III KÖRPER (ERWEITERUNGEN)

§6 GRUNDLEGENDE BEGRIFFE

6.1. Charakteristik

R Ring mit 1, $n \in \mathbb{N}$, $a \in R$, dann setze

$n \cdot a := \underbrace{a + \ldots + a}_{n\text{-mal}}$ [bzw. $0 \cdot a = 0$], $(-n) \cdot a := n \cdot (-a)$

$\varphi: \mathbb{Z} \to R$, $n \mapsto n \cdot 1$ ist Ringhomo $\Rightarrow$

$\ker \varphi$ Unterring ($\Rightarrow$ Untergr.) $\Rightarrow \exists m \in \mathbb{N}: \ker \varphi = m\mathbb{Z}$

wir nennen $\operatorname{char}(R) := m$ die Charakteristik von R

- $\operatorname{char}(R) = 0$ heißt, dass φ injektiv $\mathbb{Z} \to R$ ist
- falls $\operatorname{char}(R) > 0$, dann gilt

$$\operatorname{char}(R) = \min \{ k \in \mathbb{N} \mid k > 0,\ k \cdot 1 = 0 \}$$

SATZ: K Körper $\Rightarrow$ $\operatorname{char}(K) = 0$ oder $\operatorname{char}(K)$ Primzahl

Beweis: sei $m = \operatorname{char}(K)$ und $m > 0$; wäre m nicht prim, dann $\exists k, \ell \in \mathbb{N}: m = k \cdot \ell$, $1 < k, \ell < m$

$\Rightarrow 0 = m \cdot 1 = (k\ell) \cdot 1 = (k \cdot 1) \cdot (\ell \cdot 1)$ .... K Körper! $\Rightarrow$

$\Rightarrow k \cdot 1 = 0$ oder $\ell \cdot 1 = 0$

$\Rightarrow \operatorname{char}(K) < m$ ↯ □

6.2. Grad einer Körpererweiterung

sei $F \subseteq K$ Körpererweiterung (F Unterkörper von K),

wenn L weiterer Unterkörper von K mit $F \subseteq L$,

dann nennen wir $F \subseteq L \subseteq K$ einen

Zwischenkörper

BEISP: $\mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$

Idee: K kann als Vektorraum über F

aufgefasst werden: Vektoraddition in K,

skalare Multiplikation $F \times K \to K$, $(x, y) \mapsto x \cdot y$

mittels Einschränkung der üblichen Mult. in K

DEF: der Körpergrad von $F \subseteq K$ ist

$[K : F] := \dim_F(K)$ .... VR-Dim. von K als F-VR.

BEISP: 1) $[\mathbb{C} : \mathbb{R}] = 2 \ldots = \dim_{\mathbb{R}}(\mathbb{C})$ (klar)

2) $[\mathbb{R}:\mathbb{Q}] = \infty$, denn wäre $\mathbb{R}$ als $\mathbb{Q}$-VR endlichdimensional mit Basis $x_1, \dots, x_n \in \mathbb{R}$

$$\Rightarrow \mathbb{R} = \{\lambda_1 x_1 + \dots + \lambda_n x_n \mid \lambda_1, \dots, \lambda_n \in \mathbb{Q}\}$$

diese Menge ist überabzählbar

diese Menge ist abzählbar, nämlich gleichmächtig mit $\mathbb{Q}^n$

Widerspruch ↯

SATZ (Gradformel): $F \subseteq L \subseteq K$ Zwischenkörper

$$\Rightarrow [K:F] = [K:L] \cdot [L:F]$$

Beweis: Falls $\dim_L(K) = \infty$ oder $\dim_F(L) = \infty$, dann auch $\dim_F(K) = \infty$, denn eine L-lin. unabh. Menge in K ist sicher auch F-lin. unabh. bzw. eine F-lin. unabh. Menge in L auch F-lin. unabh. in $K \supseteq L$.

Bleibt also der Fall $[L:F] = n < \infty$ und $[K:L] = n < \infty$ zu betrachten:

Sei $x_1, \dots, x_m$ Basis im F-VR L und
$y_1, \dots, y_n$ Basis im L-VR K.

Wir zeigen: $\{x_i \cdot y_j \mid i = 1, \dots, m \text{ und } j = 1, \dots, n\}$ ist
Basis im F-VR K (das ergibt m·n Basis-
elemente, also fertig)

- $y \in K$ beliebig hat eind. Darstellung
$$y = b_1 y_1 + \dots + b_n y_n \quad \text{mit } b_1, \dots, b_n \in L,$$
$\forall j$: es gibt eind. Darstellung
$$b_j = a_{1j} \cdot x_1 + \dots + a_{mj} \cdot x_m \quad \text{mit } a_{ij} \in F,$$
also
$$y = \sum_{i,j} a_{ij} \cdot x_i y_j, \text{ also } \operatorname{span}\{x_i \cdot y_j\} = K.$$

- $\{x_i y_j \mid i = 1, \dots, m;\ j = 1, \dots, n\}$ ist lin. unabh. über F:

$$\sum_{i,j} \underbrace{a_{ij}}_{\in F} x_i y_j = 0 \Rightarrow \sum_j \underbrace{\left(\sum_i a_{ij} x_i \right)}_{\in L} y_j = 0$$
↑ lin. unabh. über L

$$\Rightarrow \forall j: \sum_i a_{ij} x_i = 0$$
↑ lin. unabh. über F

$$\Rightarrow a_{ij} = 0 \ \forall i \forall j$$

□

KOR: $F \subseteq L \subseteq K$ Zwischenkörper und $[K:F] < \infty$, dann gilt:

(a) $[K:L] = [K:F] \Rightarrow F = L$,

(b) $[K:F]$ Primzahl $\Rightarrow F = L$ oder $L = K$.

Beweis: (a): $[K:F] = [K:L] \cdot [L:F]$

($=$ und $\neq \infty$)

$\Rightarrow [L:F] = 1$,

also wegen $L \supseteq F$ als VR $L = F$.

