gamma}{2}}_{=\gamma^3-9\gamma \in \mathbb{Q}(\gamma)} \cdot x - 3 \in \mathbb{Q}(\gamma)[x]$

Tutorium #11: 06.02.2014

Algebraische Körpererweiterungen II: Konstruierbare Zahlen und endliche Körper

1 Algebraische Elemente

Def.: $K \subset L$ Körper, $a \in L$.

a algebraisch über $K \Leftrightarrow \exists p \in K[X]: p(a) = 0$

$\Leftrightarrow \exists c_0, \dots, c_n \in K: c_n \cdot a^n + c_{n-1} \cdot a^{n-1} + \dots + c_1 a + c_0 = 0$

Satz 1: $K \subset L$, $\underbrace{a, b \in L}_{\text{alg. über } K} \Rightarrow a+b,\ a^{-1},\ a \cdot b,\ -a$ alg. über K

Cor.: $\overline{\mathbb{Q}} := \{a \in \mathbb{C} \mid a \text{ alg. über } \mathbb{Q}\}$ ist ein Körper.
„algebraische Zahlen".

Lemma 1: $K \subset \mathbb{C}$, so dass $\forall c \in K: \bar{c} \in K$. Sei $z \in \mathbb{C}$.

z ist algebraisch über $K \Leftrightarrow$ $Re(z)$ und $Im(z)$ algebraisch über K

Beweis: „$\Leftarrow$": Seien $Re(z)$, $Im(z)$ alg.
$\overset{(S1)}{\Rightarrow} i \cdot Im(z)$ alg.
$i \in \mathbb{C}$ alg. über K: $x^2 + 1 \in K[X]$
$\Rightarrow \underbrace{Re(z) + i\, Im(z)}_{z}$ alg.

„$\Rightarrow$": Sei z alg. Beh.: $\bar{z}$ alg.

z alg. $\Leftrightarrow \exists c_0, \dots, c_n \in K: c_n z^n + \dots + c_1 z + c_0 = 0$ | konjugieren

$\Rightarrow \bar{c}_n \bar{z}^n + \dots + \bar{c}_1 \bar{z} + \bar{c}_0 = 0$

$\Rightarrow p(\bar{z}) = 0$ für $p(X) = \bar{c}_n X^n + \dots + \bar{c}_1 X + \bar{c}_0 \in K[X]$

$\Rightarrow \bar{z}$ alg.

$\Rightarrow \underbrace{\frac{z+\bar{z}}{2}}_{Re(z)}$ und $\underbrace{\frac{z-\bar{z}}{2i}}_{Im(z)}$ alg. über K

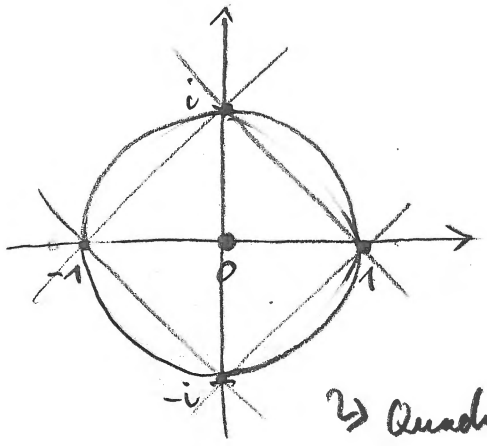
Bem.: $K \subset \mathbb{C}$. $K \subset \mathbb{R}$ oder $i \in K \Leftrightarrow \forall c \in K: \bar{c} \in K$.

② Konstruierbare Zahlen

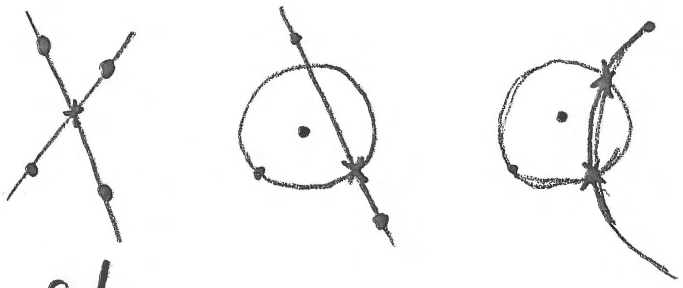
. fasse $\mathbb{C}$ als Ebene auf!

