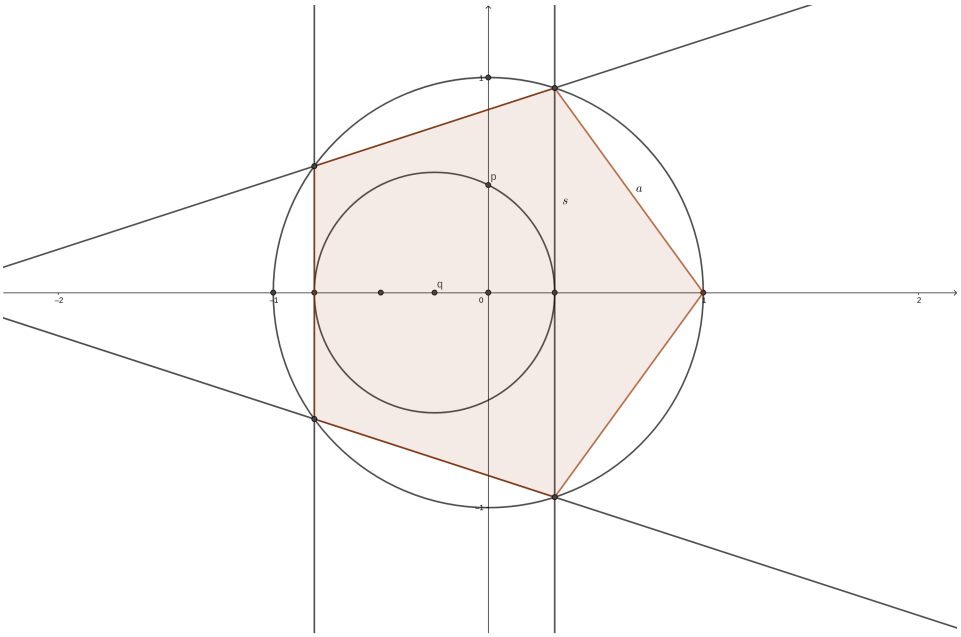
Skript Algebra

Lukas Metzger

22. Oktober 2018

0 Konstruktion mit Zirkel und Lineal

Beispiel 0.1 (Konstruktion des regelmäßigen 5-Ecks)**.** Anleitung zur Konstruktion



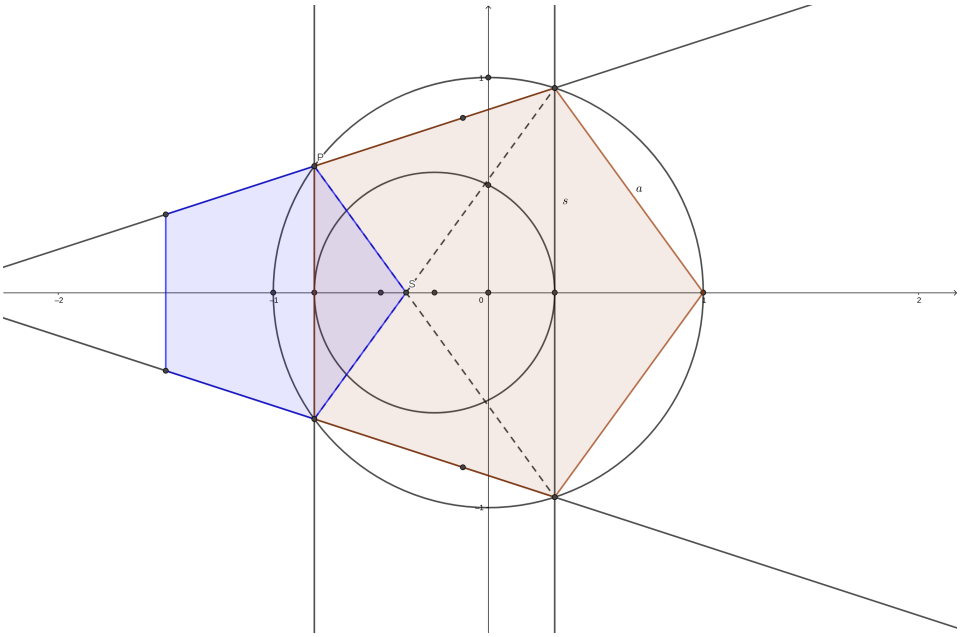
Erste Frage: Gegeben $n \in \mathbb{N}$, kann ich das regelmäßige n-Eck konstruieren?