(b) $[K:F] = [K:L] \cdot [L:F]$

($[K:F]$ prim)

$\Rightarrow [K:L] = 1$ oder $[L:F] = 1$

$\Rightarrow K = L$ oder $L = F$ □

BEISP: $[\mathbb{C}:\mathbb{R}] = 2$ prim

$\Rightarrow$ es gibt keine echten Zwischenkörper

$\mathbb{R} \subsetneq L \subsetneq \mathbb{C}$!

6.3. Adjunktion von Elementen

Sei $F \subseteq K$ Körpererweiterung und $A \subseteq K$

$F(A)$ ... kleinste Zwischenkörper $F \subseteq F(A) \subseteq K$ mit $A \subseteq F(A)$

$F[A]$ ... kleinste Unterring von K mit $F \cup A \subseteq F(A)$

BEISP: $F = \mathbb{R}$, $K = \mathbb{C}$, $A = \{i\}$: $\mathbb{R}(i) = \mathbb{C}$, weil $\mathbb{R}(i) \neq \mathbb{R}$ und $\nexists$ echte Zwischenkörper $\mathbb{R} \subsetneq L \subsetneq \mathbb{C}$

$\mathbb{R}(i) = \{a+bi \mid a,b \in \mathbb{R}\}$

- Im Falle $A = \{\alpha\}$ schreiben wir $F[A] = F[\alpha]$, $(F(A) = F(\alpha))$, es gilt

$F[\alpha] = \{ f(\alpha) \mid f \in F[X] \}$, denn $\sigma_\alpha : f \mapsto f(\alpha)$

ist Homo $F[X] \to K$, dessen $S := \sigma_\alpha(F[X]) =$

$= \{ f(\alpha) \in K \mid f \in F[X] \}$ ein Unkring von K

mit $\alpha \in S$, weil $\sigma_\alpha(X) = \alpha$; somit $F[\alpha] \subseteq S$;

ist R Unkring von K mit $\alpha \in R$ und $F \subseteq R$

$\Rightarrow f(\alpha) \in R \quad \forall f \in F[X]$, weil $f = b_0 + \dots + b_n X^n$

$\Rightarrow f(\alpha) = b_0 + \dots + b_n \alpha^n \in R$

also $S \subseteq R$; somit S minimal, d.h. $F[\alpha] = S$ □

- Ohne Beweis: $F(A) = Q(F[A])$ ... Quotientenkörper

$\quad \{ a \cdot b^{-1} \mid a,b \in F[A], b \neq 0 \}$

BEISP-Fortsetzung: $\mathbb{R}[i] = \{f(i) \in \mathbb{C} \mid f \in \mathbb{R}[X]\}$

mit $f(X) = a + bX$ $(a, b \in \mathbb{R})$ ergibt sich

$f(i) = a + bi$; also $\mathbb{R}[i] = \mathbb{R}(i) = \mathbb{C}$

BEM: $F(A_1 \cup A_2) = (F(A_1))(A_2)$

speziell $F(\{a_1, a_2\}) = (F(a_1))(a_1)$

6.4. Algebraische und transzendente Elemente

DEF: Sei $K \supseteq F$ Körpererweiterung

$a \in K$ heißt algebraisch über F, falls $\exists$ Polynom $f \in F[X]$, $f \neq 0$ mit $f(a) = 0$.

Andernfalls heißt a transzendent über F.

BEM: (i) $\forall a \in K$: a algebraisch über K, denn $f = X - a \in K[X]$ hat Nullstelle in a

(ii) $K = F(X) \supseteq F$: hier ist X transzendent über F, [↑ rationale Funktionen]

denn $\forall f \in F[X]$ mit $f \neq 0$ ist $f(X) = f \neq 0$

[vgl. Ü-Aufgabe 34 (b)]

(iii) ohne Beweise: e und π in $\mathbb{R}$ sind transzendent über $\mathbb{Q}$ (Hermite 1873; Lindemann 1882)

Betrachte den Einsetzungshomomorphismus

$$\sigma_\alpha : F[X] \to K, \quad f \mapsto f(\alpha)$$

Es gilt klarer Weise

- α transzendent über $F \iff \operatorname{Ker}\sigma_\alpha = \{0\}$
  $\iff \sigma_\alpha$ injektiv,
- α algebraisch über $F \iff \operatorname{Ker}\sigma_\alpha \neq \{0\}$.

SATZ: Ist $\alpha \in K \supseteq F$ transzendent über F, dann gilt:

(a) σ_α ergibt Isomorphismen $F[X] \to F[\alpha]$
und $F(X) \to F(\alpha)$

(b) $[F(\alpha) : F] = \infty$

Beweis: (a) haben in 6.3 gesehen: $F[\alpha] = \sigma_\alpha(F[X])$
und σ_α ist injektiv, daher $F[\alpha] \cong F[X]$;
somit auch $F(\alpha) = Q(F[\alpha]) \cong Q(F[X]) = F(X)$.

(b) $\{1, X, X^2, X^3, \ldots\}$ ist eine unendliche linear unabhängige Menge im F-VR $F[X] \cong F[\alpha]$,
daher auch im F-VR $F(X) \cong F(\alpha)$.
$\Rightarrow \dim_F(F(\alpha)) = \infty$

□

Insbesondere folgt aus (b):

(*) $[F(\alpha):F] < \infty \Rightarrow \alpha$ algebraisch,

was wir aber noch einmal direkt durchspielen können.

Sei $\dim_F(F(\alpha)) = n$, dann sind die $n+1$ Vektoren $1, \alpha, \alpha^2, \dots, \alpha^n$ sicher linear abhängig, d.h.

$\exists \lambda_0, \dots, \lambda_n \in F$ (nicht alle 0): $\lambda_0 \cdot 1 + \lambda_1 \cdot \alpha + \dots + \lambda_n \alpha^n = 0$,

d.h. $f(\alpha) = 0$ für $f = \lambda_0 + \lambda_1 X + \dots + \lambda_n X^n \in F[X]$, $f \neq 0$.

LEMMA: Sei $\alpha \in K$ algebraisch über F, dann gibt es ein eindeutiges normiertes Polynom $f_\alpha \in F[X]$ mit $\deg(f_\alpha) \geq 1$, sodass $\ker(\sigma_\alpha) = (f_\alpha)$ gilt.

f_α heißt Minimalpolynom von α über F.

Beweis: wir wissen, dass $\ker(\sigma_\alpha) \neq \{0\}$ gilt;

lt. 4.4. Kor. ist $F[X]$ ein Hauptidealring,

daher $\exists g \in F[X]: \ker(\sigma_\alpha) = (g)$;

lt. Beweis von 4.4. Satz haben wir

$\deg(g) = \min\{\deg(f) \mid f \in \ker\sigma_\alpha, f \neq 0\}$,

Wir können g normieren (d.h. Leitkoeffizient gleich 1 erreichen), indem wir geeignet multiplizieren

$\exists\, c \in F$: $f_\alpha := c \cdot g \in (g) = \mathrm{Kern}(\sigma_\alpha)$ normiert,

somit gilt $(f_\alpha) = \mathrm{Kern}(\sigma_\alpha)$, f_α normiert und von minimalem Grad.

Ist $h_\alpha \in F[X]$ ebenfalls normiert mit $h_\alpha \in \mathrm{Kern}(\sigma_\alpha)$ und $\deg(h_\alpha) = \deg(f_\alpha)$,

dann folgt $h_\alpha = r \cdot f_\alpha$ mit $r \in F[X]$,

$\deg(r) = 0$, also $r \in F$;

weil h_α und f_α normiert, folgt $r = 1$ □

6.5. Eigenschaften des Minimalpolynoms

Sei $F \subseteq K$ Körpererweiterung

LEMMA: Für $\alpha \in K$ und $f \in \mathrm{Kern}(\sigma_\alpha)$ (normiert) sind äquivalent:

(i) f ist das Minimalpolynom von α,

(ii) $\forall\, g \in \mathrm{Kern}(\sigma_\alpha),\ g \neq 0$: $\deg(g) \geq \deg(f)$,

(iii) f ist irreduzibel in $F[X]$.

Beweis: (i) $\Rightarrow$ (ii): $f = f_\alpha$ und $g \in \ker(\sigma_\alpha) = (f_\alpha)$

$\Rightarrow \exists\, h \in F[X],\ h \neq 0:\ g = \underbrace{h \cdot f_\alpha}$

$\deg g = \deg(h) + \deg(f_\alpha) \geq \deg(f_\alpha)$

(ii) $\Rightarrow$ (iii): Sei $f = g \cdot h$ mit $g, h \in F[X] \Rightarrow$

$0 = f(\alpha) = g(\alpha) \cdot h(\alpha) \Rightarrow g \in \ker(\sigma_\alpha)$ oder $h \in \ker(\sigma_\alpha)$,

wegen $\deg(f) \leq \deg(g)$, oder $\deg(f) \leq \deg(h)$

muss g oder h den Grad 0 haben, d.h.

$g \in F^\times$ oder $h \in F^\times$

(iii) $\Rightarrow$ (i): wegen $f \in \ker(\sigma_\alpha) = (f_\alpha)$ $\exists\, h \in F[X],\ h \neq 0$:

$f = h \cdot f_\alpha$; wegen $f_\alpha \notin F^\times$ ($\deg \geq 1$!)

muss noch (iii) $h \in F^\times$ gelten;

f und f_α normiert $\Rightarrow h = 1$, also $f = f_\alpha$ □

SATZ: α algebraisch über F, $f_\alpha \in F[X]$ das Minimalpolynom, dann gilt:

(a) $F[\alpha] = F(\alpha) \cong F[X]/(f_\alpha)$,

(b) $[F(\alpha) : F] = \deg(f_\alpha)$,

(c) $n = \deg(f_\alpha) \Rightarrow 1, \alpha, \alpha^2, \dots, \alpha^{n-1}$ ist Basis des F-VR $F(\alpha)$.

erinnere:
$\sigma_\alpha : F[X] \to K$
$f \mapsto f(\alpha)$

Beweis: (a): $(f_\alpha) = \ker(\varepsilon_\alpha)$, $\operatorname{im}\varepsilon_\alpha \overset{[6.3]}{=} F[\alpha]$;

Isomorphiesatz $\Rightarrow$ $F[\alpha] \cong F[X]/(f_\alpha)$;

f_α nach Lemma irreduzibel, daher $F[X]/(f_\alpha)$ und somit $F[\alpha]$ ein Körper (Satz 5.1);

also $F(\alpha) = F[\alpha]$.

(b) und (c): zunächst Behauptung

(*) $F[\alpha] = \{ h(\alpha) \in K \mid h \in F[X],\ \deg(h) < \deg(f_\alpha) \}$,

denn: $b \in F[\alpha] \Rightarrow \exists\, g \in F[X]: b = g(\alpha)$;

Division mit Rest: $g = q \cdot f_\alpha + h$ mit $\deg(h) < \deg(f_\alpha)$

es ist insbesondere $g(\alpha) = q(\alpha) \cdot \underbrace{f_\alpha(\alpha)}_{0} + h(\alpha)$

$\Rightarrow g(\alpha) = h(\alpha)$; d.h. $b \in$ rechter Seite in (*);

$F[\alpha] \supseteq$ re. Seite in (*) ist klar.