$\vee$

$\mathbb{K}$:= Punkte in $\mathbb{C}$, die mit Zirkel und Lineal aus 0 und 1 konstruierbar sind.



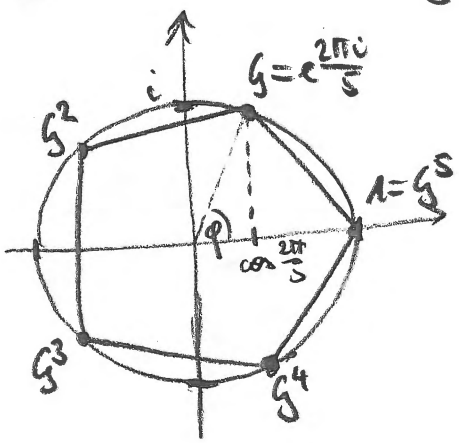
$\rightsquigarrow$ Quadrat konstruierbar



Satz:
$\mathbb{K}$ ist ein Körper mit

- $\mathbb{Q}(i) \subset \mathbb{K} \subset \overline{\mathbb{Q}}$
- $\forall\, c \in \mathbb{K}$: $\bar{c} \in \mathbb{K}$ und $\sqrt{c} \in \mathbb{K}$

Frage: Ist das Pentagon konstruierbar?



$\pentagon$ konstr. $\Leftrightarrow$ $\zeta, \zeta^2, \zeta^3, \zeta^4 \in \mathbb{K}$

$\Leftrightarrow$ $\underbrace{\zeta}_{\varphi} \in \mathbb{K}$

$e^{\frac{2\pi i}{5}} = \underbrace{\cos\frac{2\pi}{5}}_{\operatorname{Re}\zeta} + i\,\underbrace{\sin\frac{2\pi}{5}}_{\operatorname{Im}\zeta} \in \mathbb{K}$

Lemma 1
$\Leftrightarrow$ $\cos\varphi$ und $\sin\varphi \in \mathbb{K}$

$\Leftrightarrow$ $\cos\varphi \in \mathbb{K}$

[„$\Leftarrow$": $\sin^2\varphi + \cos^2\varphi = 1 \Rightarrow \sin\varphi = \pm\sqrt{\underbrace{1-\cos^2\varphi}_{\in\mathbb{K}}} \in \mathbb{K}$]

Bch.: $\cos\frac{2\pi}{5} = \underbrace{\frac{\sqrt{5}-1}{4}}_{\in\mathbb{K}}$ $\rightsquigarrow$ Daraus folgt: Pentagon konstruierbar!

Bew. Idee: $\frac{\sqrt{5}-1}{4}$ ist Lösung einer quadratischen Gleichung.

$\rightsquigarrow$ suche nach quadr. Gleichung, die $\cos\frac{2\pi}{5}$ erfüllt.

$\cdot\ \zeta = e^{\frac{2\pi i}{5}} = \cos\frac{2\pi}{5} + i\sin\frac{2\pi}{5}$

$\bar{\zeta} = e^{-\frac{2\pi i}{5}} = \cos\frac{2\pi}{5} - i\sin\frac{2\pi}{5} = \zeta^{-1}$

$\Rightarrow \zeta + \zeta^{-1} = 2\cos\frac{2\pi}{5} =: z$

$\zeta^5 = 1 \Rightarrow g(\zeta) = 0$ für $g(x) = x^5 - 1$

$= (x-1)\underbrace{(x^4 + x^3 + x^2 + x + 1)}$

$\zeta \neq 1 \Rightarrow f(\zeta) = \zeta^4 + \zeta^3 + \zeta^2 + \zeta + 1 = 0$ $\quad 1\cdot\zeta^2$ $f(x)$ irred.