Beispielproblem: Betrachte Das 5-Eck, sei a die Kantenkänge und s die Sekantenlänge.

Dann ist $\frac{s}{a} \notin \mathbb{Q}$.

Beweis. Angenommen $\frac{s}{a}$ wäre in $\mathbb{Q}$. Dann schreibe $\frac{s}{a} = \frac{p}{q}$ mit $p, q \in \mathbb{N}$. Dann gibt es also eine Länge $d \in \mathbb{R}$, so dass s und a beides ganzzahlige Vielfache von d sind. $\exists n, m \in \mathbb{N}$ $a = n \cdot d, s = m \cdot d$.

Betrachte/Erweitere die Konstruktion des 5-Ecks und erhalte kleines (blaues) 5-Eck wie gezeichnet mit Sekantenlänge $s' = a$ und Kantenlänge $a' = s - a$.



Dann sind aber sowohl a' als auch s' wieder Vielfache von d. Das Verfahren kann ich wiederholen und erhalte immer kleinere 5-Ecke, deren Größe nach 0 konvergiert, wo Kanten- und Sekantenlänge ganzzahlige Vielfache von d sind. ↯ □

Weitere Konstruktionsprobleme:

- 3-Teilung des Winkels
- Verdoppelung des Würfels (d.h. Verdoppelung des Volumens)
- Quadratur des Kreises (Gegeben ein Kreis, konstruiere Quadrat mit demselben Flächeninhalt)

Wiederholung: Was kann ich mit Zirkel und Lineal eigentlich machen?

Antwort: 3 Konstruktionen

1) Gegeben Punkte a_1, a_2, b_1, b_2 der Ebene, betrachte die Geraden $\overline{a_1a_2}$ und b_1b_2 und erhalte Schnittpunkt $\overline{a_1a_2} \cap \overline{b_1b_2}$.

2) Gegeben Punkte a_1, a_2, b_1, b_2, b_3 der Ebene betrachte Kreis $K(b_1, \|b_2 - b_3\|)$ um b_1 mit Radius $\|b_2 - b_3\|$ und erhalte die Schnittpunkte $\overline{a_1a_2} \cap K(b_1, \|b_2 - b_3\|)$

3) Gegeben Punkte $a_1, a_2, a_3, b_1, b_2, b_3$, erhalte Schnittpunkte $K(a_1, \|a_2 - a_3\|) \cap K(b_1, \|b_2 - b_3\|)$

Definition 0.2. Sei $M \subset \mathbb{R}^2$ eine Menge, $p \in \mathbb{R}^2$ ein Punkt.

Sage: p ist aus M mit Zirkel und Lineal konstruierbar, falls es Kette von Mengen gibt

$$M = M_1 \subseteq M_1 \subseteq \cdots \subseteq M_n \ni p$$

Wobei $\forall i$ die Menge M_i entsteht aus M_{i-1} durch Hinzunahme der Punkte die durch einen Konstruktionsschritt entstehen.

Historie: Einen Durchbruch bei der Lösung dieser Probleme gab es erst, als man begann, die Punkte des $\mathbb{R}^2$ mit komplexen Zahlen zu identifizieren.

Bemerkung. Frage nach der Konstruierbarkeit macht nur Sinn, wenn M mindestens 2 Punkte enthält $\rightsquigarrow$ Häufig $M = \{0, 1\} \subset \mathbb{C}$.

In dieser Sprache

- Konstruktionsproblem: n-Eck ist äquivalent zu, kann ich die n-ten Einheitswurzeln $e^{\frac{i2\pi}{n}}$ aus $M = \{0, 1\}$ konstruieren? Ist $e^{\frac{2\pi i}{n}} \in \text{Kons}(\{0, 1\})$?

