

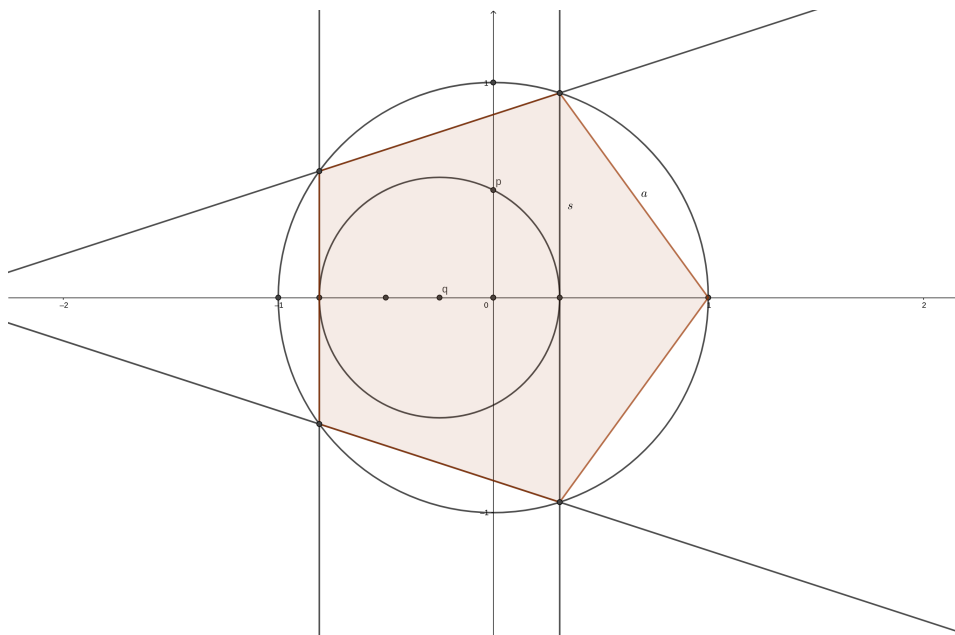
# Skript Algebra

Lukas Metzger

29. 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 Kantenlänge 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.  $\nexists$   $\square$

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  $\overline{a_1 a_2}$  und  $b_1 b_2$  und erhalte Schnittpunkt  $\overline{a_1 a_2} \cap \overline{b_1 b_2}$ .
- 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  $\overline{a_1 a_2} \cap K(b_1, \|b_2 - b_3\|)$
- 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  $m : G \times G \rightarrow G$  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:  $(\mathbb{Z}, +)$ ,  $(\mathbb{Z}/p\mathbb{Z}, +)$ ,  $(\text{Vektorraum}, +)$
- Nicht-Abelsche Gruppen: Sei  $M$  eine Menge mit  $> 2$  Elementen. Die bijektiven Abbildungen  $M \rightarrow M$  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** (Ring). Ein Ring ist eine Menge  $R$  mit 2 Verknüpfungen  $+$  und  $\cdot$  so dass gilt:

- $(R, +)$  ist eine Abelsche Gruppe
- Distributivgesetz:  $\forall a, b, c \in R \quad (a + b) \cdot c = ac + bc$  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/ $C^\infty$ /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  $\forall a, b \in R \quad ab = ba$ .

*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 Ring. Die Menge der Elemente, die ein multiplikatives Inverses haben, wir mit  $R^*$  bezeichnet.

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

*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
- $\text{Kons}(\{0, 1\})$  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.

- $\sqrt{7} \dots$  algebraisch
- $\pi, e \dots$  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  $f(x) = x^2 - 7$
- $\pi$  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 minimalem Grad. Wenn so ein  $f$  gegeben ist:

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

dann dividiere durch  $a_n$  und erhalte Polynom

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

mit  $a$  als Nullstelle.

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

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

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

**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)  $\deg f$  ist minimal unter den Graden der Polynome die  $a$  als Nullstelle haben:

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

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

Nenne dieses  $f$  das Minimalpolynom von  $a$  über  $k$ .

Die Zahl  $\deg f$  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  $K := \bigcap_{i \in I} L_i$  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).

