a alg. über $K \Rightarrow K[X]/(m_{a,K}(X)) \xrightarrow{\sim} K[a]$

3.3.10 Beispiel: Die reelle Zahl $\omega := 2\cos\frac{\pi}{9}$ ist algebraisch mit $m_{\omega,\mathbb{Q}}(X) = X^3 - 3X - 1$ und $[\mathbb{Q}(\omega)/\mathbb{Q}] = 3$.

Additionstheorem $\Rightarrow \omega^3 - 3\omega - 1 = 0$.
Jede Nullstelle in $\mathbb{Q}$ von $X^3 - 3X - 1$ ist in $\mathbb{Z}$ und teilt -1. $\Rightarrow$ Kandidaten ± 1.
Division mit Rest.
$\Rightarrow$ keine Nullstellen in $\mathbb{Q}$ $\Rightarrow$ irred. $\Rightarrow$ Minimalpolynom.

3.3.11 Bemerkung: Im Fall $n := [K(a)/K] < \infty$ ist jedes Element von $K(a)$ gleich $f(a)$ für ein eindeutiges Polynom $f \in K[X]$ vom Grad $< n$. Die Summe zweier solcher Elemente berechnet sich direkt, das Produkt durch Division mit Rest als $f(a)g(a) = r(a)$ für $q, r \in K[X]$ mit $fg = qm_a + r$ und $\deg(r) < n$. Ist $f(a) \neq 0$, so gilt $\mathrm{ggT}(f, m_a) \sim 1$ in $K[X]$. Mit dem euklidischen Algorithmus findet man dann Polynome $u, v \in K[X]$ mit $uf + vm_a = 1$. Auswerten in a liefert dann die Gleichung $u(a)f(a) = 1$, also $f(a)^{-1} = u(a)$.

$\Rightarrow u(a)\cdot f(a) + v(a)\cdot \underbrace{m_a(a)}_{=0} = 1 \Rightarrow \frac{1}{f(a)} = u(a)$.

3.3.12 Beispiel: Für $a := \sqrt[3]{2}$ ist $m_{a,\mathbb{Q}}(X) = X^3 - 2$ und $\frac{1}{1+a} = \frac{1-a+a^2}{3}$.

Nullstelle a, keine Nullstelle in $\mathbb{Q}$, da $\pm 1, \pm 2$ keine sind.
$\Rightarrow$ irred. $\Rightarrow$ Min.Pol. von a.

$u\cdot(1+X) + v\cdot(X^3 - 2) = 1$.

$u = \alpha + \beta X + \gamma X^2$
$v = \delta$

$\alpha + \beta X + \gamma X^2 + \alpha X + \beta X^2 + \gamma X^3 + \delta X^3 - 2\delta = 1$

$\Leftrightarrow \begin{cases} \alpha - 2\delta = 1 \\ \beta + \alpha = 0 \\ \gamma + \beta = 0 \\ \gamma + \delta = 0 \end{cases} \Leftrightarrow \begin{cases} \alpha = -\beta = \gamma = -\delta \\ \alpha + 2\alpha = 1 \\ \Rightarrow \alpha = 1/3 \end{cases} \Rightarrow u = \frac{1}{3} - \frac{1}{3}X + \frac{1}{3}X^2$

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

3.4 Algebraische Körpererweiterungen

3.4.1 Definition: Eine Körpererweiterung L/K heisst *algebraisch*, wenn jedes Element von L algebraisch über K ist; andernfalls heisst sie *transzendent*.

3.4.2 Proposition: Für jeden Körperturm $M/L/K$ und jedes Element $a \in M$ gilt: Ist a algebraisch über K, so ist es auch algebraisch über L.

Bew.: Sei $f \in K[x] \setminus \{0\}$ mit $f(a) = 0$.
$\Rightarrow f \in L[x] \setminus \{0\} \Rightarrow a$ alg. über L. qed.

$a \in M$
|
L
|
K

3.4.3 Proposition: Sind $a_1, \dots, a_n$ algebraisch über K, so ist $K(a_1, \dots, a_n)/K$ endlich.

Bew.: $n=0$ ✓
$n-1 \rightsquigarrow n \Rightarrow K(a_1, \dots, a_n) = K(a_1, \dots, a_{n-1})(a_n)$
endlich über K nach IV.
a_n algebraisch über $K(a_1, \dots, a_{n-1})$ $\Rightarrow K(a_1, \dots, a_n)/K(a_1, \dots, a_{n-1})$ endlich nach §3.3.
$\Rightarrow K(a_1, \dots, a_n)/K$ endlich nach §3.2
qed.

3.4.4 Proposition: Ist L/K endlich, so ist L/K algebraisch.

Bew.: Sei $a \in L$ und $n := [L/K]$.
$\Rightarrow 1, a, \dots, a^n \in L$ sind K-linear abhängig.
$\Rightarrow \exists \alpha_0, \dots, \alpha_n \in K$, nicht alle 0 mit $\sum \alpha_i a^i = 0$.

mit $f(X) := \sum_{i=0}^{n} \alpha_i X^i \in K[X] \setminus \{0\}$.
Folgt $f(a) = 0 \Rightarrow a$ algebraisch über K.
qed.