- Verdopplung des Würfels $\Leftrightarrow$ Ist $\sqrt[3]{2} \in \text{Kons}(\{0, 1\})$

- Quadratur des Kreises $\Leftrightarrow$ Ist $\sqrt{\pi} \in \text{Kons}(\{0, 1\})$

- 3-teilung des Winkels $\Leftrightarrow$ Ist für gegebenes $\varphi \in (0, 2\pi)$ $e^{\frac{i\varphi}{3}} \in \text{Kons}(\{0, 1, e^{i\varphi}\})$

Zentrale Beobachtung

Sei $M \subset \mathbb{C}$ eine Menge die 0 und 1 enthält. Sei $\text{Kons}(M)$ die Menge der aus M konstruierbaren Punkte.

Dann ist $\text{Kons}(M) \subset \mathbb{C}$ ein Unterkörper.

Dazu zu prüfen: Konstruierbarkeit von Summen, Differenzen, Produkten, Quotienten ....

Zusammenfassung/zentrales Thema der Vorlesung

Körpererweiterung / wie können Körper ineinander enthalten sein?

1 Körpererweiterungen

1.1 Ultrakurzwiederholung zentraler Begriffe

Definition 1.1 (Gruppe)**.** Eine Gruppe ist eine Menge G zusammen mit einer Abbildung $m : G \times G \to G$ so dass folgendes gilt:

1) Assoziativ: $\forall a, b, c \in G\, m(m(a, b), c) = m(a, m(b, c))$

2) Neutrales Element: $\exists n \in G \forall a \in G : m(n, a) = m(a, n) = a$

3) Inverse Elemente: $\forall a \in G \exists b \in G : ab = ba$ und dieses Produkt ist neutrales Element wie in 2)

Lemma 1.2 (Elementare Eigenschaften von Gruppen)**.** Für jede Gruppe gilt:

- Das neutrale Element ist eindeutig
- Inverse Elemente sind eindeutig

Definition 1.3 (Abelsche Gruppe)**.** Nenne Gruppe (G, m) Abelsch, falls $\forall a, b \in G$: $m(a, b) = m(b, a)$.

Notation: Statt m schreibt man oft $+$ oder $\cdot$, wobei $+$ hauptsächlich für Abelsche Gruppen verwendet wird.

Beispiel 1.4. Beispiele für Gruppen:

- Abelsche Gruppen: $(\mathbb{Z}, +)$, $(\mathbb{Z}/p\mathbb{Z}, +)$, $(Vektorraum, +)$
- Nicht-Abelsche Gruppen: Sei M eine Menge mit > 2 Elementen. Die bijektiven Abbildungen $M \to M$ mit der Hintereinanderausführung ist eine nicht-Abelsche Gruppe.

  Sei K ein Schiefkörper, z.B. $K = \mathbb{R}, \mathbb{C}, \mathbb{H}$. Sei $K^*K \setminus \{0\}$. Dann ist $(K^*, \cdot)$ eine Gruppe.
- Nicht-Beispiel: $G = \mathbb{R}^3$. Ich erhalte durch das Kreuzprodukt keine Gruppenkonstruktion.

Definition 1.5 (Gruppe)**.** Ein Ring ist eine Menge R mit 2 Verknüpfungen $+$ und $\cdot$ so dass gilt:

- $(R, +)$ ist eine Abelsche Gruppe
- Distributivgesetz: $\forall a, b, c \in T(a + b) \cdot c = ac + bc$ und $a(b + c) = ab + ac$
- $(R \setminus 0, \cdot)$ ist fast Gruppe nämlich assoziativ und es existiert ein neutrales Element

Beispiel 1.6. Beispiele für Ringe:

- $\mathbb{R}, \mathbb{Z}/n\mathbb{Z}$, Polynome, $\mathbb{Z}$
- Funktionen auf $\mathbb{R}/\mathbb{C}$
- holomorphe/stetige/C^∞/reell analytische lokal quadratintegrierbare Funktionen bilden ebenfalls einen Ring

Bemerkung. Mit Ringen kann ich fast rechnen wie mit Zahlen, aber ACHTUNG

- Nicht jedes Element in $R \setminus 0$ hat ein multiplikatives Inverses
- Ich kann aus $a \cdot b = 0$ und $a \neq 0$ im Allgemeinen nicht folgern, dass $b = 0$
- Ich kann aus $ab = ac$ und $a \neq 0$ im allgemeinen nicht folgern, dass $b = c$ ist

Definition 1.7 (Nullteiler)**.** Sei R ein Ring, $a \in R \setminus \{0\}$. Falls $b \neq 0$ existiert mit $a \cdot b = 0$, nenne ich a einen Nullteiler.

Ringe ohne Nullteiler heißen Nullteilerfrei oder Integritätsringe.

Definition 1.8 (Abelscher Ring)**.** Ein Ring heißt Abelsch, falls $\forall a, b \in R\ ab = ba$.

Bemerkung. In der Literatur heißen unsere Ringe oft Ringe mit 1.

Beispiel 1.9. Beispiele zu Nullteilern

- $\mathbb{R}, \mathbb{Z}$ sind nullteilerfrei
- $\mathbb{Z}/n\mathbb{Z}$ ist nullteilerfrei $\Leftrightarrow$ n ist Prim
- Polynome sind nullteilerfrei
- Stetige Funktionen sind nicht nullteilerfrei

Bemerkung. Sei R ein Ringe. Die Menge der Elemente, die ein multiplikatives Inverses haben, wir mit R^* bezeichnet.

- $\mathbb{Z}^* = \{1, -1\}$
- $(\mathbb{Z}/n\mathbb{Z})^* = \{[x] \mid x \text{ ist teilerfremd zu } n\}$
- $(C^\infty(\mathbb{R}))^* = \{f : \mathbb{R} \to \mathbb{R} \mid f \text{ ist } C^\infty \text{ und hat keine Nullstelle}\}$

Bemerkung. Sei R ein Ring, x eine Variable. Dann bezeichne mit $R[x]$ die Polynome mit Koeffizienten in R und Variable x.

- $1x + 2 \in \mathbb{Z}[x]$
- $\frac{\pi}{4} \cdot x^2 \notin \mathbb{Z}[x]$

Definition 1.10 (Schiefkörper)**.** Schiefkörper sind Ringe R wobei $R^* = R \setminus \{0\}$

Definition 1.11 (Körper)**.** Ein Körper ist ein Schiefkörper, der auch noch kommutativ ist.

Beispiel 1.12. Beispiele für Körper und Schiefkörper

- Quaternionen sind Schiefkörper
- $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}/p\mathbb{Z}$ sind Körper
- Kons$(\{0, 1\})$ ist Unterkörper von $\mathbb{C}$
- Die Menge der Rationale Funktionen über einem Körper bilden wieder einen Körper

1.2 Algebraische und transzendente Elemente

Sei L ein Körper und $k \subset L$ ein Unterkörper (z.B. $L = \mathbb{C}, k \subset \mathbb{R}$ oder $L = \mathbb{R}, k = \mathbb{Q}$).

Im Fall $k = \mathbb{Q}, L = \mathbb{R}$ wissen wir, dass es in $\mathbb{R}$ sehr unterschiedliche Elemente gibt.

- $\sqrt{7}$ ... algebraisch
- π, e ... transzendent

Definition 1.13. Situation wie oben. Sei $a \in L$ gegeben. Nenne a algebraisch über k falls es ein Polynom gibt $f \in k[x]$ und $f \neq 0$ so dass $f(a) = 0$.

Bemerkung. Nicht algebraische Elemente heißen transzendent.

Beispiel 1.14. Beispiele für algebraische und transzendente Zahlen

- $\sqrt{7}$ ist algebraisch über $\mathbb{Q}$, denn $f(\sqrt{7}) = 0$ mit $f(x) = x^2 - 7$
- π ist nicht algebraisch über $\mathbb{Q}$ (Lindemann, 1844)

Bemerkung. In $\mathbb{R}$ gibt es praktisch keine Zahlen, die algebraisch über $\mathbb{Q}$ sind.

Wir wissen $\mathbb{Q}$ ist abzählbar, also sind auch die Polynome mit Koeffizienten in $\mathbb{Q}$ abzählbar. Jedes Polynom hat aber nur endlich viele Nullstellen. Das heißt die Menge der algebraischen Zahlen ist abzählbar, also eine Nullmenge im Sinne der Integrationstheorie.

Beispiel 1.15. Körpererweiterung $\mathbb{R} \subset \mathbb{C}$ - Beobachte: i ist algebraisch über $\mathbb{R}$, denn $f(i) = 0$ wobei $f(x) = x^2 + 1$

$z = i + 1$ ist Algebraisch mit $f(x) = (x-1)^2 + 1$

$z = a + bi$ ist Algebraisch mit $f(x) = \left(\frac{(x-a)}{b}\right)^2 + 1$

$\Rightarrow$ Jede komplexe Zahl ist algebraisch über $\mathbb{R}$

Definition 1.16. Eine Körpererweiterung $k \subset L$ heißt algebraisch, falls jedes $a \in L$ algebraisch über k ist.

Ansonsten nenne Körpererweiterung transzendent.

Bemerkung. Sei $k \subset L$ eine Körpererweiterung, sei $a \in L$ algebraisch über k und sei $f \in k[x]$ ein Polynom $\neq 0$ mit $f(a) = 0$.

Solche Polynome gibt es viele, wir interessieren uns für f's mit mimimalem Grad. Wenn so ein f gegeben ist:

$$f = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$$

dann dividiere durch a_n und erhalte Polynom

$$\hat{f} = x^n + \frac{a_{n-1}}{a_n} x^{n-1} + \cdots + \frac{a_0}{a_n} \in k[x]$$

mit a als Nullstelle.

Falls $\hat{f}$ und $\overline{f}$ in $k[x]$ zwei normierte Polynome von minimalem Grad sind mit $\hat{f}(a) = \overline{f}(a) = 0$, dann betrachte Polynom $(\hat{f} - \overline{f}) \in k[x]$. Dann gilt

$$(\hat{f} - \overline{f})(a) = \hat{f}(a) - \overline{f}(a) = 0 - 0 = 0$$

und der Grad von $(\hat{f} - \overline{f})$ ist kleiner als der Grad von $\hat{f}$. Weil aber der Grad von $\hat{f}$ minimal war, folgt: $\hat{f} = \overline{f}$.

Satz 1.17. Sei $k \subset L$ eine Körpererweiterung, sei $a \in L$ algebraisch über k. Dann gibt es genau ein Polynom $f \in k[x] \setminus \{0\}$ so dass gilt:

1) $f(a) = 0$

2) $\operatorname{grad} f$ ist minimal unter den Graden der Polynome die a als Nullstelle haben:

$$\operatorname{grad}(f) = \min\{\operatorname{grad} g \mid g \in k[x] \setminus \{0\}, g(a) = 0\}$$

3) f ist normiert (d.h. Leitkoeffizient = 1)

Nenne dieses f das Minimalpolynom von a über k.

Die Zahl $\operatorname{grad} f$ wird als Grad von a über k bezeichnet, in Symbolen $[a : k]$

Bemerkung. Sei $k \subset L$ Erweiterung, $a \in L$ algebraisch über k. Falls $[a : k] = 1$, dann $a \in k$.

Mehr Beispiele für Körpererweiterungen

Sei $k \subset L$ eine Körpererweiterung, sei $(L_i)_{i \in I}$ eine Menge von Zwischenkörpern, d.h. $k \subseteq L_i \subseteq L$.

Dann ist auch $K \coloneqq \bigcap_{i \in I} L_i$ ein Körper.

Nutzanwendung: Sei $A \subset L$ irgendeine Teilmenge. Sei $(L_i)_{i \in I}$ die Menge der Zwischenkörper $k \subseteq L_i \subseteq L$ so dass $\forall i : A \subset L_i$. Dann betrachte K und es gilt:

- $k \subseteq K \subset L$, also K ist Zwischenkörper
- $A \subseteq K$
- K ist der kleinste Zwischenkörper der A enthält

Bemerkung. Bezeichne K mit $k(A)$ und sage $k(A)$ entsteht aus k durch Adjunktion der Elemente von A.

Spezialfall: $A = \{a\}$ dann schreibe ich $k(a)$. Das ist dann der kleinste Unterkörper von L, der sowohl k als auch a enthält.

Definition 1.18 (Einfache Körpererweiterung)**.** Eine Körpererweiterung $k \subset L$ heißt einfach, falls a existiert, so dass $L = k(a)$.

Definition 1.19 (Grad der Körpererweiterung)**.**

$$[L : k] = \dim_k L \qquad \text{Grad der Körpererweiterung}$$

Beispiele

$$[\mathbb{C} : \mathbb{R}] = 2 \qquad [\mathbb{R} : \mathbb{Q}] = \infty$$

Satz 1.20. Sei L/k eine Körpererweiterung, $a \in L$ dann gilt

$$[a : k] = [k(a) : k]$$

Beweis. Falls a tanszendent, dann sind $1, a, a^2, \ldots$ k-linear unabhängig, also ist $\dim_k k(a) = \infty$.

Betrachte also den Fall, wo a algebraisch ist mit Minimalpolynom $f(x) = x^n + b_{n-1} + \cdots + b_0 \in k[x]$.

Klar ist: Die Elemente $1, a, a^2, \ldots, a^{n-1} \in k(a)$ sind linear unabhängig, denn jede lineare Relation gäbe ein Polynom $g(x)$ vom Grad $< n$ mit $g(a) = 0$ ↯.

Also: $\dim_k k(a) \geq n$

Um Gleichheit zu zeigen, genügt es zu zeigen, dass $\langle 1, a, a^2, \ldots, a^{n-1} \rangle_k =: \tilde{k}$ bereits $k(a)$. Klar ist $\tilde{k} \in k(a)$. Wegen der Minimalität von $k(a)$ genügt es für die Umkehrrichtung zu zeigen, dass $\tilde{k}$ ein Körper ist.

Klar ist $0, 1 \in \tilde{k}$.

Zu zeigen ist Abgeschlossenheit unter Addition/Subtraktion (hier klar wegen Vektorraum) und unter Multiplikation/Division (noch nicht klar).

Zwischenbehauptung: Sei $s = \sum_{i=0}^{n-1} \lambda_i a^i \in \tilde{k}$ ein beliebiges Element. Dann ist $a \cdot s \in \tilde{k}$.

Wir wissen:

$$a \cdot s = \underbrace{\sum_{i=0}^{n-2} \lambda_i a^{i+1}}_{\in \tilde{k}} + \lambda_{n-1} a^n$$

Ein Blick auf das Minimalpolynom zeigt:

$$a^n = -\sum_{i=0}^{n-1} b_i \cdot a^i \in \tilde{k}$$

Konsequenz: Wenn $s, t \in \tilde{k}$ beliebig sind, dann $s \cdot t \in \tilde{k}$, also gilt die Abgeschlossenheit unter Multiplikation.

Letzte Aufgabe: Existenz von multiplikativen Inversen. Sei also $s \in \tilde{k}, s \neq 0$ gegeben. Wegen abgeschlossenheit unter Multiplikation ist $s, s^2, s^3, \ldots$ wieder in $\tilde{k}$. Also ist $1, s, \ldots, s^n$ linear abhängig $\Rightarrow$ s ist algebraisch über k.

Sei $p(x) = x^m + p_{m-1} \cdot x^{m-1} + \cdots + p_0$ das Minimalpolynom.

Beobachtung: $p_0 \neq 0$, denn sonst könnte ich x ausklammern, p wäre nicht minimal. Damnach kann ich schreiben:

$$\begin{aligned} 0 = p(s) &= s^m + p_{m-1}s^{m-1} + \cdots + p_0 \\ \Leftrightarrow -p_0 &= s(s^{m-1} + p_{m-1}s^{m-1} + \cdots + p_1) \\ \Leftrightarrow \frac{1}{s} &= \underbrace{\frac{1}{-p_0}}_{\in k} \underbrace{(s^{m-1+p_{m-1}s^{m-2}+\cdots+p_1})}_{\in \tilde{k} \text{ wegen Abg. unter Mult.}} \in \tilde{k} \end{aligned}$$

□

Folgerung 1.21.

1) Wenn $[a : k] = n$, dann ist $k(a) = \{\lambda_0 + \lambda_1 a + \cdots + \lambda_{n-1}a^{n-1} \mid \lambda_i \in k\}$

2) Wenn $[a : k] < \infty$, dann ist $k(a)/k$ algebraisch

Beispiel 1.22. Sei $L = \mathbb{C}, k \subset C$ ein Unterkörper, sei $b \in k$ und $a = \sqrt{b}$. Dann gilt:

$$[k(a) : k] = \begin{cases} 2 & \text{falls } a \notin k \\ 1 & \text{falls } a \in k \end{cases}$$

Proposition 1.23 (Umkehrung der Beobachtung)**.** Sei L/k eine Körpererweiterung von Grad 2. Dann entsteht L durch Adjunktion einer Quadratwurzel.

Lemma 1.24. Sei L/k eine algebraische Körpererweiterung, so dass der Erweiterungsgrad $[L : k]$ eine Primzahl ist. Dann ist die Erweiterung einfach, das heißt $\exists a \in L : L = k(a)$.

Beweis. Übung □

Beweis. (von Proposition 1.23) Wähle $a \in L$ wie im Lemma. Dann ist klar $[a : k] = 2$. Also existieren $\lambda_1, \lambda_0 \in k$, so dass $a^2 + \lambda_1 a + \lambda_0 = 0$ ist. Also:

$$a \in \underbrace{\frac{-\lambda_1}{2}}_{\in k} \pm \underbrace{\sqrt{\left(\frac{\lambda_1}{2}\right)^2 - \lambda_0}}_{=b}$$

Weil a und b sich nur um Elemente von k unterscheiden, ist $k(a) = k(b)$. Das Element b ist aber Quadratwurzel! □

Bemerkung. Falls $\text{char}(k) = 2$ ist, muss man die Lösungsformel richtig hinschreiben.

Satz 1.25. Sei $k \subseteq L \subseteq M$ eine Kette von Körpern. Dann ist

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

Beweis. (nur im Fall, wo $[M : L] < \infty$ und $[L : k] < \infty$)

Wähle Basis $m_1, \ldots, m_a$ für M als L-Vektorraum und $l_1, \ldots, l_b$ für L als k-Vektorraum.

Behauptung: Dann bilden die Elemente $(m_i \cdot l_j)_{i,j}$ eine Basis von M als k-Vektorraum.

Erzeugendensystem: Sei $m \in M$ gegeben. Dann ist m schreibbar als

$$m = \sum_{i=1}^{a} \lambda_i \cdot m_i$$

mit $\lambda_i \in L$.

Dann kann ich jedes λ_i schreiben als

$$\lambda_i = \sum_{j=1}^{b} \mu_j^i \cdot l_j$$

mit $\mu_j \in k$.

Einsetzten zeigt m kann geschrieben werden als k-Linearkombination der Produkte $m_i \cdot l_j$.