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



## Beispiele

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

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

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

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

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

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

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

Um Gleichheit zu zeigen, genügt es zu zeigen, dass  $\langle 1, a, a^2, \dots, a^{n-1} \rangle_k =: \tilde{k}$  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:

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

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  $s, s^2, s^3, \dots$  wieder in  $\tilde{k}$ . Also ist  $1, s, \dots, s^n$  linear abhängig  $\Rightarrow s$  ist algebraisch über  $k$ .

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

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

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

□

**Folgerung 1.21.**

- 1) Wenn  $[a : k] = n$ , dann ist  $k(a) = \{\lambda_0 + \lambda_1 a + \dots + \lambda_{n-1} a^{n-1} \mid \lambda_i \in k\}$
- 2) Wenn  $[a : k] < \infty$ , dann ist  $k(a)/k$  algebraisch

**Beispiel 1.22.** Sei  $L = \mathbb{C}, k \subset \mathbb{C}$  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  $m_1, \dots, m_a$  für  $M$  als  $L$ -Vektorraum und  $l_1, \dots, l_b$  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  $\lambda_i$  schreiben als

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

mit  $\mu_j \in k$ .

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

Lineare Unabhängigkeit: Sei eine lineare Relation

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

gegeben, wobei  $\mu_j^i \in k$ . Dann gilt

$$0 = \sum_i \left( \underbrace{\sum_j \mu_j^i \cdot l_j}_{\in L} \right) \cdot m_i$$

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

Weil die  $l_j$  per Wahl aber  $k$ -linear unabhängig sind, ist  $\forall i \forall j \mu_j^i = 0$ . □

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

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

2  $\Rightarrow$  3: trivial

3  $\Rightarrow$  1: Betrachte

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

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  $[L : k] = \prod_i [k_i : k_{i-1}] < \infty$ .  $\square$

**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  $L' = k(l_0, \dots, l_a)$ . 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.  $\square$

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

$$\bar{k} := \{a \in L \mid a \text{ ist algebraisch über } k\}$$

Dann ist  $\bar{k}$  ein Körper.

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

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

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

## 1.3 Lösungsformel für Polynome

Wissen aus der Schule: Quadratische Gleichungen in einer Variable haben Lösungsformel.

Wissen seit der Renaissance: Haben Formeln für Gleichungen von Grad 3 und 4.

Beispiel:  $x^3 + ax^2 + bx + c = 0$  Setze:

$$h = -\frac{1}{2}c + \frac{1}{6}ab - \frac{1}{24}a^3$$

$$w_1 = \sqrt{-3(a^2b^2 - 4a^3c - 4b^3 + 18abc - 27c^2)}$$

$$w_2 = \sqrt[3]{h + \frac{1}{18}w_1}$$

$$w_3 = \sqrt[3]{h - \frac{1}{18}w_1}$$

Dann ist

$$x = -\frac{1}{3}a + w_2 - w_3$$

eine Lösung, wenn die Wurzeln  $w_2, w_3$  so gewählt sind dass  $w_2w_3 = \frac{1}{8}a^2 - \frac{1}{3}b$ .

Frage: Gibt es eine Lösungsformel für Gleichungen vom Grad 5?

Bescheidener: Kann ich die Lösung überhaupt hinschreiben? (als komplizierten Ausdruck in Wurzeln/Polynomen)

**Definition 1.30.** Sei  $L/k$  eine Körpererweiterung, nenne diese Erweiterung Radikalerweiterung, falls es  $a_1, \dots, a_n$  und  $m_1, \dots, m_n \in \mathbb{N}$  gibt, so dass

$$1) \quad L = k(a_1, \dots, a_m)$$

$$2) \quad \forall i a_i^{m_i} \in k(a_1, \dots, a_{i-1}) \text{ also } a_i \text{ ist die } m_i\text{-te Wurzel eines Elementes aus } k(a_1, \dots, a_{i-1}).$$

Was bedeutet das?