Sei also $n = \deg(f_\alpha)$; nach (*) gilt

$$F[\alpha] = \{ \lambda_0 + \lambda_1 \alpha + \dots + \lambda_{n-1} \alpha^{n-1} \mid \lambda_0, \dots, \lambda_{n-1} \in F \} =$$

$$= \operatorname{span}\{1, \alpha, \alpha^2, \dots, \alpha^{n-1}\} \text{ im } F\text{-VR } F[\alpha] = F(\alpha)$$

noch zu zeigen: $1, \alpha, \dots, \alpha^{n-1}$ sind lin. unabhängig

ang. $\exists\, \lambda_0, \dots, \lambda_{n-1} \in F$ mit $(\lambda_0, \dots, \lambda_{n-1}) \neq 0$ in F^n,
sodass $\lambda_0 + \lambda_1 \alpha + \dots + \lambda_{n-1} \alpha^{n-1} = 0$;

denn wäre $f := \lambda_0 + \lambda_1 X + \dots + \lambda_{n-1} X^{n-1} \in F[X]$,
$f \neq 0$ mit $f(\alpha) = 0$ und $\deg(f) < \deg(f_\alpha)$ ↯

Somit ist $1, \alpha, \dots, \alpha^{n-1}$ Basis von $F(\alpha)$ (also gilt (c))
und $[F(\alpha) : F] = n = \deg(f_\alpha)$ (also gilt (b)). □

BEISP: $F = \mathbb{Q}$; $\alpha \in \mathbb{C}$ mit $b := \alpha^2 \in \mathbb{Q}$, aber $\alpha \notin \mathbb{Q}$
[z.B: $\alpha = i$ oder $\alpha = \sqrt{2}$ .....],
dann ist $X^2 - b \in \mathbb{Q}[X]$ irreduzibel
[sonst $X^2 - b = (X - b_1)(X - b_2)$ und $b_1, b_2 \in \mathbb{Q}$
Nullstellen von $X^2 - b \Rightarrow \{b_1, b_2\} = \{\alpha, -\alpha\} \notin \mathbb{Q}$];
da $X^2 - b$ auch normiert ist, ist $f_\alpha = X^2 - b$
das Minimalpolynom von α über $\mathbb{Q}$;
$[\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg(f_\alpha) = 2$ und

$$\mathbb{Q}(\alpha) = \mathbb{Q}[\alpha] = \{\alpha + \beta\alpha \mid \alpha, \beta \in \mathbb{Q}\}$$

$$\frac{1}{\alpha + \beta\alpha} = \frac{\alpha - \beta\alpha}{(\alpha + \beta\alpha)(\alpha - \beta\alpha)} = \frac{\alpha - \beta\alpha}{\alpha^2 - \beta^2\alpha^2} = \frac{\alpha}{\alpha^2 - \beta^2 b} + \frac{-\beta}{\alpha^2 - \beta^2 b} \cdot \alpha \in \mathbb{Q}(\alpha)$$

6.6. Kurzer Ausblick:

(A) Körpererweiterung $K \supseteq F$ heißt *algebraisch*, falls jedes $\alpha \in K$ algebraisch über F ist.

Im Falle $[K:F] = n < \infty$ („endliche Körpererweiterung") ist $K \supseteq F$ algebraisch, denn für $\alpha \in K$ muss $1, \alpha, \dots, \alpha^n$ lin. abh. sein, d.h.

$\exists\, \lambda_0, \dots, \lambda_n \in F$: $\lambda_0 + \lambda_1 \alpha + \dots + \lambda_n \alpha^n = 0$, (nicht alle 0)

d.h. $f := \lambda_0 + \lambda_1 X + \dots + \lambda_n X^n \in F[X]$, $f \neq 0$ und $f(\alpha) = 0$.

Insbesondere ist $\mathbb{C} \supseteq \mathbb{R}$ algebraisch.
(Konkret trifft $w = a + bi$ als Nullstelle von $(X - (a+bi)) \cdot (X - (a-bi)) = X^2 - 2aX + a^2 + b^2 \in \mathbb{R}[X]$ auf)

(B) Körper K heißt *algebraisch abgeschlossen*, wenn jedes Polynom $f \in K[X]$ mit $\deg(f) \geq 1$ mindestens eine Nullstelle in K hat.

Durch sukzessive Anwendung von 3.7 (Nullstellen ~ Linearfaktoren) können wir also $f \in K[X]$ mit $n = \deg(f) \geq 1$ in diesem Fall immer in der Form

$$f = a \cdot (X - x_1) \cdots (X - x_n)$$ schreiben

mit $a \in K^\times$, $x_1, \ldots, x_n \in K$ (die Nullstellen).

Also:

K algebraisch abgeschlossen

$\Leftrightarrow$

jedes irreduzible Polynom in $K[X]$ hat Grad 1

<u>Fundamentalsatz der Algebra</u>:

$\mathbb{C}$ ist algebraisch abgeschlossen. (ohne Bew.)

„Ironie dabei": es gibt keinen rein algebraischen Beweis davon (Topologie oder komplexe Analysis oder Analysis ....)

<u>Reelle Fassung</u>: $f \in \mathbb{R}[X]$ mit $n := \deg(f) \geq 1$ hat Darstellung

$$f = (X - x_1) \cdots (X - x_m) \cdot g_1 \cdots g_r,$$

wobei $m + 2r = n$, $x_1, \ldots, x_m$ die reellen Nullst. und $g_1, \ldots, g_r$ irreduzible quadratische Polynome in $\mathbb{R}[X]$ sind.

BEM: ein algebraisch abgeschlossener Körper muss unendlich viele Elemente besitzen (denn andernfalls $K = \{a_0, a_1, \dots, a_n\}$ hätte Polynom $f := (X-a_0)\cdot(X-a_1)\cdots(X-a_n)+1$ in $K[X]$ ohne Nullstelle, weil $f(a_j) = 1$ $(j=1,\dots,n)$

(C) für $f = a_n X^n + \dots + a_r X^r + \dots + a_1 X + a_0 \in F[X]$ ist formale Ableitung definiert durch

$$f' := n a_n X^{n-1} + \dots + r a_r X^r + \dots + a_1 \in F[X]$$

Rechenregeln für $F[X] \to F[X]$, $f \mapsto f'$

$\forall a,b \in F: \forall f,g \in F[X]:$ $(af+bg)' = af' + bg'$ F-Linearität

und $(f\cdot g)' = f'\cdot g + f\cdot g'$ (Produktregel).