Lineare Unabhängigkeit: Sei eine lineare Relation

$$0 = \sum_{i,j} \mu_j ij \cdot (m_i \cdot l_j)$$

gegeben, wobei $\mu_j ij \in k$. Dann gilt

$$0 = \sum_i \underbrace{\left(\sum_j \mu_{ij} \cdot l_j \right)}_{\in L} \cdot m_i$$

Weil die m_i per Wahl aber L-linear unabhängig sind folgt für alle i $\sum_j \underbrace{\mu_{ij}}_{\in k} \cdot l_j = 0$.

Weil die l_j per Wahl aber k-linear unabhängig sind, ist $\forall i \forall j \mu_{ij} = 0$. □

Folgerung 1.26. Wenn eine Kette von Körpererweiterungen gegeben ist, $k \subseteq L \subseteq M$ und wenn $[M : k] < \infty$ dann ist $[L : k] < \infty$ und sogar ein Teiler von $[M : k]$.

Satz 1.27. Sei L/k eine Körpererweiterung, dann ist äquivalent:

1) $[L : k] < \infty$

2) L ist algebraisch über k, und es gibt endlich viele $a_1, \ldots, a_n \in L : L = k(a_1, \ldots, a_n)$

3) Es gibt endlich viele $a_1 \ldots, a_n \in L$, die algebraisch über k sind und $L = k(a_1, \ldots, a_n)$

Beweis. 1 ⇒ 2: Sei $s \in L$ beliebig. Dann sind $1, s, s^2, \ldots, s^{[L:k]}$ linear abhängig, also ist s algebraisch über k. Das heißt L/k ist algebraisch. Um $a_1, \ldots, a_n$ zu finden, wähle Vektorraumbasis von L über k.

2 ⇒ 3: trivial

3 ⇒ 1: Betrachte

$$\underbrace{k}_{=:k_0} \subseteq \underbrace{k(a_1)}_{=:k_1} \subseteq \underbrace{k(a_1, a_2)}_{=:k_2} \subseteq \cdots \subseteq \underbrace{k(a_1, \ldots, a_n)}_{=:k_n}$$

Dann klar: $\forall i : a_i$ ist algebraisch über k_{i-1} (sogar algebraisch über k_0) also $[k_i : k_{i-1}] < \infty$, dann $k_i = k_{i-1}(a_i)$ und $[L : k] = \prod_i [k_i : k_{i-1}] < \infty$. □

Lemma 1.28 (Nutzanwendung (Transitivität der Algebraizität))**.** Sei $k \subseteq L \subseteq M$ eine Kette von Körpererweiterungen. Falls L/k algebraisch ist und M/L algebraisch ist, dann ist M/k algebraisch.

Beweis. Sei $m \in M$ gegeben. Ziel: m ist algebraisch über k.

m ist algebraisch über L, das heißt es hat ein Minimalpolynom

$$f(x) = \sum_{i=0}^{a} l_i \cdot x^i \in L[x]$$

Wir wissen auch: Jedes der l_i ist algebraisch über k.

Betrachte jetzt den Zwischenkörper $L' = k(l_0, \ldots, l_a)$. Dann ist L'/k endlich und m ist algebraisch über L', also ist $m \in L'(m)$ und $L'(m)/L'$ ist endlich. Damit ist $L'(m)/k$ endlich, also algebraisch. □

Proposition 1.29. Sei $k \subseteq L$ eine Körpererweiterung. Sei

$$\overline{k} :- \{a \in L \mid a \text{ ist algebraisch über } k\}$$

Dann ist $\overline{k}$ ein Körper.

Man nennt $\overline{k}$ den algebraischen Abschluss von k in L.

Beweis. Klar ist, dass $0, 1 \in \overline{k}$ sind. Wir müssen klären, ob mit $a, b \in \overline{k}$ auch $a+b, a-b, a \cdot b$ und gegebenenfalls für $\frac{1}{a} \in \overline{k}$ sind. Das ist aber klar, denn all diese Elemente liegen in $k(a, b)$. Nach Satz ist $k(a, b)$ algebraisch über k. □

Bemerkung. Achtung: Es gibt einen anderen Begriff von (absolutem) algebraischen Abschluss, der nicht von einem Oberkörper $L \supseteq k$ abhängt.