§5. Körper, Körpererweiterungen und Konstruierbarkeit

1. **Def** Sei K ein Körper, sei $c: \mathbb{Z} \to K$ der Ringhomomorphismus $c(n) = n \cdot 1_K$. Es gibt $\ker(c) = l\mathbb{Z}$ für ein $l \in \mathbb{N}$ nach §3.8. Die Zahl l nennt man die Charakteristik von K, $l = \mathrm{char}(K)$. Da $c(\mathbb{Z}) \subseteq K$ ein Integritätsbereich ist, folgt $l = 0$ oder l ist Primzahl, vgl §3.13, §3.15.

2. **Beobachtungen über Körper** (a) Sind K, L Körper und ist $\varphi: K \to L$ ein Ringhomomorphismus, so ist φ injektiv, weil $\{0\}, K$ die einzigen Ideale in K sind und weil $\varphi(1_K) = 1_L$. Es folgt $\mathrm{char}(K) = \mathrm{char}(L)$.

(b) Ist K ein Körper, $X \subseteq K$ eine Teilmenge, so ist $\bigcap \{ L \subseteq K \mid L \text{ Teilkörper}, X \subseteq L \} \subseteq K$ ein Teilkörper, der von X erzeugte Teilkörper.

3. **Satz** Jeder Körper K besitzt einen eindeutig bestimmten minimalen Teilkörper $K_0 \subseteq K$, den **Primkörper**. Wenn $\mathrm{char}(K) = 0$ gilt, ist $K_0 \cong \mathbb{Q}$ und wenn $\mathrm{char}(K) = l > 0$ gilt, ist $K_0 = c(\mathbb{Z}) \cong \mathbb{Z}/l\mathbb{Z}$.

Beis Sei $K_0 = \bigcap \{ L \subseteq K \mid L \text{ Teilkörper} \}$, dann ist $K_0 \subseteq K$ ein Teilkörper nach §5.2. Wegen $1_K \in K_0$ folgt $c(\mathbb{Z}) \subseteq K_0$. Wenn $l > 0$ ist $c(\mathbb{Z}) \cong \mathbb{Z}/l\mathbb{Z}$ ein Teilkörper, also $c(\mathbb{Z}) \supseteq K_0$, also $c(\mathbb{Z}) = K_0$.

Ist $\mathrm{char}(K) = 0$, so ist c injektiv, nach §3.11
Existiert ein (ein deutiger) Homomorphismus $\tilde{c}: \mathrm{Quot}(\mathbb{Z}) = \mathbb{Q} \to K_0$

$$\begin{array}{ccc} \mathbb{Z} & \xrightarrow{c} & K_0 \subseteq K \\ \hookrightarrow \mathbb{Q} & \nearrow_{\tilde{c}} & \end{array}$$

. Da $\tilde{c}$ injektiv ist, ist
$\tilde{c}(\mathbb{Q}) \subseteq K_0$ Teilkörper
$\Rightarrow \tilde{c}(\mathbb{Q}) = K_0$ □

4. Erinnerung an LA II, § 5.1: Der "verallgemeinerte Einsetzungshomomorphismus". Seien R, S kommutative Ringe, $\varphi: R \to S$ ein Ringhomomorphismus. Sei $a \in S$.
Definiere $\Phi_a: R[T] \to S$ durch

$$\Phi_a(\underbrace{r_0 + r_1 T + \ldots + r_n T^n}_{= f}) = \varphi(r_0) + \varphi(r_1)\cdot a + \ldots + \varphi(r_n) a^n$$

Das ist ein Ringhomomorphismus, der Einsetzungshomomorphismus. Für $R = S$ und $\varphi = \mathrm{id}_R$ schreibt $f(a) = \Phi_a(f)$.

5. Sei $K \subseteq L$ ein Teilkörper des Körpers L.
Dann nennt man L eine Körpererweiterung von K.
Bsp $\mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$ sind Körpererweiterungen.

Sei nun $u \in L$, betrachte $\Phi_u: K[T] \to L$.
(1.) Möglichkeit Φ_u ist injektiv. Dann heißt u transzendent über K. Es gibt dann kein Polynom $f \neq 0$ in $K[T]$ mit $\Phi_u(f) = f(u) = 0$, u erfüllt keine algebraische Gleichung über K. Bsp: $e = 2.71828\ldots = \exp(1)$ und $\pi = 3.14159\ldots$ sind transzendent über $\mathbb{Q}$. (!)

Der kleinste Teilkörper von L, der K und u enthält, ist dann isomorph zu $K(T) = \mathrm{Quot}(K[T])$
$= \left\{ \frac{f}{g} \mid f, g \in K[T], g \neq 0 \right\}$, dem Körper der rationalen Funktionen auf K, denn wir haben nach § 3.11

$$\begin{array}{ccc} K[T] & \xrightarrow{\Phi_u} & L \\ \downarrow & \nearrow \text{inj} & \\ K(T) & & \end{array}$$

Man schibt $K(u) = \left\{ \frac{f(u)}{g(u)} \in L \mid f, g \in K[T], g \neq 0 \right\} \cong K(T)$

(2.) Möglichkeit $\Phi_u : K[T] \to L$ ist nicht injektiv, es gibt $f \neq 0$, $f \in K[T]$ mit $\Phi_u(f) = f(u) = 0$. Nach § 4.12 ist $K[T]$ ein Hauptidealbereich, also gibt es ein Polynom $\mu \in K[T]$ mit $\ker(\Phi_u) = (\mu) \subseteq K[T]$. Es gilt $\deg(\mu) \geq 1$ (denn für $f \in K[T]$ mit $\deg(f) = 0$ gilt $\Phi_u(f) \neq 0$). Bis auf Multiplikation mit Skalaren $\alpha \in K^*$ ist μ eindeutig bestimmt (*), wir dürfen annehmen, dass $\mu = \mu_u = r_0 + \cdots r_{n-1} T^{n-1} + T^n$ und $\deg(\mu) = n \geq 1$ Leit koeffizient ist 1

(*) § 4.1

Man nennt $\mu = \mu_u = r_0 + \dots + T^n$ das Minimalpolynom von u über K und nennt u algebraisch über K.

Da L ein Integritätsbereich ist, ist (μ) ein Primideal in $K[T]$, und da $\deg(\mu) \geq 1$ ist $(\mu) \neq K[T]$. Also ist (μ) nach § 4.5 ein maximales Ideal und damit ist $K[T]/(\mu) \cong \Phi_u(K[T]) \subseteq L$ ein Körper, der kleinste Teilkörper von L, der $K \cup \{u\}$ enthält. Man schreibt kurz

$$K[u] = \{ f(u) \mid f \in K[T] \} \subseteq L$$

und nennt u einen primitiven Erzeuger von $K[u]$.

Bsp $K = \mathbb{Q}$, $L = \mathbb{R}$, $u = \sqrt{2} \notin \mathbb{Q}$. Es gilt $f(u) = 0$ für $f = T^2 - 2$ und $\deg(f) = 2$, also ist $\mu = f$ das Minimalpolynom von u.

Es folgt, dass $\mathbb{Q}[\sqrt{2}] \subseteq \mathbb{R}$ ein Teilkörper ist.

In beiden Fällen (1) und (2) schreibt man

$$K(u) = \bigcap \{ \Pi \subseteq L \text{ Teilkörper} \mid K \cup \{u\} \subseteq \Pi \},$$

u algebraisch $\Rightarrow K(u) = K[u]$

u transzendent $\Rightarrow K(u) = \left\{ \frac{f(u)}{g(u)} \mid f, g \in K[T], g \neq 0 \right\}$

6. Def Sei $K \subseteq L$ ein Körpererweiterung. Dann ist L ein K-Vektorraum: $(L,+)$ ist abelsche Gruppe, für $v \in L$ und $a \in K$ ist $va \in L$ und die Vektorraumaxiome gelten alle. Man nennt die Dimension von L als K-Vektorraum den Grad der Körpererweiterung und schreibt

$$[L:K] = \dim_K L$$

↑ wichtig: $K \subseteq L$ mit angeben!

Satz Sei $K \subseteq L$ Körpererweiterung, sei $u \in L$, $n \in \mathbb{N}$.

Dann sind äquivalent:

(i) u ist algebraisch über K mit Minimalpolynom μ und $\deg(\mu) = n$.

(ii) $[K(u):K] = n < \infty$

Beis (i) $\Rightarrow$ (ii) Sei $g \in K[T]$ beliebig $\Rightarrow g = q \cdot \mu + r$ mit $q, r \in K[T]$, $\deg(r) < n = \deg(\mu)$, vgl § 4.11.