Satz (o.B.): $f \in F[X]$, $\deg(f) \geq 1$, dann ist äquivalent:

(i) $\exists$ Erweiterungskörper $K \supseteq F$, in dem f mindestens eine mehrfache Nullstelle hat,

(ii) f und f' haben in $F[X]$ einen gemeinsamen Teiler $g \in F[X]$ mit $\deg(g) \geq 1$.

BEM: (i) ist x Nullstelle von $f \in F[X]$, dann gilt Vielfachheit von $x := \max\{r \in \mathbb{N} \mid (X-x)^r \text{ teilt } f\}$

(ii) $\text{char}(K) = 0 \Rightarrow$ Vielfachheit der Nullstelle x

$$\| $$

$$\max\{r \in \mathbb{N} \mid f(x) = \dots = f^{(r-1)}(x) = 0\}$$

(D) Wenn $f = X^n + a_{n-1}X^{n-1} + \dots + a_1 X + a_0 \in K[X]$ vollständig in Linearfaktoren zerfällt, d.h.

$f = (X-x_1)\cdot\dots\cdot(X-x_n)$ mit $x_1, \dots, x_n \in K$,

dann ergibt sich leicht für die Koeffizienten als Funktionen der Nullstellen

$$a_0 = (-1)^n \cdot x_1 \cdot x_2 \cdots x_n$$

$$a_1 = (-1)^{n-1} \cdot (x_2 x_3 \cdots x_n + x_1 x_3 \cdots x_n + \dots + x_1 \cdots x_{n-1})$$

$$\vdots \qquad\qquad \vdots$$

$$a_{n-1} = -(x_1 + x_2 + \dots + x_n)$$

sog. Wurzelsatz von Vieta

- rechts stehen symmetrische Funktionen, d.h. Permutation der $x_1, \dots, x_n$ ändert nichts!

Frage nach Auflösung obiger Formeln nach $x_1, \dots, x_n$ als Funktionen der Koeff. $a_0, \dots, a_{n-1}$ entspricht also der Suche nach Lösungsformeln für Nullstellen allgemeiner Polynome, möglichst nur durch Summen und Wurzeln in eventuellen Erweiterungskörpern („Auflösung durch Radikale"), einem sogenannten <u>Zerfällungs-körper</u> K für $f \in F[X]$, also $K \supseteq F$ so, „dass f in K in linearfaktoren zerfällt und K möglichst klein gewählt werden kann".

Klärung der Frage gelang auf Umweg über die Gruppentheorie: sei $K \supseteq F$ Körpererweiterung

$$\mathrm{Aut}(K,F) := \{ \varphi \in \mathrm{Aut}(K) \mid \varphi|_F = \mathrm{id}_F \}$$

Gruppe der Körperautomorphismen $\varphi: K \to K$, die F fix lassen

Wenn $K \supseteq F$ Zerfällungskörper von $f \in F[X]$ ist, so heißt

$$Gal(f;F) := Aut(K;F)$$

die Galoisgruppe von f über F.

Galoistheorie liefert Korrespondenz:

Zwischenkörper von $K \supseteq F$ $\longleftrightarrow$ Untergruppen von $Aut(K;F)$

Wenn $char(F) = 0$, dann gilt für $f \in F[X]$:

f ist durch Radikale auflösbar

$\Updownarrow$

$Gal(f;F)$ ist eine auflösbare Gruppe,

d.h. $\exists$ Untergruppen $N_0, N_1, \dots, N_k$ von $Gal(f;F)$,

sodass

$$G = N_0 \rhd N_1 \rhd \dots \rhd N_k = \{e\}$$

und N_j / N_{j+1} ist abelsch $(j = 0, \dots, k-1)$.

Für allgemeines Polynom n-ten Grades
(d.h. mit Koeff. als symm. Fkt. von n Variablen)
lässt sich die Galoisgruppe mit der
Permutationsgruppe S_n identifizieren (als
isomorphes Bild).
Weil man zeigen kann, dass S_n für $n \geq 5$
keine auflösbare Gruppe ist, folgt, dass
es keine allgemeine Lösungsformeln durch
Radikale für Polynomgleichungen vom
Grad ≥ 5 geben kann!

Für Grade 2, 3, 4 sind Formeln bekannt.
Für spezielle Typen/Klassen von Polynomen
höheren Grades können Auflösungen durch
Radikale gelingen, z.B. Kreisteilungspolynome.

§7 ANWENDUNG AUF KONSTRUKTIONEN MIT ZIRKEL UND LINEAL

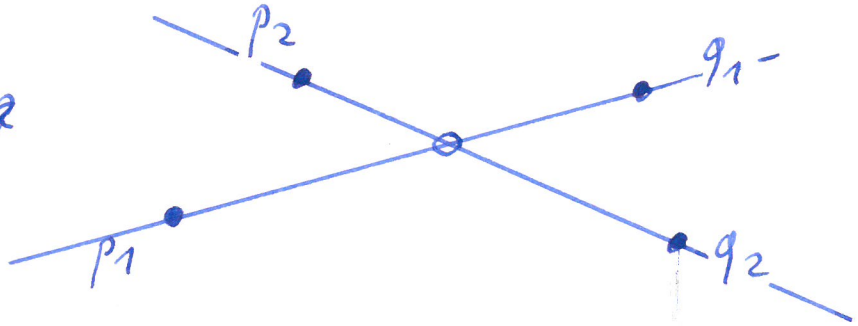
Zeichenebene $\mathbb{R}^2$, vorgegebene Teilmenge $M \subseteq \mathbb{R}^2$;
wir werden die Menge, der aus M mit Zirkel und Lineal (ohne Maßeinheiten benutzt) exakt konstruierbaren Punkte im $\mathbb{R}^2$ mit Hilfe algebraischer Begriffe und Methoden beschreiben