$\Rightarrow$ Min. Polynom von ζ

$\Leftrightarrow \quad \zeta^2 + \zeta + 1 + \zeta^{-1} + \zeta^{-2} = 0$

$\Leftrightarrow \quad \underbrace{(\zeta^2 + \zeta^{-2})}_{z^2-2} + \underbrace{(\zeta + \zeta^{-1})}_{z} + 1 = 0$

$\cdot\ z^2 = (\zeta + \zeta^{-1})^2 = \zeta^2 + 2\zeta\zeta^{-1} + \zeta^{-2} = \zeta^2 + \zeta^{-2} + 2$

$\Rightarrow \quad z^2 + z - 1 = 0$

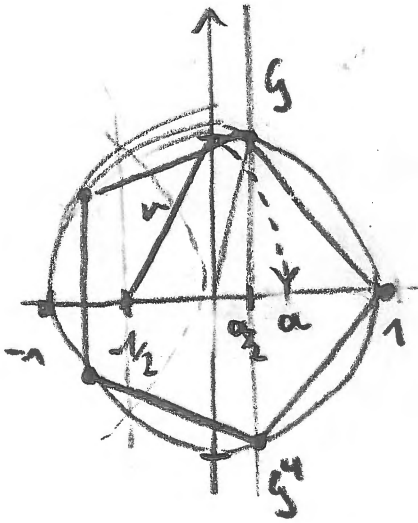
$\Rightarrow \quad z_{1,2} = -\frac{1}{2} \pm \sqrt{\frac{1}{4} + 1} = \frac{-1 \pm \sqrt{5}}{2}$

$\Rightarrow 2\cos\left(\frac{2\pi}{5}\right) = \frac{-1 \pm \sqrt{5}}{2} \Rightarrow \cos\left(\frac{2\pi}{5}\right) = \frac{-1+\sqrt{5}}{4}$ $\quad \square$

$\cos\left(\frac{2\pi}{5}\right) > 0$

denn $\frac{2\pi}{5} \leq \frac{\pi}{2}$

Konstruktion des Pentagons



(1) $r = \sqrt{1 + \left(\frac{1}{2}\right)^2} = \frac{\sqrt{5}}{2}$

$\Rightarrow a = \frac{\sqrt{5}-1}{2} \Rightarrow \frac{a}{2} = \cos\frac{2\pi}{5}$!

entspricht $\Rightarrow \sin\frac{2\pi}{5} = \sqrt{1 - \left(\frac{a}{2}\right)^2} =: b$

$\mathbb{Q} \subset \mathbb{Q}(a) \subset \mathbb{Q}(\underbrace{a + ib}_{\zeta}) \cong \mathbb{Q}[X]/(X^4 + X^3 + X^2 + X + 1)$

$\Rightarrow [\mathbb{Q}(\zeta) : \mathbb{Q}(a)] = 2$

$[\mathbb{Q}(a) : \mathbb{Q}] = 2$

$\cdot\ \mathbb{Q}(a) \cong \mathbb{Q}[z]/(z^2 + z - 1)$

③ Zwei Aufgaben zu endlichen Körpern

$K = \mathbb{Z}_p$ p prim.

Aufg. 1: Sei $p \neq 2$. Zeige dass folgende Aussagen äquivalent sind:

(i) -1 ist ein Quadrat in $\mathbb{Z}_p$

(ii) $f(x) = x^2+1$ hat Nullstelle in $\mathbb{Z}_p$

(iii) $\mathbb{Z}_p^*$ hat Element der Ordnung 4

(iv) $p \equiv 1 \bmod 4$.