- 1)  $a_1^{m_1} \in k$  Also  $k(a_1) = \langle 1, a_1, a_1^2, \dots, a_1^{m_1-1} \rangle_k$
- 2)  $a_2^{m_2} \in k$  Also  $k(a_1, a_2) = \langle 1, a_2, a_2^2, \dots, a_2^{m_2-1} \rangle_{k(a_1)}$
- 3) ...

Bescheidene Frage, präzise formuliert: Gegeben ein Polynom

$$f(x) = \sum_{i=1}^n a_i x^i \in \mathbb{Q}[x] \text{ oder } \mathbb{R}[x]$$

gibt es dann eine Radikalerweiterung  $L/\mathbb{Q}(a_0, \dots, a_n)$  (beziehungsweise  $L/\mathbb{R}$ ) so dass  $f$  in  $L$  eine Nullstelle hat? Gerne  $L \subseteq \mathbb{C}$ .

## 2 Ringe

Warum Ringe betrachten? Gegeben eine Körpererweiterung  $L/k$  und  $a \in L$  und ich suche das Minimalpolynom  $f_a(x) \in k[x]$ .

Häufig findet man  $g \in k[x]$  mit  $g(a) = 0$  und muss dann entscheiden ob  $g$  das Minimalpolynom ist. Das ist gar nicht leicht!

Beobachtung: Polynomdivision zeigt:

$$g(x) = s(x) \cdot f_a(x) + \text{rest}(x)$$

wobei  $\deg \text{rest}(x) < \deg f_a(x)$ .  $a$  einsetzen ergibt

$$\underbrace{g(a)}_{=0} = s(a) \cdot \underbrace{f_a(a)}_{=0} + \text{rest}(a) \Rightarrow \text{rest}(a) = 0$$

$$\Rightarrow \text{rest}(x) \equiv 0$$

$$\Rightarrow g(x) = s(x) \cdot f_a(x).$$

Wir sehen: Das Minimalpolynom ist ein Teiler von  $g$  im Ring der Polynome.

Ziel: Wir müssen Teilbarkeit verstehen!

## 2.1 Teilbarkeit

**Definition 2.1.** Sei  $R$  ein Ring. Dann bezeichne mit  $R[x]$  den Ring der Polynome mit Variable  $x$  und Koeffizienten aus  $R$ .

Warnung: Polynome geben Funktionen  $R \rightarrow R$  aber Polynome sind nicht Funktionen.

**Definition 2.2.** Sei  $f \in R[x]$  ein Polynom. Dann definiere den Grad von  $f$  wie üblich.

**Lemma 2.3.** Sei  $R$  ein Integritätsring,  $f, g \in R[x]$ . Dann ist

$$\deg(f \cdot g) = \deg(f) + \deg(g)$$

*Beweis.* Sei  $n_f = \deg(f)$  und  $n_g = \deg(g)$  schreibe

$$\begin{aligned} f(x) &= a_f \cdot x^{n_f} + (\text{kleinere Terme}), a_f \neq 0 \\ g(x) &= a_g \cdot x^{n_g} + (\text{kleinere Terme}) \end{aligned}$$

Dann ist

$$(f \cdot g)(x) = a_f \cdot a_g \cdot x^{n_f+n_g} + (\text{kleinere Terme})$$

und weil  $R$  ein Integritätsring ist, ist  $a_f \cdot a_g \neq 0$ , also  $\deg(f \cdot g) = n_f + n_g$ .  $\square$

**Folgerung 2.4.** Sei  $R$  ein Integritätsring. Dann ist  $R[x]$  selbst wieder ein Integritätsring.

*Beweis.* Seien  $f, g \in R[x] \setminus \{0\}$ .

Wir müssen zeigen:  $f \cdot g \neq 0 \in R[x]$  (\*).

Falls  $\deg f = \deg g = 0$ , folgt (\*) weil  $R$  ein Integritätsring ist.

Ansonsten folgt (\*), weil  $\deg f \cdot g = \deg f + \deg g > 0$ .  $\square$

Ausblick: Dann ist  $(R[x])[y]$  auch wieder ein Integritätsring. Und natürlich ist  $(R[x])[y] \simeq R[x, y]$ .