Es folgt $g(u) = \underbrace{\mu(u)}_{=0} \cdot q(u) + r(u) = r(u)$, also

$K[u] = \{ r_0 + r_1 u + r_2 u^2 + \dots + r_{n-1} u^{n-1} \mid r_0, \dots, r_{n-1} \in K \}$

$\Rightarrow \dim_K K[u] \leq n$, denn $\{1, u, u^2, \dots u^{n-1}\}$ ist ein lineares Erzeugendensystem von $K[u]$. Dieses EzS ist linear unabhängig:

$$r_0 1 + r_1 u + \dots + r_{n-1} u^{n-1} = 0 \Rightarrow f = r_0 + r_1 T + \dots + r_{n-1} T^{n-1}$$

$f \in (\mu)$ aber $\deg(f) < \deg(\mu) \Rightarrow f = 0$

Also ist $\{1, u, \dots, u^{n-1}\}$ ein Basis von $K[u]$ als K-Vektorraum.

(ii) $\Rightarrow$ (i) Angenommen, u ist transzendent über K.

Dann gilt $g(u) \neq 0$ für alle $g \neq 0$, $g \in K[T]$.

Folglich ist die unendliche Menge

$\{1, u, u^2, u^3, \dots\}$ linear unabhängig über K

$\Rightarrow \dim_K K(u)$ ist nicht endlich. □

7. Satz Seien $K \subseteq L \subseteq M$ Körpererweiterungen.

Dann gilt $[M:K] = n < \infty$ genau dann, wenn

$[M:L] = \ell < \infty$ und $[L:K] = k < \infty$, mit $n = k \cdot \ell$,

$$[M:K] = [M:L] \cdot [L:K]$$

Beweis: Ist $\dim_K(M) = n$, so folgt $\dim_K(L) = \ell < \infty$,

da $L \subseteq M$ ein Unterraum ist. Sei $u_1, \dots, u_n \in M$

eine Basis für M über K, so ist $u_1, \dots, u_n$ ein

Erzeugendensystem für M über L, also $\dim_L(M) \leq n$.

Sei nun $v_1, \dots, v_\ell \in M$ eine Basis für M über L

$w_1, \dots, w_k \in L$ eine Basis für L über K.

Sei $x \in M$, $x = \sum_{j=1}^{\ell} v_j x_j$ mit $x_j \in L$.

Schon $x_j = \sum_{i=1}^{k} w_i \xi_{ij}$ mit $\xi_{ij} \in K$

$\Rightarrow x = \sum_{i,j} v_j w_i \xi_{ij}$, also ist die Menge

$\{ v_j w_i \mid 1 \leq j \leq \ell, 1 \leq i \leq k \}$ ein Erzeugendensystem

für M über K und $[M:K] \leq \underbrace{[M:L]}_{=\ell} \cdot \underbrace{[L:K]}_{=k}$

Beh diese Menge $\{v_j w_i \mid i,j \dots\}$ ist linear unabhängig über K. Dann angenommen, $\xi_{ij} \in K$ mit

$$\sum_{i,j} v_j \underbrace{w_i \xi_{ij}}_{\in L} = 0 \quad \Rightarrow \quad \sum_i w_i \xi_{ij} = 0 \quad \Rightarrow \quad \xi_{ij} = 0$$

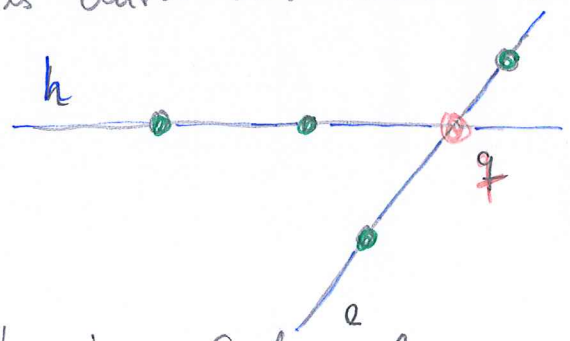
$\uparrow$ $\{v_j\}$ Basis; $\uparrow$ $\{w_i\}$ Basis

Also $n = k \cdot l$. □ #

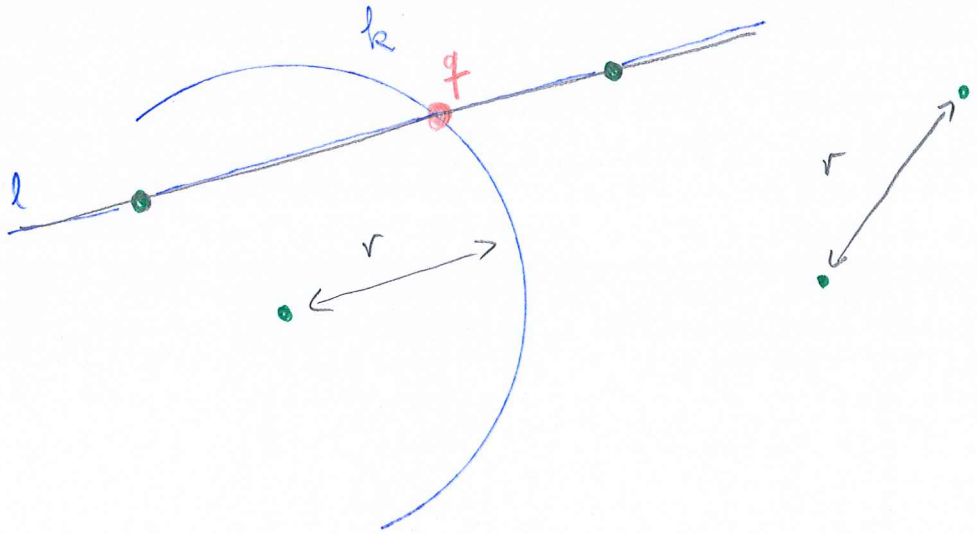
8. Konstruierbarkeit mit Zirkel und Lineal

Gegeben sei eine endliche Menge von Punkten $S = \{P_1, \dots, P_n\} \subseteq \mathbb{R}^2$ in der Ebene. Ein Punkt $q \in \mathbb{R}^2$ heißt elementar konstruierbar aus S, wenn q von den folgenden Typen ist

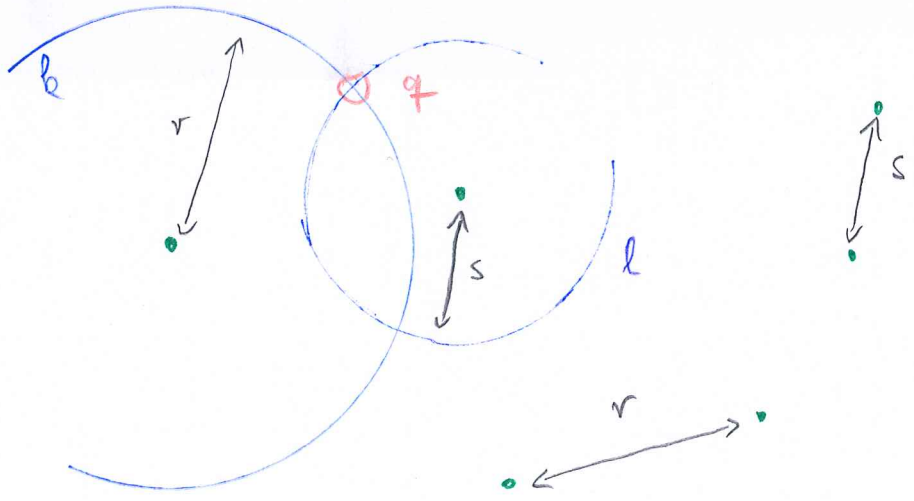
(a) q ist Schnittpunkt zweier Geraden h, l, wobei h und l jeweils durch zwei Punkte in S gehen



(b) q ist Schnittpunkt einer Geraden l, die durch zwei Punkte in S geht mit einem Kreis k, dessen Mittelpunkt in S ist und dessen Radius der Abstand zweier Punkte in S ist (Abstand heißt: euklidischer Abstand, $p = (x,y)$ $p' = (x',y')$ $d(p,p') = \left((x-x')^2 + (y-y')^2\right)^{1/2}$)



(c) q ist Schnittpunkt zweier Kreise k, l, deren Mittelpunkte in S sind und deren Radien Abstände von Punkten in S sind



Setze nun $S = S_0$ und

$$S_{j+1} := S_j \cup \{ q \in \mathbb{R}^2 \mid q \text{ aus } S_j \text{ elementar konstruierbar} \}$$

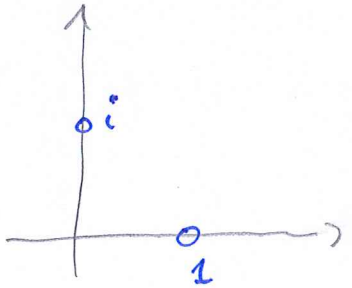
sowie $\mathcal{K}(S) = \bigcup_{j \geq 0} S_j$. Die Punkte in $\mathcal{K}(S)$ ist die Menge aller aus S in endlich vielen Schritten mit Zirkel und Lineal konstruierbaren Punkte.