7.1. Die geometrischen Konstruktionsregeln

Typ I: Schnittpunkte nichtparalleler Geraden

gegeben: •

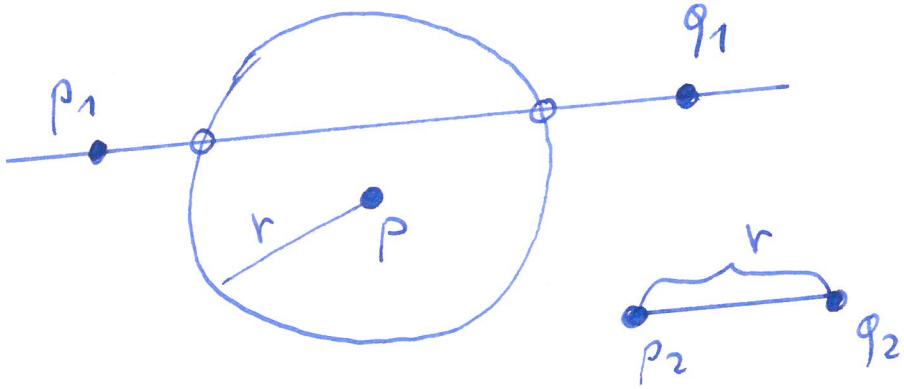
konstruiert: ○



Typ II: Schnitt Gerade mit Kreis

gegeben: •

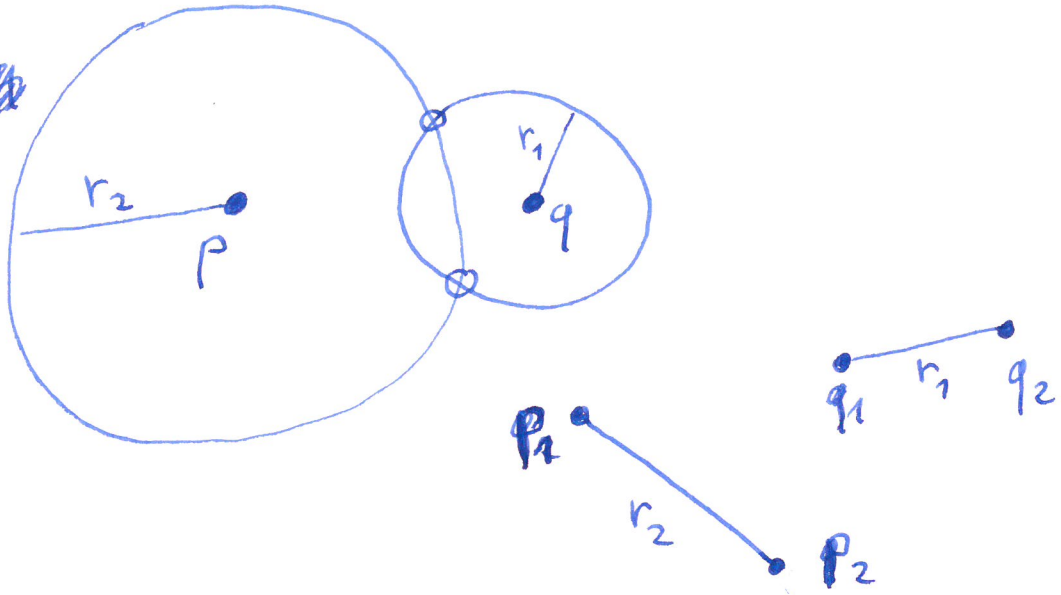
konstruiert: ○



Typ III: Schnitt zweier Kreise

gegeben: •

konstruiert: ○



DEF: $M \subseteq \mathbb{R}^2$, dann besteht die Menge $Kon(M) \subseteq \mathbb{R}^2$ aus jenen Punkten $p \in \mathbb{R}^2$, für die es ein $n \in \mathbb{N}$ und eine Kette von Teilmengen

$$M = M_0 \subseteq M_1 \subseteq \ldots \subseteq M_n$$ von $\mathbb{R}^2$ gibt, sodass jedes M_j aus M_{j-1} durch eine Konstruktionsregel I, II oder III entsteht und $p \in M_n$ gilt.

$Kon(M)$ heißt die Menge aller aus M mit Zirkel und Lineal konstruierbaren Punkte.

- in jedem Schritt kommen 0, 1 oder 2 Punkte hinzu !

7.2. „Algebraisierung" von $\mathrm{Kon}(M)$

wir identifizieren $\mathbb{R}^2$ mit $\mathbb{C}$, damit wir die Körperstruktur von $\mathbb{C}$ verwenden können.

SATZ: Sei $M \subseteq \mathbb{C}$ mit $0, 1 \in M$ und setze $\overline{M} := \{\overline{z} \mid z \in M\}$. Dann gilt:

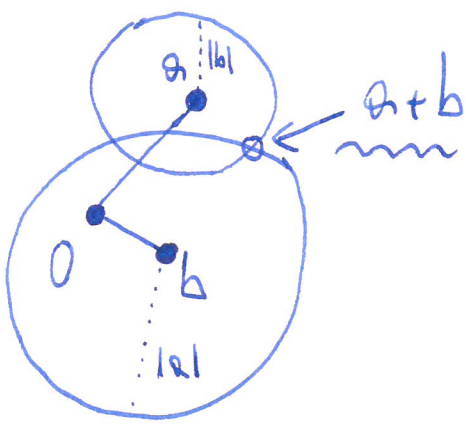
(i) $\mathrm{Kon}(M)$ ist Unterkörper von $\mathbb{C}$,