**Folgerung 2.5.** Sei  $R$  ein Integritätsring. Dann ist  $(R[x])^* = R^*$ .

*Beweis.* Sei  $f(x) \in (R[x])^*$ , das heißt  $\exists g(x) \in R[x] : f \cdot g \equiv 1$ .

$$\Rightarrow \deg f + \deg g = \deg 1 = 0$$

$\Rightarrow \deg f = 0$ , also ist Polynom  $f$  konstant, ebenso für  $g$ .  $\square$

*Bemerkung.* Per Induktion folgt auch  $(R[x_1, \dots, x_n])^* = R^*$

**Definition 2.6.** Sei  $R$  ein Ring, seien  $s, r \in R$  Elemente. Ich sage:  $s$  ist Teiler von  $r$  (in Symbolen  $s \mid r$ ), wenn es  $a \in R$  gibt, so dass  $s \cdot a = r$ .

**Lemma 2.7.** Sei  $R$  ein Integritätsring, seien  $s, r$  Elemente. Dann ist äquivalent

- 1)  $\exists \varepsilon \in R^*, s = \varepsilon \cdot r$
- 2)  $s \mid r$  und  $r \mid s$

Wenn diese Bedingungen erfüllt sind, nenne ich  $s$  und  $r$  assoziiert (in Symbolen  $s \sim r$ ).

*Beweis.* 1)  $\Rightarrow$  2) ✓

2)  $\Rightarrow$  1) Aus  $s \mid r$  und  $r \mid s \Rightarrow a, b \in R : s \cdot a = r$  und  $r \cdot b = s$ .

$$\Rightarrow (r \cdot b) \cdot a \Rightarrow r(ba - 1) = 0$$

Da  $R$  Integritätsring ist:  $\Rightarrow ba = 1 \quad \Rightarrow b, a \in R^*$  □

**Definition 2.8.** Sei  $R$  ein Integritätsring, seien  $s, r \in R$  Elemente. Dann nenne  $s$  einen echten Teiler von  $r$  (in Symbolen  $s \parallel r$ ) falls gilt:

- 1)  $s \mid r$
- 2)  $s \notin R^*$
- 3)  $r$  und  $s$  sind nicht assoziiert

**Definition 2.9.** Sei  $R$  ein Integritätsring. Ein Element  $r \in R$  heißt irreduzibel, falls  $r \notin R^*$  und falls  $r$  keine echten Teiler hat.

**Beispiel 2.10.** Die irreduziblen Elemente von  $R = \mathbb{Z}$  sind exakt  $\pm$ (Primzahl).

**Lemma 2.11.** Sei  $R$  ein Integritätsring. Seien  $r, s, t, s_1, s_2, u, v \in R$ . Dann gilt:

- 1)  $r \mid r$
- 2)  $r \mid s$  und  $s \mid t \Rightarrow r \mid t$
- 3)  $r \mid s_1$  und  $r \mid s_2 \Rightarrow r \mid (s_1 + s_2)$
- 4)  $r \mid s_1$  und  $r \mid (s_1 + s_2) \Rightarrow r \mid s_2$
- 5)  $r \mid s$  und  $u \mid v \Rightarrow ru \mid sv$



Nächstes Ziel: In  $\mathbb{Z}$  ist jede Zahl darstellbar als Produkt von Primzahlen und die Darstellung ist eindeutig bis auf Reihenfolge und Vorzeichen.

Wunschtraum: Sei  $R$  ein Integritätsring. Dann ist jedes Element eindeutig darstellbar als Produkt von irreduziblen Elementen.

**Beispiel 2.12.** Betrachte  $R = \mathbb{Z}[\sqrt{-5}] = \{a + b \cdot \sqrt{-5} \mid a, b \in \mathbb{Z}\} \subset \mathbb{C}$

Dieser Ring ist ein Unterring von  $\mathbb{C}$  und deshalb Nullteilerfrei und

$$9 = 3 \cdot 3 = \underbrace{(2 + \sqrt{-5})(2 - \sqrt{-5})}_{2^2 - (\sqrt{-5})^2}$$

Die Elemente  $3, 2 \pm \sqrt{-5}$  sind irreduzibel und nicht zueinander assoziiert.