Ist $S = \emptyset$, so ist $S_j = \emptyset$ für alle j und $\mathcal{K}(S) = \emptyset$.
Ist $S = \{p\}$, so ist $S_j = \{p\}$ für alle j und $\mathcal{K}(S) = \{p\}$,
diese beiden Fälle sind uninteressant.

Beobachtung: Verschiebungen, Drehungen und zentrische Streckungen von $\mathbb{R}^2$ überführen Kreise in Kreise und Geraden in Geraden. Wenn also $\#S \geq 2$ gilt, dann dürfen wir annehmen, dass die Punkte $(0,0)$ und $(1,0)$ in S liegen, indem wir S geeignet verschieben, drehen und strecken; die ganze Menge $\mathcal{K}(S)$ wird dann auch verschoben, gedreht und gestreckt.

9. Erinnerung: Die komplexen Zahlen $\mathbb{C} = \mathbb{R}^2$, setze

$1 = (1,0)$ und $i = (0,1)$



Jede komplexe Zahl $z \in \mathbb{C}$
ist von der Form

$z = (u,v) = u \cdot 1 + v \cdot i$

$u, v \in \mathbb{R}$. Die Addition ist die Addition im $\mathbb{R}$-Vektorraum $\mathbb{R}^2$, die Multiplikation ist erklärt durch

$z = (u,v) = u1 + v \cdot i \qquad u, v, x, y \in \mathbb{R}$

$w = (x,y) = x \cdot 1 + y \cdot i$

$$z \cdot w = (u \cdot 1 + v \cdot i) \cdot (x \cdot 1 + y \cdot i) = (ux - vy) \cdot 1 + (uy + vx) \cdot i$$

Damit ist $\mathbb{C}$ ein Körper, der $\mathbb{R}$ als Teilkörper enthält via $r \mapsto r \cdot 1 + 0 \cdot i \qquad r \in \mathbb{R}$

Es gilt $i^2 = -1$, vgl LA I §3.18

Ist $z = u1 + vi \in \mathbb{C}$, $u, v \in \mathbb{R}$, so setzt man

$\mathrm{Re}(z) = u$ Realteil von z

$\mathrm{Im}(z) = v$ Imaginärteil von z

$\overline{z} = u \cdot 1 - v \cdot i$ komplex Konjugiertes von z.

Nachrechnen zeigt: $\overline{z \cdot w} = \overline{z} \cdot \overline{w}$, $\overline{z + w} = \overline{z} + \overline{w}$, $\overline{\overline{z}} = z$

$\overline{1} = 1$

also ist die Abbildung

$$\mathbb{C} \to \mathbb{C}, \quad z \mapsto \overline{z}$$

ein Automorphismus des Körpers $\mathbb{C}$.

Beachte auch: $z \cdot \overline{z} = (u^2 + v^2) \cdot 1_{\mathbb{R}} \in \mathbb{R} \subseteq \mathbb{C}$. Der Absolutbetrag von z wird definiert als $|z| = \sqrt{z\overline{z}} \in \mathbb{R}_{\geq 0}$.

10. Sei nun $S \subseteq \mathbb{R}^2$ endlich. Wir identifizieren $\mathbb{R}^2$ mit $\mathbb{C}$ und betrachten S als Teilmenge des Körpers $\mathbb{C}$.

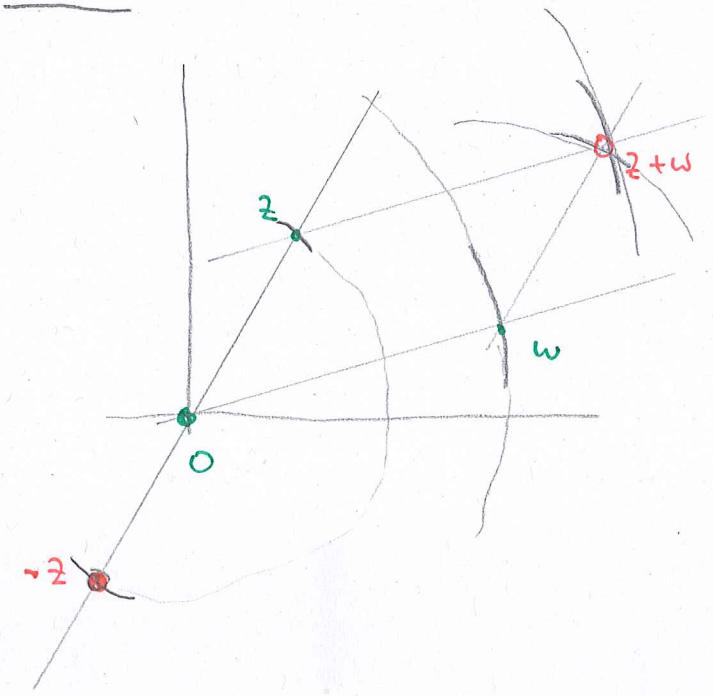
Satz Sei $S \subseteq \mathbb{C}$ endlich mit $0, 1 \in S$.

Dann ist $\mathcal{K}(S) \subseteq \mathbb{C}$ ein Teilkörper. Für alle $z \in \mathbb{C}$ gilt folgendes:

(i) $z \in \mathcal{K}(S) \Leftrightarrow \overline{z} \in \mathcal{K}(S)$

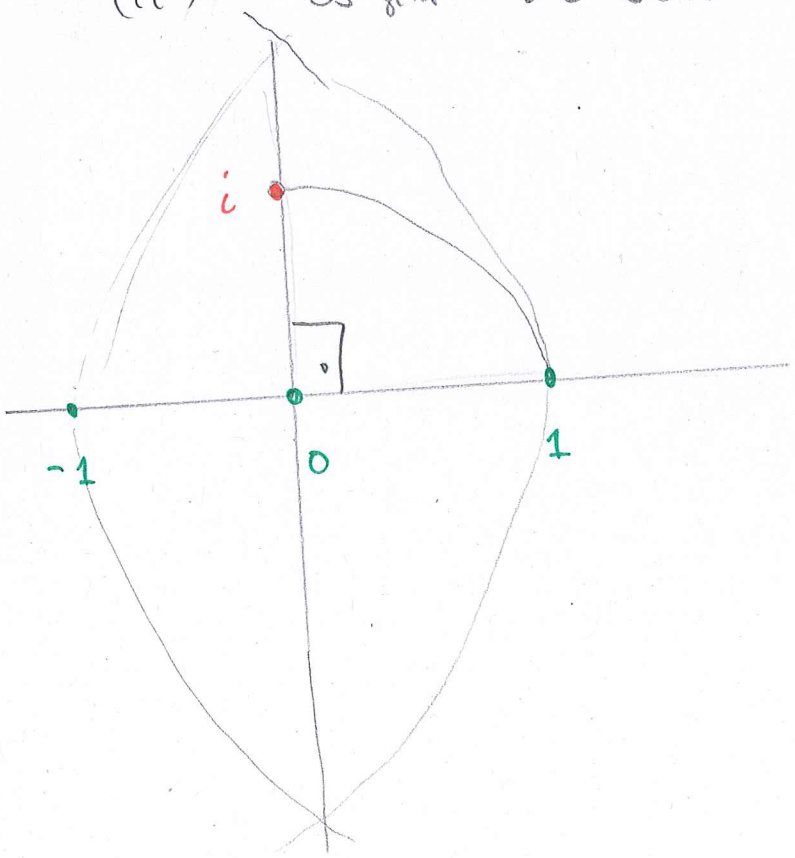
(ii) $z^2 \in \mathcal{K}(S) \Leftrightarrow z \in \mathcal{K}(S)$

Beweis (i) $J\kappa(S)$ ist Gruppe bzgl $+$.

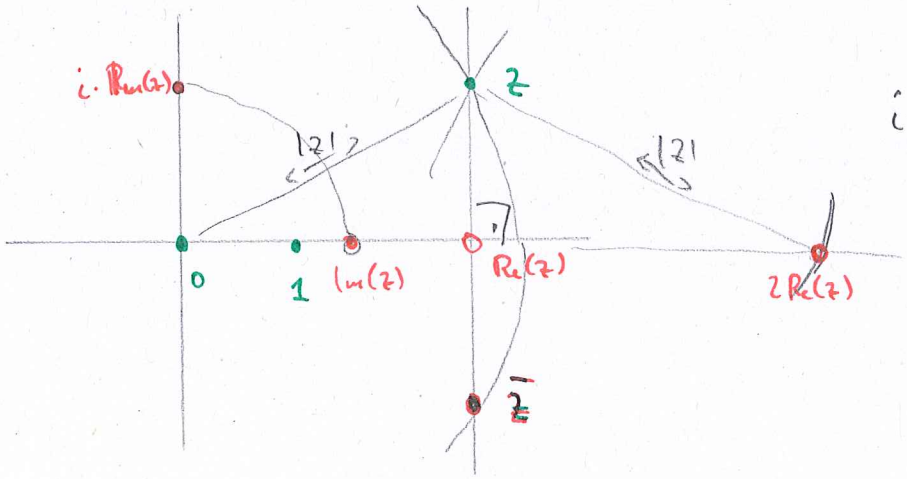


sei $z, w \in J\kappa(S)$

(ii) Es gilt $i \in J\kappa(S)$

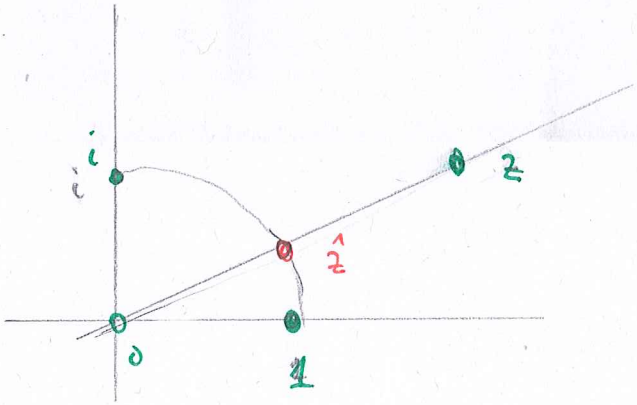


(iii) $z \in \mathcal{JK}(S) \Rightarrow \mathrm{Re}(z), \mathrm{Im}(z), \bar{z} \in \mathcal{JK}(S)$