3.4.5 Proposition: Eine Körpererweiterung ist endlich genau dann, wenn sie endlich erzeugt und algebraisch ist.

Bew.: "$\Leftarrow$" folgt aus 3.4.3.

"$\Rightarrow$" L/K endlich $\overset{3.4.4}{\Rightarrow}$ algebraisch.

Wähle Basis $a_1, \dots, a_n \in L$ über K. $\Rightarrow L = K(a_1, \dots, a_n)$

$\Rightarrow$ endlich erzeugt. qed

3.4.6 Proposition: Für $L = K(A)$ ist L/K algebraisch genau dann, wenn jedes Element von A algebraisch über K ist.

Bew.: L/K algebraisch $\Rightarrow$ Jedes $a \in A$ algebraisch über K.

Sei jedes $a \in A$ algebraisch über K.

Sei $b \in L$ beliebig. Dann existiert $a_1, \dots, a_n \in A$ und $f, g \in K[X_1, \dots, X_n]$ mit $g(a_1, \dots, a_n) \neq 0$ und $b = \frac{f(a_1, \dots, a_n)}{g(a_1, \dots, a_n)}$

Also $b \in K(a_1, \dots, a_n)$

3.4.3 $\Rightarrow K(a_1, \dots, a_n)/K$ endlich.

3.4.4 $\Rightarrow$ " " algebraisch

$\Rightarrow b$ algebraisch über K. qed.

3.4.7 Bemerkung: Dies bedeutet, dass für alle über K algebraischen Elemente $a, b \in L$ auch $a \pm b$ und ab sowie, falls definiert, a/b algebraisch über K sind.

3.4.8 Beispiel: Die reelle Zahl $a := \sqrt{2} + \sqrt{3}$ ist algebraisch. Ihr Minimalpolynom ist $m_{a,\mathbb{Q}}(X) = X^4 - 10X^2 + 1$, und es ist $[\mathbb{Q}(\sqrt{2} + \sqrt{3})/\mathbb{Q}] = 4$.

$a - \sqrt{2} = \sqrt{3}$

$\Rightarrow (a - \sqrt{2})^2 = 3$

$\Rightarrow a^2 - 2\sqrt{2}a + 2 = 3$

$\Rightarrow a^2 - 1 = 2\sqrt{2}a$

$\Rightarrow (a^2 - 1)^2 = 8a^2$

$a^4 - 2a^2 + 1$

$a^4 - 10a^2 + 1 = 0$.

Ist $X^4 - 10X^2 + 1$ reduzibel in $\mathbb{Q}[X]$, $\Rightarrow$ auch $\mathbb{Z}[X]$. Sicher Norm. 4. Keine Nullstelle $\in \mathbb{Q}$, da ± 1 keine sind.

$\Rightarrow X^4 - 10X^2 + 1 = (X^2 + bX + c)(X^2 - bX + c)$ mit $b \in \mathbb{Z}$, $c = \pm 1$.

$= (X^2 + c)^2 - (bX)^2 = X^4 + 2cX^2 + c^2 - b^2X^2$

$\Rightarrow -10 = 2c - b^2$

$\Rightarrow b^2 = 10 + 2c = \begin{cases} 12 \\ 8 \end{cases} \Rightarrow$ Widerspr.

Also ist das Polynom irred. $\Rightarrow$ gleich $m_{a,\mathbb{Q}}(X)$.

$\mathbb{Q}(a) \subset \mathbb{Q}(\sqrt{2}, \sqrt{3})$

$[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] \leq [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] \cdot [\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2 \cdot 2 = 4$

Es folgt $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$.

Vorsicht: $\sqrt{2}$ hat Min.Pol. $X^2 - 2$ über $\mathbb{Q}$ und Min.Pol. $X - \sqrt{2}$ über $\mathbb{Q}(\sqrt{2})$

3.4.9 Proposition: Für jeden Körperturm $M/L/K$ und jedes Element $a \in M$ gilt: Ist L/K algebraisch, und ist a algebraisch über L, so ist a auch algebraisch über K.

Bew.: Wähle $f \in L[X] \setminus \{0\}$ mit $f(a)=0$ $\Rightarrow$ a alg. über L'

Schreibe $f = \sum_{i=0}^{n} b_i X^i$ mit $b_i \in L$. $\Rightarrow$ $L'(a)/L'$ endlich

Jedes b_i algebraisch über K $\Rightarrow$ $L'(a)/K$ endlich.

$\Rightarrow L' := K(b_0, \dots, b_n)/K$ endlich nach 3.4.3 $\Rightarrow$ $L'(a)/K$ algebraisch.

$\Rightarrow$ a algebraisch über K. qed.

3.4.10 Proposition: Für jeden Körperturm $M/L/K$ ist M/K algebraisch genau dann, wenn M/L und L/K algebraisch sind.

Bew.: Ω/K alg. $\Rightarrow$ L/K alg. und Ω/L alg. nach 3.4.2.