**Definition 2.13.** Sei  $R$  ein Integritätsring. Eine Teilerkette ist eine Folge  $(r_i)_{i \in \mathbb{N}}$  von Elementen aus  $R$ , so dass  $\forall i \ r_{i+1} \mid r_i$ . Ich sage, im Ring  $R$  gilt der Teilerkettensatz für Elemente, falls in jeder Teilerkette die stärkere Bedingung  $r_{i+1} \parallel r_i$  nur endlich oft gilt.

**Beispiel 2.14.** Im Ring  $\mathbb{Z}$  gilt der Teilerkettensatz für Elemente, denn falls  $r_{i+1} \parallel r_i$  ist, dann gilt  $|r_{i+1}| < |r_i|$ .

Analog im Polynomring mit  $\deg$  statt  $|\cdot|$ .

**Satz 2.15.** Sei  $R$  ein Integritätsring in dem der Teilerkettensatz für Elemente gilt. Dann ist jedes  $r \in R, r \notin R^*, r \neq 0$  als Produkt von endlich vielen irreduziblen Elementen darstellbar.

*Beweis.* (Noether Rekursion) Wir wollen zeigen, dass  $M = \{r \in R \mid r \notin R^*, r \neq 0 \text{ und } r \text{ nicht als Produkt von endlich vielen irreduziblen darstellbar}\}$  leer ist. Widerspruchsbeweis: angenommen  $M \neq \emptyset$ .

Beobachtungen:

- 1)  $\forall r \in M$   $r$  ist nicht irreduzibel (denn sonst wäre  $r$  eine Darstellung), also hat  $r$  echte Teiler
- 2)  $\exists r \in M$ , so dass alle echten Teiler von  $r$  nicht mehr in  $M$  liegen (denn sonst nehme echten Teiler aus  $M$ , wiederhole das Verfahren, erhalte unendliche Teilerkette wo ich in jedem Schritt echte Teiler habe  $\nexists$  zur Annahme)

Also gegeben  $r$  wie in Beobachtung 2), dann ist jeder echte Teiler als Produkt von endlich vielen irreduziblen darstellbar, also auch  $r$  selbst. (Schreibe  $r = r_1 \cdot r_2$  mit  $r_1, r_2$  echte Teiler. Dann  $r_1 = a_1 \cdots a_n, r_2 = b_1 \cdots b_m$  mit  $\forall i, j \ a_i, b_j$  irreduzibel dann  $r = a_1 \cdots a_n b_1 \cdots b_m$ )  $\nexists$ . □

**Definition 2.16.** Sei  $R$  ein Integritätsring, sei  $r \in R, r \notin R^*, r \neq 0$ . Seien

$$r = a_1 \cdots a_n = b_1 \cdots b_m$$

zwei Darstellungen von  $r$  als Produkt von endlich vielen Irreduziblen.

Nenne die Darstellung äquivalent, falls gilt

- 1) gleich lang:  $n = m$
- 2)  $\exists$  Permutation  $\sigma \in S_n$  und Einheiten  $\varepsilon_1 \cdots \varepsilon_n \in R^*$  so dass  $\forall i : a_i = \varepsilon_i \cdot b_{\sigma(i)}$

*Bemerkung.* In Ringen, in denen der Teilerkettensatz gilt, sind Darstellungen nicht immer äquivalent! Zum Beispiel  $R = \mathbb{Z}\sqrt{-5}$ .

Das Problem ist, dass die irreduziblen Elemente in  $\mathbb{Z}[\sqrt{-5}]$  nicht unbedingt prim sind.

**Definition 2.17.** Sei  $R$  ein Integritätsring,  $r \in R, r \neq 0$  ein Element. Nenne  $r$  prim falls  $\forall a, b \in R$

$$r \mid (a \cdot b) \quad \implies \quad r \mid a \text{ oder } r \mid b$$

**Beispiel 2.18.** In  $R = \mathbb{Z}[\sqrt{-5}]$  ist  $(2 + \sqrt{-5})$  irreduzibel, aber nicht prim, denn  $(2 + \sqrt{-5}) \mid 3 \cdot 3$  aber  $(2 + \sqrt{-5}) \nmid 3$ .