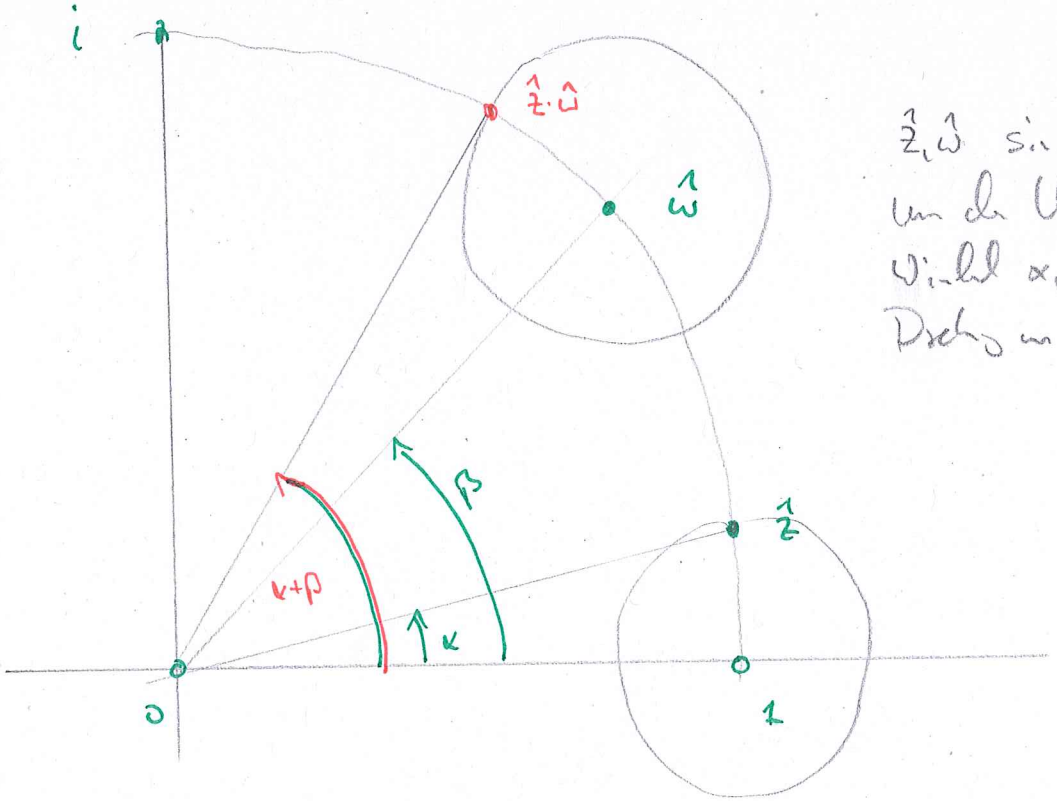


i. $\mathrm{Im}\, z = z - \mathrm{Re}(z) \in \mathcal{JK}(S)$

(iv) $z \in \mathcal{JK}(S), z \neq 0 \Rightarrow \hat{z} = \frac{z}{|z|} \in \mathcal{JK}(S)$



(v) $z, w \in \mathcal{JK}(S), z, w \neq 0 \Rightarrow \hat{z} \cdot \hat{w} \in \mathcal{JK}(S)$

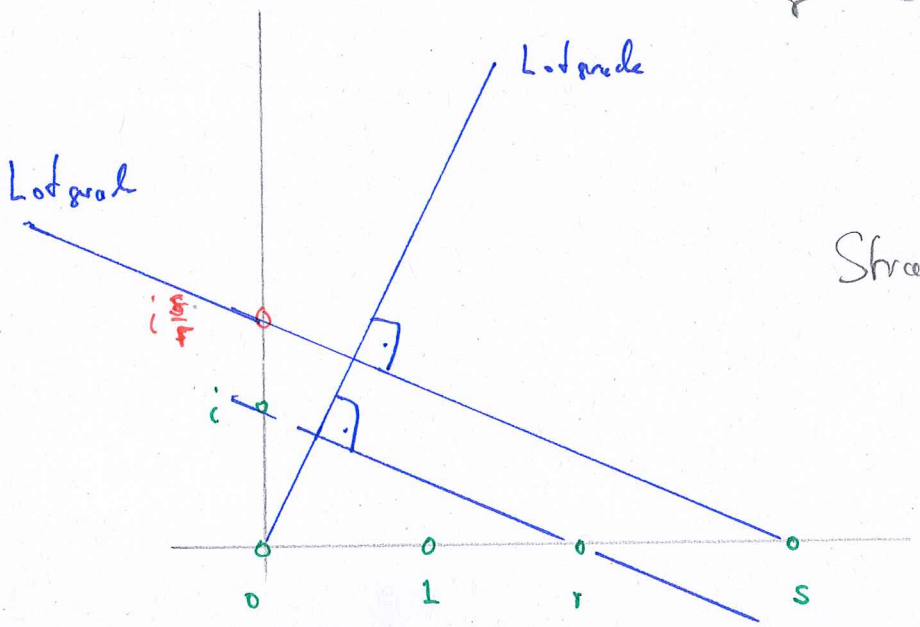


$\hat{z}, \hat{w}$ sind Drehungen um den Ursprung um Winkel $\alpha, \beta \Rightarrow \hat{z} \cdot \hat{w}$ Drehung um Winkel $\alpha + \beta$.

#

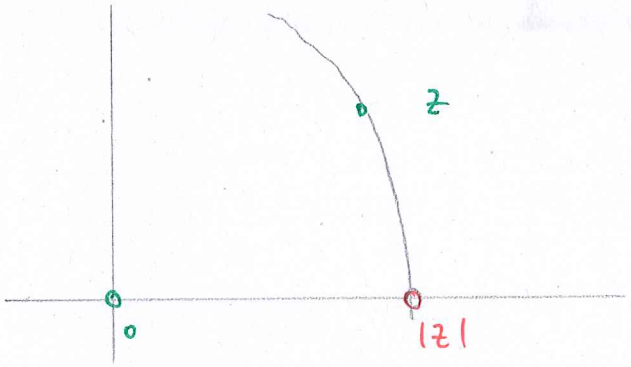
$r, s \neq 0$

(vi) $r, s \in \mathcal{K}(S) \cap \mathbb{R} \Rightarrow \frac{s}{r} \in \mathcal{K}(S)$

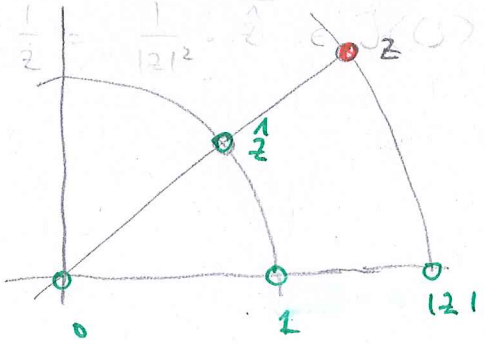


Strahlsatz!