Bew.:

i) $\Leftrightarrow$ ii): $\exists a \in \mathbb{Z}_p: a^2 = -1 \Leftrightarrow a^2+1 = 0$

$\Leftrightarrow \exists a \in \mathbb{Z}_p: f(a) = 0$

ii) $\Rightarrow$ iii): $\exists a \in \mathbb{Z}_p: \underbrace{f(a)}_{a^2+1} = 0 \Rightarrow a^4 = (-1)^2 = 1$

$\Rightarrow \operatorname{ord}(a) \mid 4$

$\Rightarrow \operatorname{ord}(a) = 4$

- falls $a^2 = 1 \Rightarrow -1 = a^2 = 1 \Rightarrow 2 = 0$
- falls $a = 1 \Rightarrow \underbrace{a^2+1}_{2} = 0$ $\Big\}$ $p = 2$ ↯
- falls $a = 0 \Rightarrow 0+1 = 0$ ↯

$\Rightarrow a \in \mathbb{Z}_p^*$.

iii) $\Rightarrow$ iv): $\exists g \in \mathbb{Z}_p^*: \operatorname{ord}(g) = 4 \Rightarrow \underbrace{4}_{\operatorname{ord}(g)} \mid \underbrace{p-1}_{\operatorname{ord}(\mathbb{Z}_p^*)}$

$\Leftrightarrow \exists m \in \mathbb{Z}: 4m = p-1 \Leftrightarrow p-1 \equiv 0 \bmod 4$

$\Leftrightarrow p \equiv 1 \bmod 4$

iv) $\Rightarrow$ i):

Bem.: G zyklisch, $d \mid \operatorname{ord} G \Rightarrow \exists g \in G: \operatorname{ord}(g) = d$

[$G \cong \mathbb{Z}_n$ $d \mid n \rightsquigarrow g = \frac{n}{d}$]

- $4 \mid p-1 \Rightarrow \exists g \in \mathbb{Z}_p^*: \operatorname{ord}(g) = 4 \Rightarrow \underbrace{g^4 - 1}_{(g^2-1)(g^2+1)} = 0$

$\operatorname{ord}(g) \neq 2 \Rightarrow g^2 \neq 1$

$\Rightarrow g^2+1 = 0$

$\Rightarrow g^2 = -1$ □

Aufg. 2: $p \neq 2,3$. Zeige:

(i) -3 ein Quadrat in $\mathbb{Z}_p$.

$\Rightarrow$ (ii) $f(x) = x^2+x+1$ hat Nullstelle in $\mathbb{Z}_p$

$\Rightarrow$ (iii) $\mathbb{Z}_p^*$ hat Element der Ordnung 3

$\Rightarrow$ (iv) $p \equiv 1 \bmod 3$

Bew.:

(ii) $\Leftrightarrow$ (iii): x^2+x+1 hat Nullstelle a in $\mathbb{Z}_p$

$\Leftrightarrow$ $\underbrace{(x-1)(x^2+x+1)}_{x^3-1}$ hat Nullstelle $a \in \mathbb{Z}_p \setminus \{1\}$ [$a^2+a+1 \underset{a=1}{=} 3 \neq 0$]

$\Leftrightarrow$ $\exists a \in \mathbb{Z}_p \setminus \{1\}: a^3 = 1 \Rightarrow \operatorname{ord}(a) = 3$

falls $a=0$: $\underbrace{a^2+a+1}_{1} = 0$ ↯ $\Rightarrow a \in \mathbb{Z}_p^*$

(iii) $\Leftrightarrow$ (iv): $\exists g \in \mathbb{Z}_p^*: \operatorname{ord}(g) = 3 \overset{\text{Bem.}}{\Leftrightarrow} 3 \mid \underbrace{p-1}_{\operatorname{ord}\mathbb{Z}_p^*}$

$\Leftrightarrow p-1 \equiv 0 \bmod 3$

$\Leftrightarrow p \equiv 1 \bmod 3$.

ii) $\Rightarrow$ i): $f(a) = a^2+a+1 = 0$

$\Rightarrow a^2+a = -1 \quad |\cdot 3$

$\Rightarrow 3a^2+3a = -3 \quad |+\underbrace{(a^2+a+1)}_{0}$

$\Rightarrow \underbrace{4a^2+4a+1}_{(2a^2+1)^2} = -3$ „$f(a)=0 \Rightarrow g(2a+1)=0$ mit $g(x)=x^2+3$"

i) $\Rightarrow$ ii): „$g(b)=0 \rightsquigarrow f(\frac{1}{2}(b-1))=0$"