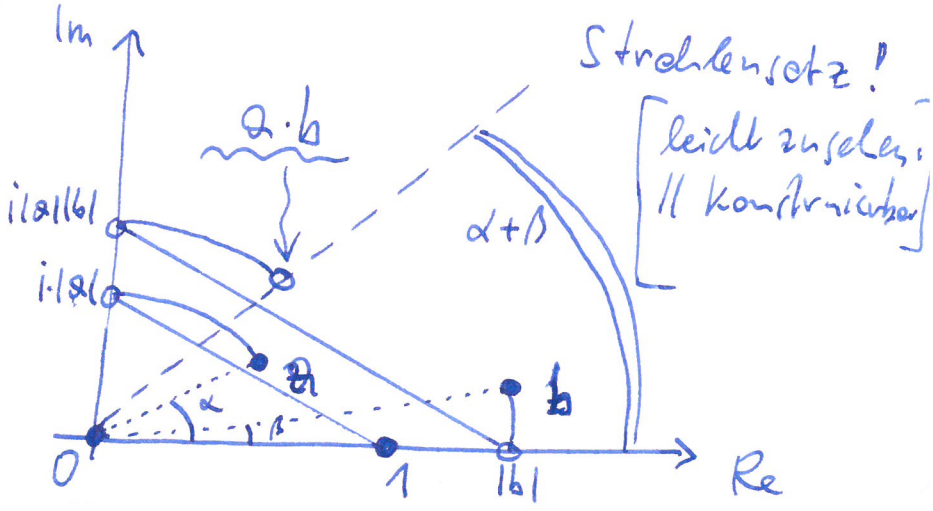
(ii) $\mathbb{Q}(M \cup \overline{M})$ ist Unterkörper von $\mathrm{Kon}(M)$ und $\overline{\mathrm{Kon}(M)} = \mathrm{Kon}(M)$,

(iii) $b \in \mathbb{C}$ und $b^2 \in \mathrm{Kon}(M) \Rightarrow b \in \mathrm{Kon}(M)$

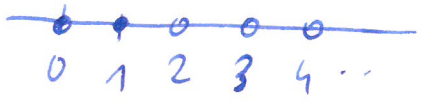
(in $\mathrm{Kon}(M)$ können also Quadratwurzeln konstruiert werden).

Beweisskizze: zu (i): $a, b \in \mathrm{Kon}(M)$





zu (ii): $0,1 \in M \Rightarrow \mathbb{Z} \subseteq \mathrm{Kon}(M)$

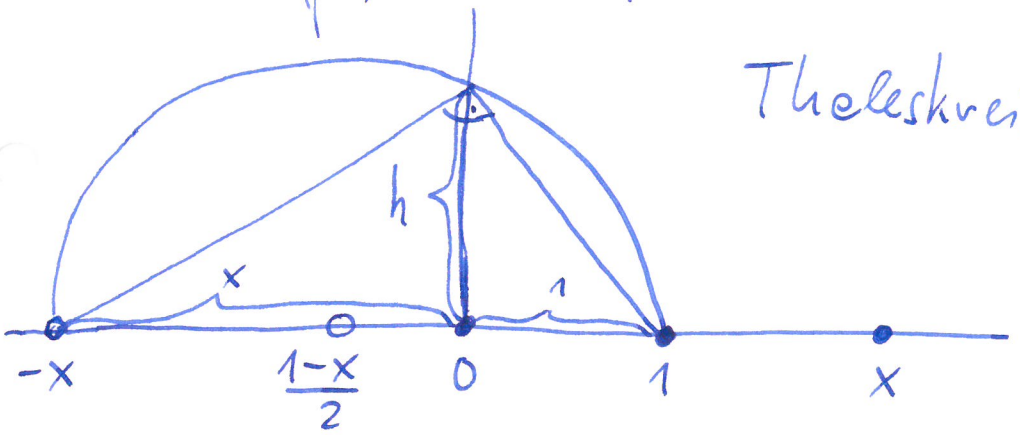


weil $\mathrm{Kon}(M)$ Körper muss

$\mathbb{Q} = Q(\mathbb{Z}) \subseteq \mathrm{Kon}(M)$; wegen $\overline{M} \subseteq \mathrm{Kon}(M) = \overline{\mathrm{Kon}(M)}$

auch $\mathbb{Q}(M \cup \overline{M}) \subseteq \mathrm{Kon}(M)$ leicht zu sehen

zu (iii): • für $x \in \mathbb{R}$, $x > 0$ konstruiere $\sqrt{x}$ wie folgt



Thaleskreis: $h^2 = x \cdot 1$

• für $z \in \mathbb{C}$ mit $|z| = 1$ einfach Winkelhalbierung für Wurzel

– Ausnehmen: $b^2 \in \mathrm{Kon}(M) \Rightarrow b \in \mathrm{Kon}(M)$

□

7.3. Eigenschaften des Körpers $\mathrm{Kon}(M)$

für $M \subseteq \mathbb{C}$ mit $0,1 \in M$ haben wir Zwischenkörper

$\mathbb{Q} \subseteq \mathrm{Kon}(\{0,1\}) \subseteq \mathrm{Kon}(M) \subseteq \mathbb{C}$; es gilt

(1) die Körpererweiterung $\mathrm{Kon}(M) \supseteq \mathbb{Q}(M \cup \overline{M})$ ist algebraisch (folgt aus Eig. (3) unten)

(2) $[\mathrm{Kon}(\{0,1\}):\mathbb{Q}] = \infty$

Bew: sukzessives Wurzelziehen $-1, i, e^{i\frac{\pi}{4}}, \ldots, e^{i\frac{\pi}{2^n}}, \ldots$

Minimalpolynom ~~der 2^n-ten Wurzel~~ über $\mathbb{Q}$ ist $X^{2^n}+1$, also Index $\geq 2^n$ $\forall n \in \mathbb{N}$.