(vii) $z \in \mathcal{K}(S)$, $z \neq 0 \Rightarrow |z| \in \mathcal{K}(S)$



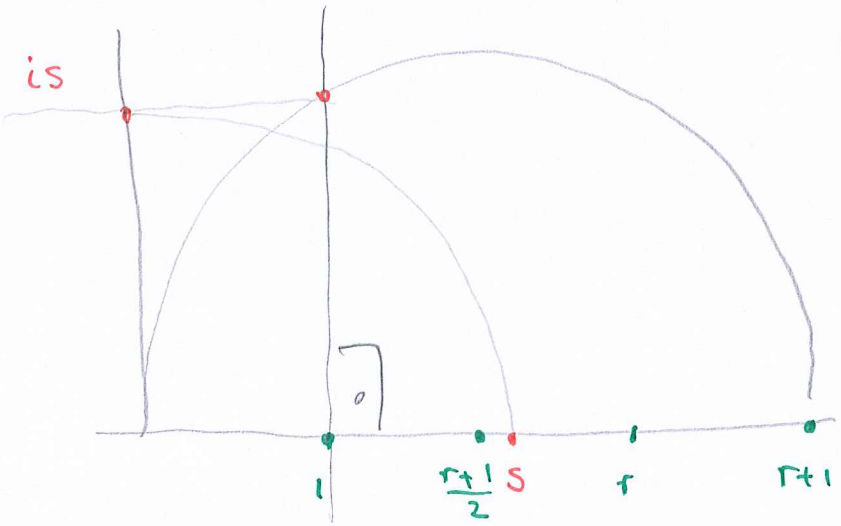
(viii) $z \neq 0$, $\frac{1}{z}, |z| \in \mathcal{K}(S) \Rightarrow z \in \mathcal{K}(S)$



Es folgt: ist $z, w \in \mathcal{K}(S)$, $z, w \neq 0$, so auch $z \cdot w = \frac{1}{\bar{z}} \cdot \frac{1}{\bar{w}} \cdot |z| \cdot |w| \in \mathcal{K}(S)$

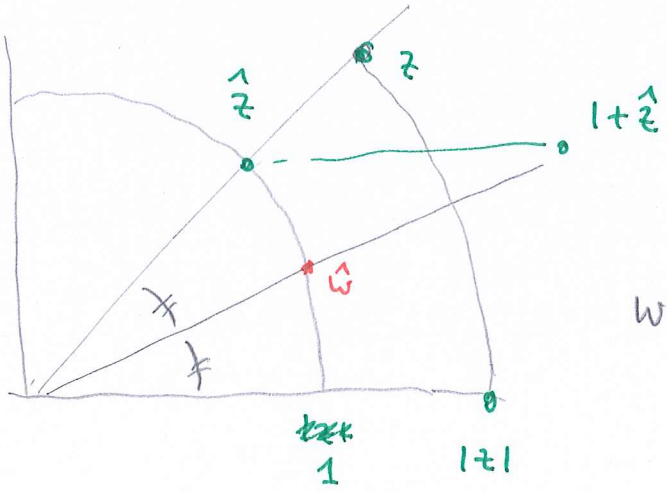
Sowie $\frac{1}{z} = \frac{1}{\bar{z}} \cdot \frac{1}{|z|} \in \mathcal{K}(S)$, also ist $\mathcal{K}(S)$ ein Körper.

(ix) $r \in \mathcal{K}(S) \cap \mathbb{R}$, $r > 0 \Rightarrow \sqrt{r} \in \mathcal{K}(S)$



2x Pythagoras $\Rightarrow$ $s^2 = r$, $s \in \mathcal{K}(S)$

(x) $z \in \mathcal{K}(S)$, $z = w^2 \neq 0 \Rightarrow w \in \mathcal{K}(S)$



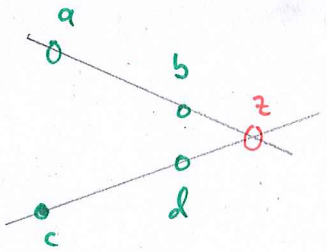
$w = \pm \hat{w} \cdot \sqrt{|z|}$

11. **Lemma A** Sei $K \subseteq L$ ein Körpererweiterung, sei $u \in L$ mit $u^2 \in K$. Dann gilt $[K(u):K] \leq 2$.

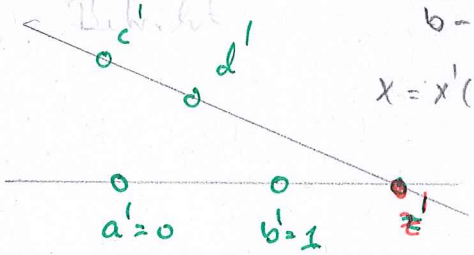
Beis. u ist algebraisch über K, denn $T^2 - u^2 \in K[T]$ hat u als Nullstelle $\Rightarrow \deg(\mu_u) \leq 2$, vgl. § 5.6 □

Lemma B Sei $K \subseteq \mathbb{C}$ ein Teilkörper mit folgender Eigenschaft: $x \in K \Rightarrow \bar{x} \in K$. Ist $z \in \mathbb{C}$ mit einer der die Konstruktionsverfahren aus § 5.8 aus K konstruierbar, so gibt es $w \in \mathbb{C}$ mit $w^2 \in K$ und $z \in K(w)$.

Beis. (a)



Betrachte $x \mapsto x' = \frac{(x-a)}{b-a}$



$x = x'(b-a) + a$

$z' = c' + (d'-c') \cdot t \in \mathbb{R} \qquad t \in \mathbb{R}$

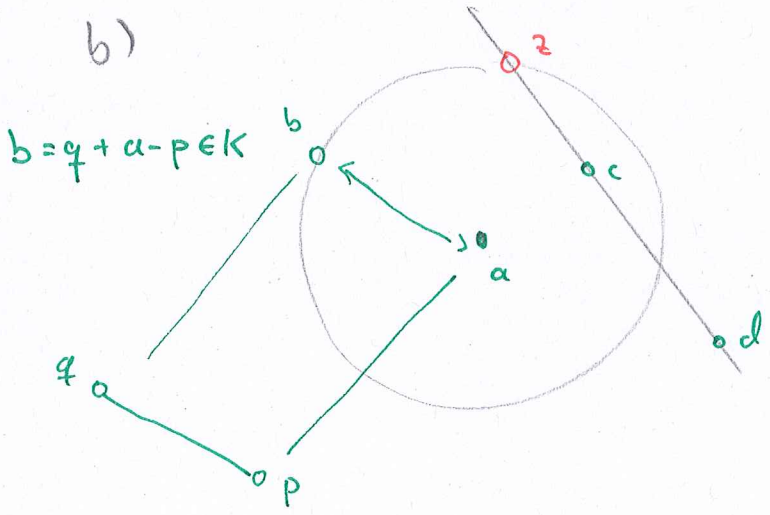
$\Rightarrow \operatorname{Im}(c' + d't - c't) = 0$

$= \underbrace{\operatorname{Im}(c')}_{=\alpha} + \underbrace{\operatorname{Im}(d'-c')}_{=\beta} \cdot t = 0 \Rightarrow t = -\alpha/\beta$

$i \cdot \operatorname{Im}(x) = \frac{1}{2}(x - \bar{x}) \in K \Rightarrow t = \frac{-i\alpha}{i\beta} \in K \Rightarrow z' \in K$

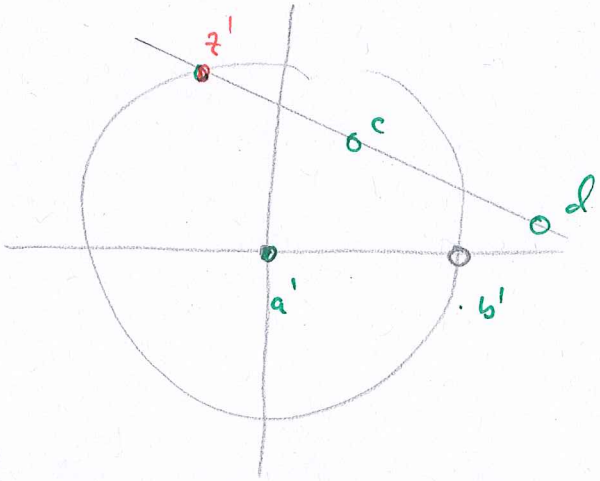
$\Rightarrow z \in K$

b)



$b = q + a - p \in K$

$x' = (x-a)\frac{1}{b}$



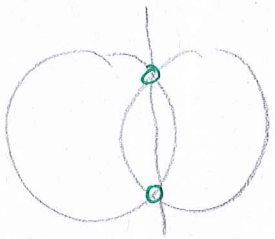
$z' = d' + t(c'-d') \qquad t \in \mathbb{R}$

$|z'|^2 = 1 = \underbrace{|d'|^2}_{\in K} + t^2 \underbrace{|c'-d'|^2}_{\in K} + \underbrace{2\,\mathrm{Re}(\overline{d'}(c'-d'))}_{\in K} t$

$\rightsquigarrow$ quadratische Gleichung für t, $t = \alpha \pm \sqrt{\delta}$ $\quad \alpha, \delta \in K \cap \mathbb{R}$

$\rightsquigarrow t \in K(\delta) \rightsquigarrow z' \in K(\delta) \rightsquigarrow z \in K(\delta)$

(c)



führt auch auf eine quadratische Gleichung.

□

12. <u>Notation</u> Sei $K \subseteq L$ ein Körpererweiterung.

Erinnerung: für $u \in L$ ist $K(u)$ der kleinste Teilkörper von L, der $K \cup \{u\}$ enthält, vgl §5.5.