**Lemma 2.19** (Elementare Rechenregeln für Prim-Elemente). Sei  $R$  ein Integritätsring,  $p, q \in R$

- 1)  $p$  prim  $\Rightarrow p$  irreduzibel
- 2)  $p$  prim,  $p \sim s \Rightarrow s$  prim
- 3)  $p, q$  prim und  $p \mid q \Rightarrow p \sim q$
- 4)  $p$  prim und  $p \mid a_1 \cdots a_n \Rightarrow \exists i \ p \mid a_i$

*Beweis.* zu 1)

Sei  $p$  prim. Angenommen  $p$  habe echten Teiler  $a \in R$ . Dann sei  $b \in R$  so dass  $p = a \cdot b$ , insbesondere  $p \mid ab$ . Also  $p \mid a$  oder  $p \mid b$ . oBdA gelte  $p \mid a$ .

Also  $\exists h \in R, p \cdot h = a$ . Einsetzen liefert

$$p = p \cdot h \cdot b \quad \iff \quad p(1 - hb) = 0 \quad \xLeftrightarrow[R \text{ Integritätsring}] \quad 1 = h \cdot b$$

$\Rightarrow b$  ist eine Einheit, kein echter Teiler. □

**Satz 2.20.** Im Ring  $\mathbb{Z}$  ist jedes irreduzible Element auch prim.

*Beweis.* Angenommen es existiert in  $\mathbb{Z}$  ein irreduzibles Element  $p$ , das nicht prim ist. Dann ist  $-p$  irreduzibel und auch nicht prim. Wir können also oBdA annehmen  $p > 0$ . Wir können auch annehmen das  $p$  das kleinste positive, irreduzible Element ist, das nicht prim ist.

Also  $\exists a, b \in \mathbb{N} : p \mid a \cdot b$  aber  $p \nmid a$  und  $p \nmid b$ .

Division mit Rest liefert

$$\begin{aligned} a &= x \cdot a + a' && \text{wobei } a' < p \\ b &= y \cdot p + b' && \text{wobei } b' < p \end{aligned}$$

Sehe sofort  $p \nmid a'$  und  $p \nmid b'$ .

Sehe auch  $a \cdot b = xyp^2 + (xb' + a'y)p + a'b'$  also  $p \mid a'b'$ .

Wähle also  $a, b$  so, dass  $ab$  minimal ist, und dann ist  $a < p, b < p, ab < p^2$ .

Finde  $h \in \mathbb{N} : p \cdot h = a \cdot b$ .

Sei jetzt  $p'$  ein irreduzibler Teiler von  $h, p' > 0$ . Dann existiert  $h' > 0, h = p' \cdot h'$  und  $p' \leq h < p$ . Nach Wahl von  $p$  (kleinstes irreduzibles das nicht prim ist) ist  $p'$  prim und  $p \cdot p' \cdot h' = a \cdot b$ .

Also gilt  $p' \mid a \cdot b \xRightarrow{p' \text{ prim}} p' \mid a$  oder  $p' \mid b$ . oBdA gelte  $p' \mid a$ . Finde also  $a' < a$  so dass  $p' \cdot a' = a$ . Einsetzen liefert

$$p \cdot p' \cdot h' = p' \cdot a' \cdot b \xRightarrow{\mathbb{Z} \text{ Integritätsring}} p \cdot h' = a'b \implies p \mid a'b$$

Da  $a'b < ab$  ist gilt nach Wahl von  $a \cdot b$  ( $a, b$  Gegenbeispiel zur Prim-Eigenschaft mit minimalem Produkt) also  $p \mid a'$  oder  $p \mid b$ . Da  $a' \mid a$  ist folgt  $p \mid a$  oder  $p \mid b$ .  $\nmid$   $\square$

**Satz 2.21.** Sei  $R$  ein Integritätsring. Dann ist äquivalent:

- 1) Jedes  $r \in R, r \notin R^*, r \neq 0$  ist als Produkt von endlich vielen Irreduziblen darstellbar und je zwei Darstellungen sind äquivalent.
- 2) In  $R$  gilt der Teilerkettensatz für Elemente und alle irreduziblen sind prim.

Falls diese Eigenschaften gelten, nenne  $R$  faktoriell oder UFD.

Beweis. 1)  $\Rightarrow$  2)

*Teilerkettensatz:* Sei  $(r_i)_{i \in \mathbb{N}}$  eine Teilerkette. Sei  $i$  so dass  $r_{i+1} \parallel r_i$  das heißt  $\exists h : h \notin R^*, h \neq 0 : r_{i+1} \cdot h = r_i$ .

Nach Annahme, kann  $r_i, r_{i+1}, h$  als Produkt von endlich vielen irreduziblen geschrieben werden

$$\begin{aligned} r_i &= a_1 \cdot a_n \\ r_{i+1} &= b_1 \cdots b_m \\ h &= c_1 \cdots c_k \end{aligned}$$

Dann gilt

$$\underbrace{b_1 \cdots b_m}_{\text{Darstellung von } r_{i+1}} \cdot c_1 \cdots c_k = \underbrace{a_1 \cdots a_n}_{\text{Darstellung von } r_i}$$

Da alle Darstellungen äquivalent sind, folgt  $n = m + k > m$ .

Also in der Teilerkette gibt es höchstens endlich viele echte Teiler, nämlich höchstens so viele, wie eine (jede) Darstellung von  $r_1$  lang ist.  $\Rightarrow$  Teilerkettensatz gilt

*Irreduzibel  $\Rightarrow$  Prim:* Sei  $r$  irreduzibel und seien  $a, b \in R \setminus \{0\}$  so dass  $r \mid ab$ . Also existiert  $h \in R \setminus \{0\}$ , so dass  $r \cdot h = a \cdot b$ . Wir wissen  $h, a, b$  haben Darstellung

$$a = a_1 \cdots a_n, \quad b = b_1 \cdots b_m, \quad h = h_1 \cdots h_k$$

Also

$$r \cdot h_1 \cdots h_k = a_1 \cdots a_n \cdot b_1 \cdots b_m$$

zwei Darstellungen von  $a \cdot b$ . Per Annahme sind diese Darstellungen äquivalent also  $\exists i : r \sim a_i$  oder  $\exists j : r \sim b_j$

$\Rightarrow r \mid a$  oder  $r \mid b$ . Also ist  $r$  prim.

2)  $\Rightarrow$  1)

Wir haben schon bewiesen: Teilerkettensatz  $\Rightarrow$  Darstellbarkeit, es fehlt noch die Äquivalenz  $\forall r \in R, r \notin R^*, r \neq 0$  und für alle Darstellungen  $r = a_1 \cdots a_n \stackrel{(*)}{=} b_1 \cdots b_m$  mit  $n \neq m$  gilt, dass beide Darstellungen äquivalent sind.

*Beweis per Induktion über  $n$*

Induktionsanfang:  $n = 1 : a_1 = b_1 \cdots b_m$

Per Annahme ist  $a_1$  prim, also  $\exists j : a_1 \mid b_j$ .

Rechenregeln:  $a_1 \sim b_j$ , insbesondere sind alle  $b_k, k \neq j$  schon Einheiten.  $\Rightarrow m = 1 = j$  (da die Faktoren in der Darstellung irreduzibel und keine Einheiten sind).

Induktionsschritt: Sei die Aussage für alle Zahlen  $< n$  schon bewiesen.

Wieder gilt  $a_1 \mid b_1 \cdots b_m \Rightarrow \exists j : a_1 \sim b_j$ . oBdA sei  $j = 1$  also existiert eine Einheit  $\varepsilon \in R^*$  so dass  $a_1 = \varepsilon b_1$ .

$R$  ist also Integritätsring, kann also in  $(*)$  kürzen, erhalte

$$a_2 \cdots a_n = (\varepsilon b_2) \cdot b_3 \cdots b_m$$

Per Induktionsannahme sind diese Darstellungen äquivalent. □

**Folgerung 2.22.**  $\mathbb{Z}$  ist faktoriell.