(3) für $z \in \mathbb{C}$ gilt: $z \in \mathrm{Kon}(M) \iff$

$\exists$ Kette von Zwischenkörpern

$\mathbb{Q}(M \cup \bar{M}) = L_0 \subseteq L_1 \subseteq \ldots \subseteq L_r \subseteq \mathbb{C}$

mit $z \in L_r$ und $[L_j : L_{j-1}] \leq 2$ $(j = 1, \ldots, r)$.

Beweisidee: jeder Konstr.schritt ergibt höchstens 2 neue Punkte, die nicht im bisherigen Teilkörper liegen, aber durch eine Wurzel erfassbar sind ....

KOR: $M \subseteq \mathbb{C}$ mit $0,1 \in M$, $L := \mathbb{Q}(M \cup \bar{M})$, $z \in \mathrm{Kon}(M)$

$\Rightarrow [L(z):L] = 2^m$ für ein $m \in \mathbb{N}$.

Insbesondere ist z algebraisch über L.

- entscheidend für Unlösbarkeit einiger klassischer Konstruktionsprobleme!

7.4. Das Delische Problem der Würfelverdopplung ist unlösbar

? Kantenlänge l eines Würfels mit doppeltem Volumen des Einheitswürfels (also Kantenlänge 1) konstruierbar? Wir müssten $l = 2^{\frac{1}{3}}$ aus $M = \{0,1\}$ konstruieren.

Beh: $2^{\frac{1}{3}} \notin \mathrm{Kon}(\{0,1\})$

denn: Minimalpolynom von $2^{\frac{1}{3}}$ über $\mathbb{Q} = \mathbb{Q}(\{0,1\})$ ist $X^3 - 2$; daher $[\mathbb{Q}(2^{\frac{1}{3}}) : \mathbb{Q}] = 3$, was keine Zer-Potenz ist!

7.5. Winkeldreiteilung ist im Allgemeinen nicht exakt mit Zirkel und Lineal möglich

Natürlich können gewisse Winkel, wie etwa $270° \hat{=} \frac{3\pi}{2}$ gedrittelt werden, d.h. es kann $e^{3\pi i/2}$ aus $\{0,1,e^{3\pi i/2}\}$ konstruiert werden.

Die Frage ist aber, ob für jeden gegeben Winkel $\alpha \in [0,2\pi]$ der Punkt $z := e^{i\frac{\alpha}{3}}$ aus der Menge $M := \{0,1,\zeta\}$ mit $\zeta := e^{i\alpha}$ konstruierbar ist.

Beh: $\underbrace{e^{2\pi i/9}}_{z} \notin \mathrm{Kon}(\{0,1,\underbrace{e^{2\pi i/3}}_{\zeta}\})$ für $\alpha \hat{=} 120° \hat{=} \frac{2\pi}{3}$

Bew: $\overline{\zeta} = \frac{1}{\zeta} \Rightarrow \mathbb{Q}(M \cup \overline{M}) = \mathbb{Q}(\zeta) =: L$

wir werden $[L(z):L]$ aus der Gradformel bestimmen

$(*)$ $[L(z):\mathbb{Q}] = [L(z):L] \cdot [L:\mathbb{Q}]$

- $\cos\frac{2\pi}{3} = -\frac{1}{2}$, $\sin\frac{2\pi}{3} = \frac{\sqrt{3}}{2}$,

	0	30°	45°	60°	90°
cos	$\sqrt{4}/2$	$\sqrt{3}/2$	$\sqrt{2}/2$	$\sqrt{1}/2$	$\sqrt{0}/2$
sin	$\sqrt{0}/2$	$\sqrt{1}/2$	$\sqrt{2}/2$	$\sqrt{3}/2$	$\sqrt{4}/2$

also $\zeta = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$,

$$\zeta^2 = \frac{1}{4} - 2\cdot\frac{1}{2}i\frac{\sqrt{3}}{2} + i^2\frac{3}{4} = \frac{1}{4} - \frac{3}{4} - i\frac{\sqrt{3}}{2} = -\frac{1}{2} - i\frac{\sqrt{3}}{2}$$

also $\zeta^2 + \zeta = -1$, d.h. $\zeta^2 + \zeta + 1 = 0$;

ζ ist Nullstelle von $X^2 + X + 1$; zweite Nullst. ist $\overline{\zeta} \notin \mathbb{Q}$; somit ist $X^2 + X + 1$ das Minimalpolynom von ζ in $\mathbb{Q}[X]$

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

- $z^6 + z^3 + 1 = e^{4\pi i/3} + e^{2\pi i/3} + 1 = \zeta^2 + \zeta + 1 = 0$,

d.h. z ist Nullstelle von $X^6 + X^3 + 1 \in \mathbb{Q}[X]$

und $X^6 + X^3 + 1$ irreduzibel (o.B.; siehe Fischer, III, §5.6)

$\Rightarrow [\mathbb{Q}(z):\mathbb{Q}] = 6$;

- wegen $z^3 = \zeta$ gilt $\mathbb{Q}(\{\zeta, z\}) = \mathbb{Q}(z)$

  $\mathbb{Q}(\zeta)(z) = L(z)$

  also $[L(z):\mathbb{Q}] = 6$

- somit ergibt (*): $6 = [L(z):L] \cdot 2$

  $\Rightarrow [L(z):L] = 3$ keine Zweierpotenz! □

7.6. Die Quadratur des Kreises ist unmöglich

? Wenn die Seitenlänge l eines Quadrats konstruiert werden, das flächengleich mit dem Kreis vom Radius 1 ist? Wir müssten $l = \sqrt{\pi}$ aus $M = \{0,1\}$ konstruieren. Mit $\sqrt{\pi}$ wäre aber auch π aus $K(\{0,1\})$; insbesondere wäre dann π algebraisch über $L = \mathbb{Q}(\{0,1\}) = \mathbb{Q}$ - Widerspruch ↯ zur Transzendenz von π.