Für $u_1, \dots, u_n \in L$ setze

$K(u_1, \dots, u_m) = K(u_1)(u_2)(\dots)(u_n)$, das ist der kleinste Teilkörper von L, der $K \cup \{u_1, \dots, u_m\}$ enthält.

13. Satz Sei $S = \{0, 1, P_1, \dots, P_m\} \subseteq \mathbb{C}$,

sei $K = \mathbb{Q}(P_1, \bar{P}_1, P_2, \bar{P}_2, \dots, P_m, \bar{P}_m) \subseteq \mathcal{K}(S) \subseteq \mathbb{C}$.

Sei $q \in \mathcal{K}(S)$. Dann gibt es Teilkörper

$K = K_0 \subseteq K_1 \subseteq \dots \subseteq K_n \subseteq \mathcal{K}(S)$ mit $q \in K_n$

und $[K_{j+1} : K_j] = 2$, also $[K_n : K] = 2^n$. #

Beweis Die Elemente von K sind Linearkombinationen von Potenzen der $P_j, \bar{P}_j$, also gilt für alle $x \in K$, dass $\bar{x} \in K$.

Wir benutzen die Notation aus §5.5: S_{j+1} entsteht aus S_j durch Hinzunahme aller Punkte, die durch die Verfahren (a), (b), (c) aus S_j mit Zirkel und Lineal konstruierbar sind, mit $S_0 = S$.

Sei $q \in S_1$. Dann gibt es nach §5.11 ein $\omega \in \mathbb{C}$ mit $\omega^2 \in K$ und $q \in K(\omega)$. Weiter ist $[K(\omega) : K] \leq 2$ und $\bar{\omega}^2 \in K \subseteq K(\omega)$ $\Rightarrow$ [illegible] $\omega, \bar{\omega} \in \mathcal{K}(S)$

$$\Rightarrow [K(\omega, \bar{\omega}) : K] = \underbrace{[K(\omega, \bar{\omega}) : K(\omega)]}_{\leq 2} \cdot \underbrace{[K(\omega) : K]}_{\leq 2} \in \{1, 2, 4\}$$

Ist also $S_1 = S_0 \cup \{q_1, \dots, q_r\}$

So gibt es $w_1, \dots, w_r \in \mathbb{C}$ mit $w_j^2 \in K$

$S_1 \subseteq K(w_1, \bar{w}_1, w_2, \bar{w}_2, \dots, w_r, \bar{w}_r) = K' \subseteq \mathcal{K}(S)$

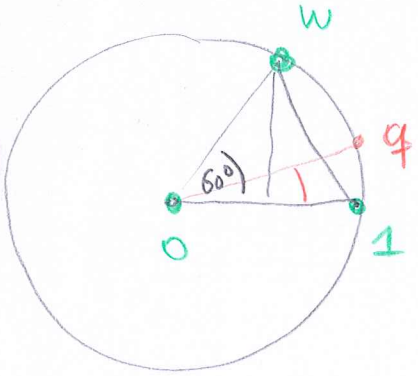
$K \subseteq K(w_1) \subseteq K(w_1, \bar{w}_1) \subseteq K(w_1, \bar{w}_1, w_2) \subseteq \dots \subseteq K'$

und $[K' : K]$ ist Zweierpotenz und $S_1 \subseteq K'$.

Jetzt weiter mit S_2 und K' usw. Beh. □

14. Satz Ausgehend von der Menge $S = \{0, 1\}$ ist die Dreiteilung des Winkels $60° = \frac{\pi}{3}$ nicht mit Zirkel und Lineal möglich.

Beweis



$w = \frac{1}{2} + i\frac{\sqrt{3}}{2}$

$q^3 = w$

$q = \cos(20°) + i \sin(20°)$

$= u + iv$ $\qquad u^2 + v^2 = 1$

$q^3 = (u+iv)^3$ $\qquad v^2 = 1 - u^2$

$$\mathrm{Re}(q^3) = \frac{1}{2} = \mathrm{Re}\left((u+iv)(u^2 - v^2 + 2iuv)\right)$$

$$= u^3 - uv^2 - 2uv^2$$

$$= u^3 - u(1-u^2) - 2u(1-u^2)$$

$$= u^3 - u + u^3 - 2u + 2u^3$$

$$= 4u^3 - 3u$$

Wenn q konstruierbar ist, so auch $u = \mathrm{Re}(q)$.

Für das Minimalpolynom von $2u$ über $\mathbb{Q}$ gilt

wegen $(2u)^3 - 3\cdot(2u) - 1 = 0$, dass

$\mu_{2u} \mid T^3 - 3T - 1$

Beh: $T^3 - 3T - 1 \in \mathbb{Z}[T]$ ist irreduzibel in $\mathbb{Z}[T]$, also auch in $\mathbb{Q}[T]$.

Beweis: $T^3 - 3T - 1 = (\alpha T + \beta)(\gamma T^2 + \delta T + \varepsilon)$

$\alpha, \beta, \gamma, \delta, \varepsilon \in \mathbb{Z}$ $\quad 1 = \alpha \cdot \gamma$ OE $\alpha = 1$

$-1 = \beta \cdot \varepsilon \Rightarrow \beta = \pm 1$ Nullstelle von f □

aber $f(1) \neq 0 \neq f(-1)$ ↯

Es folgt $\mu_{2u} = T^3 - 3 - 1$, also $[\mathbb{Q}(2u), \mathbb{Q}] = 3$.

Wäre $u \in K(\{0,1\})$, so wäre $2u \in K$ mit

$[K : \mathbb{Q}] = 2^\ell$, aber $[L : \mathbb{Q}] = [L : \mathbb{Q}(2u)] \cdot \underbrace{[\mathbb{Q}(2u) : \mathbb{Q}]}_{=3}$ ↯

15. Bem Wir hab im vorig Beweis folgd nützlich Hilfsmittel bewiesen.

(A) Ist R faktoriell und $f \in R[T]$ irreduzibel, so ist f irreduzibel in $Q[T]$ für $Q = Quot(R)$. (vgl §4.15)

(B) Sei $f = aT^3 + bT^2 + cT + d \in R[T]$ und $a = 1$ und sei R faktoriell. Wenn f reduzibel ist, so gibt es einen Teiler von d, der Nullstelle von f ist.

Denn: $f = (\alpha T + \beta)(\gamma T^2 + \delta T + \varepsilon)$ (f primitiv!)

$\Rightarrow \alpha\gamma = 1$ OE $\alpha = 1$ und $f(-\beta) = 0$ und

$d = \beta \cdot \varepsilon$

(c) Ist $K \subseteq L$ Körpererweiterung mit $m = [L:K]$, ist $u \in L$ mit Minimalpolynom μ_u über K, so gilt $\deg(\mu_u) \mid m$. Denn

$$m = [L:K] = [L:K(u)] \cdot \underbrace{[K(u):K]}_{= \deg \mu_u}$$

16. Das Delische Problem ist mit Zirkel und Lineal nicht lösbar.

Die Pest wütete in Delos... Aufgabe: einen Würfel zu konstruieren, dessen Volumen 2 ist.

Satz $\sqrt[3]{2} \notin K(\{0,1\})$, die Zahl $\sqrt[3]{2}$ ist nicht mit Zirkel und Lineal aus $\{0,1\}$ konstruierbar.

Beweis $u = \sqrt[3]{2}$ ist Nullstelle von $T^3 - 2 = f$

Da $\pm 1, \pm 2$ hier Nullstellen von f sind und f primitiv in $\mathbb{Z}[T]$ ist, ist f irreduzibel, also

$$\mu_u = T^3 - 2 \rightsquigarrow [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$$

$$\Rightarrow \sqrt[3]{2} \notin K(\{0,1\}) \qquad \square$$

Wie kann man Irreduzibilität von Polynomen in $\mathbb{Z}[T]$ prüfen?

Vorsicht: Kriterium § 5.15 (B) greift nur bei Polynomen vom Grad ≤ 3 !!

Bsp $f = (T^2+1)^2$ ist primitiv in $\mathbb{Z}[T]$, hat keine Nullstelle in $\mathbb{Z}, \mathbb{Q}$ oder $\mathbb{R}$, ist aber reduzibel!

17. Satz (Eisensteins Kriterium) Sei R faktoriell, sei $p \in R$ prim und sei $f = a_n T^n + \dots + a_0 \in R[T]$ primitiv und vom Grad $n \geq 1$.

Falls gilt: $p \mid a_j$ für $j = 0,1,2,\dots n-1$

$p \nmid a_n$ und $p^2 \nmid a_0$

so ist f irreduzibel.

Beweis Angenommen, $f = g \cdot h$ $\deg(g), \deg(h) \geq 1$

$g = b_k T^k + \dots + b_0$ $h = c_\ell T^\ell + \dots + c_0$

$a_0 = b_0 c_0$ $p \mid a_0$ o.E. $p \mid b_0$. Da $p^2 \nmid a_0$ folgt $p \nmid c_0$. Sei m minimal mit $p \nmid b_m$ (also $p \mid b_0, p \mid b_1, \dots, p \mid b_{m-1}$)

Da g primitiv ist, gilt $m \leq k$.

$$a_m = \underbrace{b_0 c_m + b_1 c_{m-1} + \dots + b_{m-1} c_1}_{\text{wird von } p \text{ geteilt}} + \underbrace{b_m c_0}_{\text{wird nicht von } p \text{ geteilt}}$$

$\Rightarrow p \nmid a_m \Rightarrow m = n \not\downarrow \deg(h) \geq 1$ □

Mit dem Eisenstein-Kriterium folgt z.B. sofort: ist $p \in \mathbb{N}$ ein Primzahl, so ist für $m \geq 1$ das Polynom

$$T^m \pm p \in \mathbb{Z}[T] \quad \text{irreduzibel in } \mathbb{Q}[T]$$ //

18. Substitution Sei R ein kommutativer Ring, sei $u \in R^*$ und $h \in R[T]$.
Für $f = a_n T^n + \dots + a_0 \in R[T]$ schreibe

$$f(uT+h) = a_n (uT+h)^n + \dots + a_0 \in R[T]$$

(substituiere/ersetze T durch $uT+h$)

Die Abbildung

$$f \longmapsto F(uT+h) \qquad R[T] \to R[T]$$

ist ein Ringisomorphismus mit Inversem

$$g \longmapsto g(u^{-1}(T-h))$$

Also gilt: f irreduzibel $\Leftrightarrow$ $F(uT+h)$ irreduzibel.

Eine Anwendung:

19. Lemma Sei $p \in \mathbb{N}$ Primzahl. Dann ist

$$f = T^{p-1} + T^{p-2} + \dots + T + 1 \in \mathbb{Z}[T]$$

irreduzibel.

Beweis $(T-1) \cdot f = T^p - 1$ (geometr. Summe)

Substitution $T \longmapsto T+1$

$$\underbrace{(T+1-1)}_{=T} \cdot \underbrace{f(T+1)}_{=\tilde{f}} = (T+1)^p - 1$$

$$\rightsquigarrow T\cdot\tilde f = \sum_{k=0}^{p}\binom{p}{k}T^k - 1 = \sum_{k=1}^{p}\binom{p}{k}T^k$$

$$\tilde f = T^{p-1} + T^{p-2}\binom{p}{p-1} + \dots + T\binom{p}{2} + \underbrace{\binom{p}{1}}_{=p}$$

$$\binom{p}{k} = \frac{p(p-1)\cdots(p-k+1)}{1\cdot 2\cdots k} \Rightarrow p \mid \binom{p}{k} \text{ für } k = 1,\dots p-1$$

Nach Eisenstein ist $\tilde f$ irreduzibel, also ist f irreduzibel. □

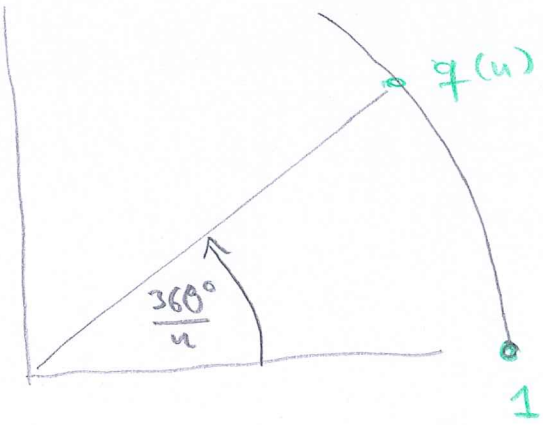
+

20. Konstruktion von regulären n-Ecken mit Zirkel und Lineal.

Sei $n\in\mathbb{N}$, $n\geq 3$. Setze

$$q(n) = \cos\left(\frac{2\pi}{n}\right) + i\cdot\sin\left(\frac{2\pi}{n}\right) \in \mathbb{C}$$

Frage: für welche n gilt $q(n)\in K(\{0,1\})$?



Vorüberlegung: ist l ein Teiler von n, so gilt

$$q(n)^l = q(n/l) \qquad \left(n = k\cdot l \Rightarrow \frac{2\pi}{k} = l\cdot\frac{2\pi}{n}\right)$$

Deswegen untersuchen wir zuerst, für welche

Primzahlen $p\in\mathbb{N}$ gilt $q(p)\in K(\{0,1\})$.

Für $\zeta(p)$ gilt $\zeta(p)^p = 1$, für das Minimalpolynom $\mu_{\zeta(p)}$ von $\zeta(p)$ über $\mathbb{Q}$ gilt also

$$\mu_{\zeta(p)} \mid T^p - 1 = (T-1)(\underbrace{T^{p-1} + \dots + T + 1}_{\text{irreduzibel nach } \S 5.18})$$

Folglich $\mu_{\zeta(p)} = T^{p-1} + \dots + T + 1$

Falls also $\zeta(p) \in K(\zeta_{0,13})$ gilt, so ist $p - 1 = 2^\ell$ für ein $\ell \geq 1$. Solche Primzahlen nennt man

Fermatsche Primzahlen

Lemma Ist $2^\ell + 1$ eine Primzahl, so ist ℓ eine Zweierpotenz.

Beweis Schreibe $\ell = q \cdot u$, q Zweierpotenz, u ungerade ($o.B.d.A. q = 1$)

$$z = 2^q \rightsquigarrow 2^\ell = z^u$$

$$p = (z^u + 1) = 1 - (-z)^u = \underbrace{(1-(-z))}_{= 1 + 2^q \geq 3}\underbrace{((-z)^{u-1} + (-z)^{u-2} + \dots + 1)}_{= \frac{1-(-z)^u}{1-(-z)}}$$

$\uparrow$ u ungerade

$$\Rightarrow 1 = \frac{1-(-z)^u}{1-(-z)} \Rightarrow u = 1 \qquad \square$$

Setze $F_j = 2^{2^j} + 1$. Dann sind

$F_0 = 3$, $F_1 = 2^2 + 1 = 5$, $F_2 = 2^4 + 1 = 17$,

$F_3 = 2^8 + 1 = 257$, $F_4 = 65537$ Primzahlen

Dagegen ist F_5 keine Primzahl – es ist ein offenes Problem, ob es außer F_0, F_1, F_2, F_3, F_4 noch weitere Fermatsche Primzahlen gibt. (!?)

Man kann zeigen: $q(n)$ ist genau dann in $K(\mathbb{Q}, 13)$ (d.h.: das regelmäßige n-Eck ist mit Zirkel und Lineal konstruierbar), wenn gilt

$$n = 2^{\ell} \cdot P_1 \cdot P_2 \cdots P_k \qquad \ell \geq 0$$

$$P_1 < P_2 < P_3 < \ldots < P_k$$ alles Fermatsche Primzahlen

Der Beweis benutzt Galois-Theorie, vgl. Jacobson §4.11

Gauß gab als erster eine Konstruktion eines regelmäßigen 17-Ecks an.

Wir betrachten jetzt transzendente Zahlen und zeigen, dass $e = \exp(1) = \sum_{k=0}^{\infty} \frac{1}{k!}$ nicht algebraisch über $\mathbb{Q}$ ist.

21. Def Sei $K \subseteq L$ ein Körpererweit.

Die algebraische Hülle von K in L ist

$$\mathrm{acl}_L(K) = \{u \in L \mid u \text{ algebraisch über } K\}$$

acl = "algebraic closure"

Satz Ist $K \subseteq L$ eine Körpererweit., so ist $K \subseteq \mathrm{acl}_L(K) \subseteq L$ ein Teilkörper. Es gilt

$$\mathrm{acl}_L(\mathrm{acl}_L(K)) = \mathrm{acl}_L(K).$$

Bew. Sei $u, v \in L^*$ algebraisch über K. Es folgt

$u \pm v, u \cdot v, u/v \in K(u,v)$ und

$$[K(u,v):K] = \underbrace{[K(u,v):K(u)]}_{\text{endlich}} \cdot \underbrace{[K(u):K]}_{\text{endlich}}$$

(weil u,v algebraisch)

Nach üA 11.4 ist jedes Elem von $K(u,v)$ algebraisch über K. Also ist $\mathrm{acl}_L(K) \subseteq L$ Körper.

Sei $K' = \mathrm{acl}_L(K)$ und $u \in \mathrm{acl}_L(K')$.

Dann gibt es $w_1, \dots, w_r \in K'$ mit

$u \in \mathrm{acl}_L K(w_1, \dots, w_r)$

$$[K(u,w_1,\dots,w_r):K] = [K(u,w_1,\dots,w_r):K(w_1,\dots,w_r)] \cdot [K(w_1\dots w_r):K]$$

Beide Faktoren sind endlich $\Rightarrow$ u algebraisch über K nach üA 11.4 $\Rightarrow u \in \mathrm{acl}_L(K)$ □

Eine Vorüberlegung zur Existenz reeller Zahlen, die transzendent über $\mathbb{Q}$ sind. $\mathbb{Q}$ ist abzählbar, jedes Polynom $f \in \mathbb{Q}[T]$ hat endlich viele rationale Koeffizienten, $\mathbb{Q}[T]$ ist abzählbar. Jedes Polynom in $\mathbb{Q}[T]$ hat nur endlich viele Nullstellen (überlegen wir später nochmal!)
$\Rightarrow$ $\mathrm{acl}_{\mathbb{C}}(\mathbb{Q})$ und $\mathrm{alc}_{\mathbb{R}}(\mathbb{Q})$ sind beides abzählbare Körper. Da $\mathbb{R}$ und $\mathbb{C}$ überabzählbar sind, ist "fast jede" reelle oder komplexe Zahl transzendent über $\mathbb{Q}$.

22. Def Für $f = a_n T^n + \dots + a_0 \in \mathbb{R}[T]$ setzen wir $Df = n a_n T^{n-1} + (n-1) a_{n-1} T^{n-2} + \dots + a_1 \in \mathbb{R}[T]$ (formale Ableitung) sowie

$F = (1 + D + D^2 + \dots + D^n) f$ $\quad n = \deg(f)$

(F löst dann formal die DGL $(1-D)F = f$)

Für $F = \frac{1}{n!} T^n \in \mathbb{Q}[T]$ ergibt sich

$$(*) \qquad F = 1 + T + \frac{1}{2} T^2 + \dots + \frac{1}{n!} T^n$$

$$= \sum_{k=0}^{n} \frac{1}{k!} T^k$$

23. Lemma Sei $f = \sum_{k=0}^{n} a_k T^k \in \mathbb{C}[T]$.

Sei $F = (1 + D + D^2 + \dots + D^n) f$. Für jedes $z \in \mathbb{C}$ gilt dann

$$|F(0)\exp(z) - F(z)| \leq \sum_{k=0}^{n} |a_k| \cdot |z|^k \exp(z)$$

Beweis: $|F(0)\exp(z) - F(z)|$

$$= \left| \sum_{k=0}^{n} a_k k! \cdot \sum_{l=0}^{\infty} \frac{z^l}{l!} - \sum_{k=0}^{n} a_k \underbrace{\sum_{l=0}^{k} \frac{k!}{l!} z^l}_{\text{mal } (*)} \right|$$

$$= \left| \sum_{k=0}^{n} a_k \cdot \sum_{l>k} \frac{k!}{l!} z^l \right|$$

$$\leq \sum_{k=0}^{n} \sum_{l>k} |a_k| \frac{k!}{l!} |z|^l$$

$$\leq \sum_{k=0}^{n} \sum_{l>k}^{\infty} |a_k| |z|^k \frac{1}{(l-k)!} |z|^{l-k}$$

$\uparrow$ $\left[\binom{l}{k} = \frac{l!}{k!(l-k)!} \geq 1 \right]$

$$\leq \sum_{k=0}^{n} |a_k| \cdot |z|^k \exp|z|$$

□

24. Sei $p \in \mathbb{N}$ eine Primzahl und sei $n \geq 1$.

Betrachte $f = \frac{1}{(p-1)!} \cdot T^{p-1} \cdot \prod_{k=1}^{n} (k-T)^p \in \mathbb{Q}[T]$

(T^{p-1}: $p-1$ fach Nullstelle; $(k-T)^p$: p-fach Nullstelle)

Es folgt

$$D^m f(\nu) = 0 \quad \text{für } m \leq p-2 \quad \nu = 0, 1, 2, 3, \ldots, n$$

$$D^{p-1} f(\nu) = 0 \quad \text{für } \nu = 1, 2, 3, \ldots n$$

$$D^{p-1} f(0) = \frac{(p-1)!}{(p-1)!} (n!)^p = (n!)^p$$

Für $m \geq p$ hat $D^m f$ ganzzahlige Koeffizienten, die alle von p geteilt werden.

(Das folgt alles mit der Produktregel für Ableitungen.)

Sei $F = (1 + D + D^2 + \ldots + D^N) f \qquad N = \deg(f)$

Es folgt $F(0) \equiv (n!)^p \mod p \quad (\Rightarrow F(0) \neq 0)$

$F(\nu) \equiv 0 \mod p$

Schreibe $f = \sum_{k=1}^{N} a_n T^n$, $a_n \in \mathbb{Q}$.

25. Theorem (Hermite 1873). Die Zahl
$e = \exp(1) \approx 2.71\ldots$ ist transzendent.

Beweis Es genügt, folgendes zu zeigen. Ist
$q_0, \ldots, q_n \in \mathbb{Z}$ mit $q_0 \neq 0$, so ist
$q_0 + q_1 e + q_2 e^2 + \ldots + q_n e^n \neq 0$ [denn
wenn e algebraisch wäre, gäbe es ein Polynom
$F \in \mathbb{Q}[T]$ mit $f(e)=0$, $\deg(f) \geq 1$.
Nach Durchmultiplizieren mit dem Hauptnenner hätte
man $F \in \mathbb{Z}[T]$ mit $f(e)=0$, $\deg(f) \geq 1$
und nach Division durch ein e-Potenz, dass $f(0) \neq 0$]

Sei nun $p \in \mathbb{N}$ Primzahl mit $p > n$ und
$p > |q_0|$. Es folgt (mit den Bezeichnungen aus
§ 5.24) für alle p und n)

$$\sum_{\nu=0}^{n} q_\nu F(\nu) \equiv q_0 \cdot (n!)^p \not\equiv 0 \pmod{p}$$

$$\Rightarrow \quad \sum_{\nu=0}^{n} q_\nu F(\nu) \in \mathbb{Z} - \{0\}$$

Weiter ist $\displaystyle\sum_{\nu=0}^{n} q_\nu F(0) e^\nu = \sum_{\nu=0}^{n} q_\nu F(\nu) + \varepsilon$

und $|\varepsilon| \leq \underbrace{\displaystyle\sum_{\nu=0}^{n} |q_\nu| e^\nu}_{\text{hängt nicht von } p \text{ ab}} \cdot \underbrace{\displaystyle\sum_{k=1}^{N} |a_k| \cdot |\nu^k|}_{\text{hängt von } p \text{ ab}}$

nach § 5.23, mit $f = \displaystyle\sum_{k=1}^{N} a_k T^k$

Nun gilt für jedes ν

$$\sum_{k=1}^{N} |a_k| \cdot |\nu|^k = \sum_{k=1}^{N} |a_k| \nu^k$$

$$\overset{(**)}{\leq} \frac{\nu^{p-1}}{(p-1)!} \prod_{k=1}^{n} (k+\nu)^p$$

$$= \frac{1}{(p-1)!} \underbrace{\prod_{k=1}^{n} (k+\nu)}_{=\alpha} \Big(\nu \underbrace{\prod_{k=1}^{n} (k+\nu)}_{=\beta} \Big)^p$$

$$= \alpha \frac{\beta^p}{(p-1)!}$$

wobei α, β nur von n und ν abhängen, nicht von p.

Für $p \gg 1$ wird $\alpha \frac{\beta^p}{(p-1)!}$ beliebig klein.

Da es beliebig große Primzahlen p gibt, können wir also durch geeignete Wahl von $p \gg 1$ erreichen, dass

$$|\varepsilon| \leq \sum_{\nu=0}^{n} |q_\nu| e^\nu \cdot \alpha \frac{\beta^p}{(p-1)!} < \frac{1}{2}$$

gilt. Da $\sum_{\nu=0}^{n} q_\nu F(\nu) \in \mathbb{Z} - \{0\}$ gilt, folgt

$$F(0) \cdot \sum_{\nu=0}^{n} q_\nu e^\nu \neq 0$$

□

[Zu (**): $(k-T)^p = \sum_{\ell=0}^{p} \binom{p}{\ell} k^{p-\ell} (-1)^\ell T^\ell$

$(k+T)^p = \sum_{\ell=0}^{p} \binom{p}{\ell} k^{p-\ell} T^\ell$

Ausmultiplizieren liefert die Abschätzung.]

Der vorige Beweis stammt aus E. Landaus Zahlentheorie-Buch. Ein etwas anderer Beweis steht bei Jacobson.
(Lindemann 1882)

Korollar Die Zahl e ist nicht mit Zirkel und Lineal aus $\{0,1\}$ konstruierbar.

Bem Mit ähnlicher Methode kann man zeigen, dass $\pi \approx 3.14\ldots$ transzendent über $\mathbb{Q}$ ist.

Der Beweis ist aber dieses erheblich länger (→ Landau) → Jacobson – im Prinzip aber genauso elementar.

Korollar Die "Quadratur des Kreises" mit Zirkel und Lineal ist unmöglich, d.h. man kann aus $\{0,1\}$ mit Zirkel und Lineal kein Quadrat mit Fläche π konstruieren.