$\exists b \in \mathbb{Z}_p: \quad b^3 = -3$

$$f\left(\tfrac{1}{2}(b-1)\right) = \tfrac{1}{4}(b-1)^2 + \tfrac{1}{2}(b-1) + 1 = \tfrac{1}{4}(b^2-2b+1) + \tfrac{1}{2}b + \tfrac{1}{2}$$

$$= \tfrac{1}{4}\underbrace{b^2}_{-3} + \tfrac{1}{4} + \tfrac{1}{2} = 0.$$

□

④ Für welche n ist das regelmäßige $\underbrace{n\text{-Eck}}_{\Delta_n}$ konstruierbar? ($n \geq 3$) (mit Zirkel und Lineal)

Satz 1: Sei $z \in \mathbb{C}$.

$z \in \mathbb{K} \Leftrightarrow \exists$ Körper L mit $\mathbb{Q} \subset L \subset \bar{\mathbb{Q}}$, $z \in L$

$[L:\mathbb{Q}] = 2^k$ $\exists k \in \mathbb{N}_0$ und L ist Zerfällungskörper einer Familie von Polynomen aus $\mathbb{Q}[X]$.

- Δ_n konstruierbar $\Leftrightarrow \zeta_n = e^{\frac{2\pi i}{n}} \in \mathbb{K}$

Satz 2: $\zeta_n \in \mathbb{K} \Leftrightarrow [\mathbb{Q}(\zeta_n):\mathbb{Q}] = 2^k$ $\exists k \in \mathbb{N}_0$.

Def.: $\Phi_n = \{1 \leq i < n \mid ggT(i,n) = 1\}$

- $\varphi(n) := \# \Phi_n$ „Eulersche φ-Funktion"
- $m_{\zeta_n}(X) = \prod_{i \in \Phi_n} (X - \zeta_n^i)$

Satz 3: $m_{\zeta_n}(X) \in \mathbb{Z}[X]$ ist irreduzibel.

$\Rightarrow$ $m_{\zeta_n}(X)$ ist Min Polynom von ζ_n

$\Rightarrow$ $[\mathbb{Q}(\zeta_n):\mathbb{Q}] = \deg m_{\zeta_n} = \varphi(n)$

Kor.: $\zeta_n \in \mathbb{K} \Leftrightarrow \varphi(n) = 2^k$ $\exists k \in \mathbb{N}_0$.

Bsp.: Sei $n = p$ $p \neq 2$ prim $\Rightarrow m_{\zeta_p}(X) = \underbrace{X^{p-1} + X^{p-2} + \ldots + X + 1}_{\text{irred. nach [VL].}} \in \mathbb{Z}[X]$

$\Rightarrow [\mathbb{Q}(\zeta_p):\mathbb{Q}] = p - 1 = \varphi(p)$

$\Rightarrow$ • $\zeta_p \in \mathbb{K} \Leftrightarrow p = 2^k + 1$ $\exists k \in \mathbb{N}$ (Lemma) $\Leftrightarrow p = 2^{2^j} + 1$ $\exists j \in \mathbb{N}_0$ $\Leftrightarrow$ p eine Fermat'sche Primzahl

Def.: $F_j := 2^{2^j} + 1$ „Fermat'sche Zahl"

p	②	⑤	7	11	13	⑰	19	...	257	...	65537	...
$\varphi(p)$	2	4	6	10	12	16	18	...	256	...	65536	...
$\zeta_p \in \mathbb{K}$?	✓	✓	×	×	×	✓	×	...	✓		✓	...
	F_0	F_1				F_2			F_3		F_4	

Satz 4: $n \in \mathbb{N}_{\geq 3}$ $\zeta_n \in \mathbb{K} \Leftrightarrow n = 2^m \cdot \underbrace{p_r \cdot \ldots \cdot p_1}_{\text{verschiedene Fermat'sche Primzahlen!}}$ $\exists m \in \mathbb{N}_0$.

Bem.: $F_0, \ldots, F_4$ sind alle bekannten Fermat'schen Primzahlen!