Ω/L und L/K alg. $\Rightarrow$ Jedes $a \in \Omega$ ist alg. über K nach 3.4.9 $\Rightarrow$ Ω/K alg.

qed

3.4.11 Beispiel: Die reelle Zahl $a := \sqrt{1+\sqrt{2}}$ ist algebraisch über $\mathbb{Q}(\sqrt{2})$, also algebraisch über $\mathbb{Q}$. Ihr Minimalpolynom ist $m_{a,\mathbb{Q}}(X) = X^4 - 2X^2 - 1$.

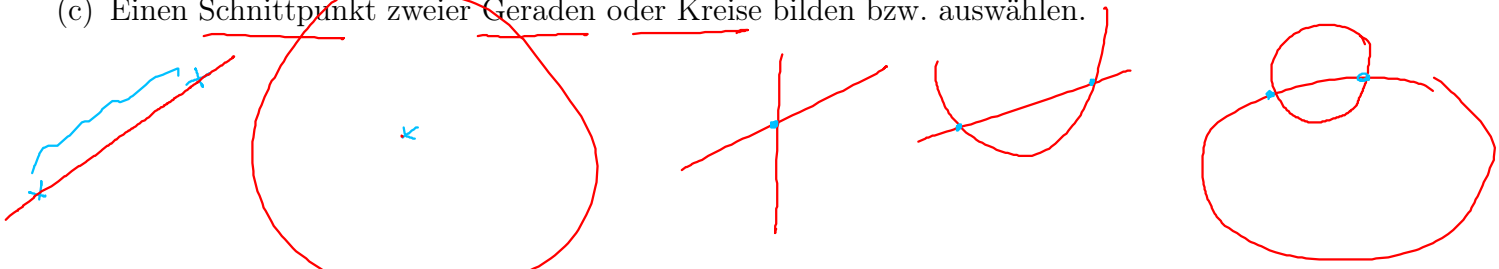
3.5 Konstruktionen mit Zirkel und Lineal

In der euklidischen Ebene erlauben wir die folgenden Konstruktionen:

(a) Mit dem Lineal die Gerade durch zwei verschiedene gegebene Punkte zeichnen.

(b) Mit dem Zirkel den Abstand zweier verschiedener gegebener Punkte aufnehmen und den Kreis mit diesem Radius um einen gegebenen Punkt zeichnen.

(c) Einen Schnittpunkt zweier Geraden oder Kreise bilden bzw. auswählen.



Für jede Menge A von Punkten sei $\mathrm{Kons}(A)$ die Menge aller Schnittpunkte, die man durch iterierte Anwendung dieser Operationen aus A konstruieren kann. Die Abstände $d(P,Q)$ für alle Punkte $P,Q \in \mathrm{Kons}(A)$ heissen die *aus A konstruierbaren Längen.* Die Winkel $\sphericalangle PQR$ für alle paarweise verschiedenen Punkte $P,Q,R \in \mathrm{Kons}(A)$ heissen die *aus A konstruierbaren Winkel.* Unser Ziel ist es, die Menge $\mathrm{Kons}(A)$ und die Menge aller aus A konstruierbaren Längen bzw. Winkel zu beschreiben.

Um dieses geometrische Problem zu algebraisieren, identifizieren wir die euklidische Ebene mit $\mathbb{C}$ mit dem üblichen Abstand $d(P,Q) := |P-Q|$. Damit man überhaupt neue Punkte konstruieren kann, nehmen wir an, dass A mindestens zwei verschiedene Punkte enthält. Durch Translation, Drehung und Streckung reduzieren wir uns dann darauf, dass A mindestens die Punkte 0 und 1 enthält.

3.5.1 Satz: Dann ist $\mathrm{Kons}(A)$ der eindeutige kleinste Unterkörper $K \subset \mathbb{C}$ mit

(a) $A \subset K$.

(b) $\forall z \in K\colon\ \overline{z} \in K$.

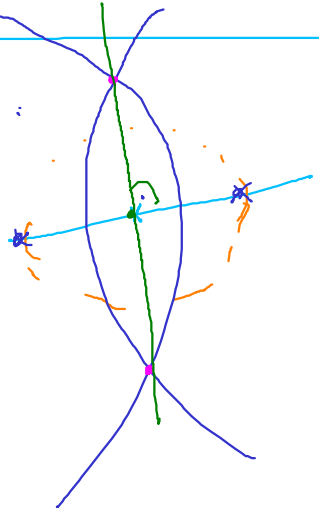
(c) $\forall z \in \mathbb{C}\colon\ z^2 \in K \longrightarrow z \in K$.

Weiter gilt:

(d) Die aus A konstruierbaren Längen sind genau die Zahlen in $\mathrm{Kons}(A) \cap \mathbb{R}^{\geqslant 0}$.

(e) Die aus A konstruierbaren Winkel sind genau die $\alpha \in \mathbb{R}$ mit $\cos\alpha \in \mathrm{Kons}(A)$.

Erinnerung: Rechten Winkel konstruieren:



Lot fällen: