Algebra und Zahlentheorie

Wintersemester 2018/19
Mitschrift von Lukas Metzger

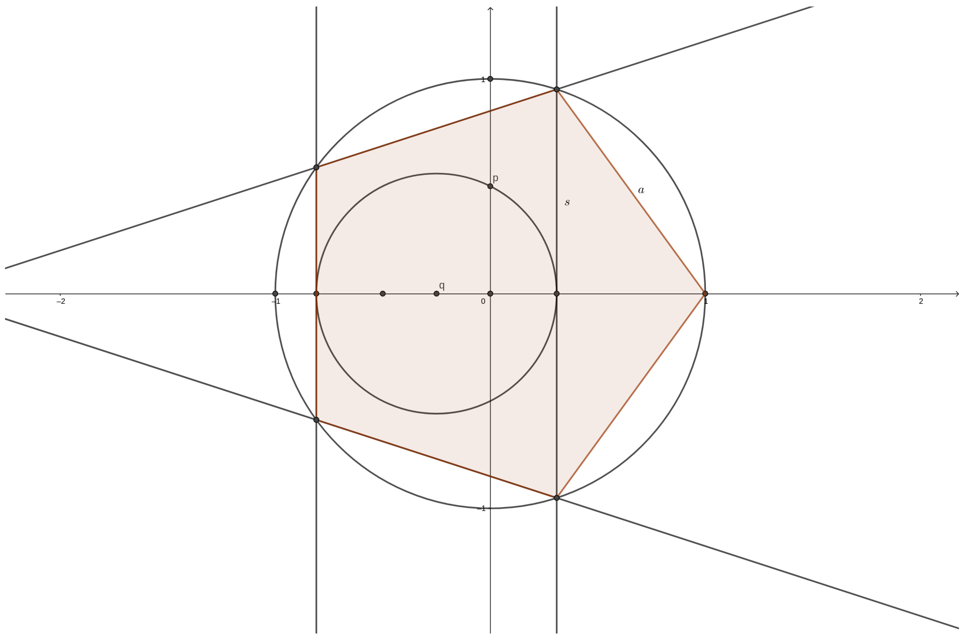
gehalten von Prof. Dr. Stefan Kebekus
Albert-Ludwigs-Universität Freiburg
Mathematisches Institut

29. Juli 2019

Inhaltsverzeichnis

0 Konstruktion mit Zirkel und Lineal

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



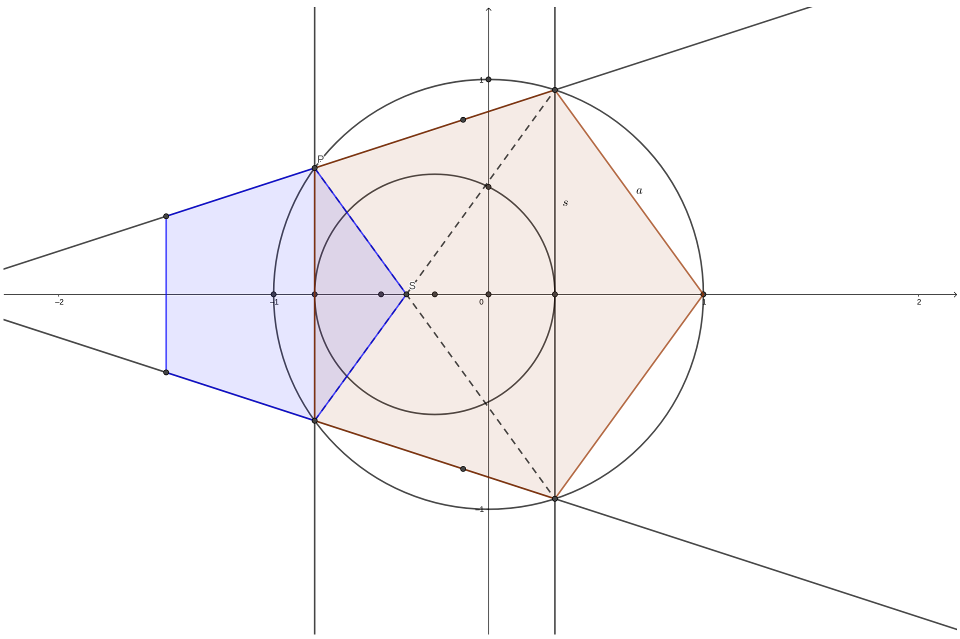
<ins>Erste Frage:</ins> Gegeben $n \in \mathbb{N}$, können wir das regelmäßige n-Eck konstruieren?

<ins>Beispielproblem:</ins> 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 $d \in \mathbb{R}$, sodass s und a beide 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 ein kleines 5-Eck (vgl. blaues 5-Eck in der Abbildung unten) mit Sekantenlänge $s' = a$ und Kantenlänge $a' = s - a$.



Dann sind aber sowohl a' als auch s' wieder Vielfache von d. Das Verfahren können wir wiederholen und erhalte immer kleinere 5-Ecke, deren Größe nach 0 konvergiert, wo Kanten- und Sekantenlänge ganzzahlige Vielfache von d sind. $\lightning$ $\square$

<u>Weitere Konstruktionsprobleme:</u>

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

<u>Wiederholung:</u> Was können wir 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 $\overline{b_1b_2}$ 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, können wir 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 $\Leftrightarrow$ Für gegebenes $\varphi \in (0, 2\pi)$ ist $e^{\frac{i\varphi}{3}} \in \text{Kons}(\{0, 1, e^{i\varphi}\})$

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 . . . (vgl. Übungsaufgabe!)

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 $m : G \times G \to G$ sodass 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) Abel'sch, 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:

- Abelsch: $(\mathbb{Z}, +)$, $(\mathbb{Z}/p\mathbb{Z}, +)$, $(Vektorraum, +)$

- Nicht-Abelsch: *Sei M eine Menge mit > 2 Elementen. Die bijektiven Abbildungen $M \to M$ mit der Hintereinanderausführung ist eine nicht-Abelsche Gruppe.*

- Nicht-Abelsch: *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: *$G = \mathbb{R}^3$. Wir erhalten durch das Kreuzprodukt keine Gruppenkonstruktion.*

Definition 1.5 (Ring)
Ein Ring ist eine Menge R mit 2 Verknüpfungen $+$ und $\cdot$ sodass gilt:

- $(R, +)$ *ist eine Abelsche Gruppe*
- *Distributivgesetz:* $\forall a, b, c \in R$ $(a + b) \cdot c = ac + bc$ *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 können wir fast rechnen wie mit Zahlen, aber ACHTUNG:

- Nicht jedes Element in $R \setminus 0$ hat ein multiplikatives Inverses
- Wir können aus $a \cdot b = 0$ und $a \neq 0$ im Allgemeinen nicht folgern, dass $b = 0$
- Wir können 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* $a \cdot b = 0$*, nennen wir* a *einen Nullteiler.*

Ringe ohne Nullteiler heißen nullteilerfrei oder Integritätsringe.

Definition 1.8 (Abelscher Ring)
Ein Ring heißt abel'sch, 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, wird 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*
- $\mathrm{Kons}(\{0, 1\})$ *ist Unterkörper von* $\mathbb{C}$
- *Die Menge der rationalen 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 $f \in k[x]$ und $f \neq 0$ gibt, sodass $f(a) = 0$.

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 minimalem 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 minimalen Grades 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 $f \in k[x] \setminus \{0\}$ sodass 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 $k \subseteq L_i \subseteq L$ sodass $\forall i : A \subset L_i$. 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 schreiben wir $k(a)$. 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, sodass $L = k(a)$.

Definition 1.19 (Grad der Körpererweiterung)

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

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 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

$$f(x) = x^n + b_{n-1} \cdot x^{n-1} + \cdots + b_0 \in k[x]$$

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 $g(x)$ mit $\deg(g) < n$ mit $g(a) = 0$ ↯.

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

Um Gleichheit zu zeigen, genügt es zu zeigen, dass $\langle 1, a, a^2, \dots, a^{n-1} \rangle_k =: \tilde{k}$ bereits $k(a)$. Klar ist $\tilde{k} \subseteq k(a)$. 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 bereits: $a \cdot s = \underbrace{\sum_{i=0}^{n-2} \lambda_i a^{i+1}}_{\in \tilde{k}} + \lambda_{n-1} a^n.$

Ein Blick auf das Minimalpolynom zeigt jetzt: $a^n = -\sum_{i=0}^{n-1} b_i \cdot a^i \in \tilde{k}$.

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

Beobachtung: $p_0 \neq 0$, denn sonst könnten wir x ausklammern, p wäre nicht minimal. Demnach können wir schreiben:

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

□

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

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

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, sodass 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 $\lambda_1, \lambda_0 \in k$, sodass $a^2 + \lambda_1 a + \lambda_0 = 0$ 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 $\mathrm{char}(k) = 2$ ist, muss man die Lösungsformel richtig hinschreiben.

Satz 1.25 (Gradformel)
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 können wir jedes λ_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

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

gegeben, wobei $\mu_{ij} \in k$. 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, dass $\sum_j \underbrace{\mu_{ij}}_{\in k} \cdot l_j = 0$.

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

Folgerung 1.26
Wenn eine Kette von Körpererweiterungen $k \subseteq L \subseteq M$ gegeben ist, 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 $a_1, \dots, a_n \in L$ sodass $L = k(a_1, \dots, a_n)$

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. <u>$1 \Rightarrow 2$:</u> 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.

<u>$2 \Rightarrow 3$:</u> trivial

<u>$3 \Rightarrow 1$:</u> Betrachte

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

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

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 1.27 ist $k(a, b)$ algebraisch über k. $\square$

Bemerkung: Achtung: Es gibt einen anderen Begriff des (absoluten) algebraischen Abschlusses, 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:

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

$$\begin{aligned} w_1 &= \sqrt{-3(a^2b^2 - 4a^3c - 4b^3 + 18abc - 27c^2)} \\ w_2 &= \sqrt[3]{h + \frac{1}{18}w_1} \\ w_2 &= \sqrt[3]{h - \frac{1}{18}w_1}. \end{aligned}$$

Dann ist

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

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

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

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

Definition 1.30
Sei L/k eine Körpererweiterung. Nenne diese Erweiterung Radikalerweiterung, falls es $a_1, \ldots, a_n \in L$ und $m_1, \ldots, m_n \in \mathbb{N}$ gibt, sodass

1) $L = k(a_1, \ldots, a_n)$

2) $\forall i : a_i^{m_i} \in k(a_1, \ldots, a_{i-1})$. Also a_i ist die m_i-te Wurzel eines Elementes aus $k(a_1, \ldots a_{i-1})$.

Was bedeutet das?

1) $a_1^{m_1} \in k$, also $k(a_1) = \langle 1, a_1, a_1^2, \ldots, a_1^{m_1-1} \rangle_k$

2) $a_2^{m_2} \in k(a_1)$, also $k(a_1, a_2) = \langle 1, a_2, a_2^2, \ldots, a_2^{m_2-1} \rangle_{k(a_1)}$

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 $L/\mathbb{Q}(a_0, \ldots, a_n)$ (beziehungsweise $L/\mathbb{R}$) sodass 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 wir suchen 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 $\deg \mathrm{rest}(x) < \deg f_a(x)$. Einsetzen von a ergibt

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

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

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

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 $R \to R$, 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 (Gradformel für Polynome)
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

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

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:

$$f \cdot g \not\equiv 0 \in R[x] \tag{$*$}$$

Falls $\deg f = \deg g = 0$, folgt $(*)$ weil R ein Integritätsring ist. Ansonsten folgt $(*)$, weil $\deg f \cdot g = \deg f + \deg g > 0$. □

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. □

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

Definition 2.6
Sei R ein Ring, seien $s, r \in R$ Elemente. Wir sagen: s ist Teiler von r (in Symbolen $s \mid r$), wenn es $a \in R$ gibt, sodass $s \cdot a = r$.

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, nennen wir s und r assoziiert *(in Symbolen $s \sim r$).*

Beweis. 1) $\Rightarrow$ 2)✓

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

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

Da R Integritätsring ist: $\Rightarrow b \cdot a = 1 \qquad \Rightarrow b, a \in R^*$

(geht so nur für $r \neq 0$, der Fall muss extra behandelt werden) □

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, sodass $\forall i : r_{i+1} \mid r_i$. Wir sagen, 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 $M = \{r \in R \mid r \notin R^*, r \neq 0 \text{ und } r \textit{ nicht} \text{ als Produkt von endlich vielen Irreduziblen darstellbar}\}$ leer ist. Widerspruchsbeweis: angenommen $M \neq \emptyset$.

Beobachtungen:

1) $\forall r \in M$ gilt: r ist nicht irreduzibel (denn sonst wäre r eine Darstellung), also hat r echte Teiler

2) $\exists r \in M$, sodass alle echten Teiler von r nicht mehr in M liegen (denn sonst nehme echten Teiler aus M, wiederhole das Verfahren, erhalte unendliche Teilerkette wo wir in jedem Schritt echte Teiler haben, $\lightning$ 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 $r_1 = a_1 \cdots a_n, r_2 = b_1 \dots b_m$ mit $\forall i, j : a_i, b_j$ irreduzibel, dann $r = a_1 \dots a_n b_1 \dots b_m$) $\lightning$. □

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 $\varepsilon_1 \cdots \varepsilon_n \in R^*$ sodass $\forall i : a_i = \varepsilon_i \cdot b_{\sigma(i)}$

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 $\forall a, b \in R$

$$r \mid (a \cdot b) \qquad \Longrightarrow \qquad r \mid a \text{ oder } r \mid b$$

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 $b \in R$ sodass $p = a \cdot b$, 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

$$p = p \cdot h \cdot b \qquad \Longleftrightarrow \qquad p(1 - hb) = 0 \qquad \underset{R \text{ Integritätsring}}{\Longleftrightarrow} \qquad 1 = h \cdot b$$

$\Rightarrow b$ 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, dass 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

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

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 $a \cdot b$ 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 $p' \mid a \cdot b \underset{p' prim}{\Rightarrow} p' \mid a$ oder $p' \mid b$. oBdA gelte $p' \mid a$. Finde also $a' < a$ sodass $p' \cdot a' = a$. Einsetzen liefert

$$p \cdot p' \cdot h' = p' \cdot a' \cdot b \underset{\mathbb{Z} \text{ Integritätsring}}{\Longrightarrow} p \cdot h' = a'b \qquad \Longrightarrow \qquad p \mid a'b$$

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 $p \mid b$. ↯ □

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 sodass $r_{i+1} \parallel r_i$, das heißt $\exists h : h \notin R^*, h \neq 0 : r_{i+1} \cdot h = r_i$.

Nach Annahme können r_i, r_{i+1}, h als Produkt von endlich vielen Irreduziblen geschrieben werden:

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

Dann gilt

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

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 $a, b \in R \setminus \{0\}$ sodass $r \mid ab$. Also existiert $h \in R \setminus \{0\}$, sodass $r \cdot h = a \cdot b$. Wir wissen h, a, b haben Darstellung

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

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.

<u>2) $\Rightarrow$ 1)</u>

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 $r = \underbrace{a_1 \cdots a_n = b_1 \cdots b_m}_{(*)}$ 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 $\varepsilon \in R^*$ sodass $a_1 = \varepsilon b_1$.

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.

Folgerung 2.23
Alle Körper sind faktoriell.

Satz 2.24 (Gauß)
Wenn R ein faktorieller Ring ist, dann auch $R[x]$.

Und damit auch $(R[x])[y] = R[x, y]$ und auch $R[x_1, \dots, x_n]\ \forall n \in \mathbb{N}$.

Beweis. Wir müssen zeigen:

1) In $R[x]$ gilt der Teilerkettensatz

2) Je zwei Darstellungen sind äquivalent

zu 1): Wenn $r(x), s(x) \in R[x]$ und $r(x) \parallel s(x)$, dann $\deg r(x) < \deg s(x)$ oder $\exists a \in R \setminus R^*, a \neq 0 : a \cdot r(x) = s(x)$.

$\Rightarrow$ alle Koeffizienten von s werden von a geteilt. In R gilt aber der Teilerkettensatz!

Hausaufgabe: Also gilt der Teilerkettensatz auch in $R[x]$.

zu 2): Widerspruchsbeweis! Angenommen es gibt $r(x) \in R[x], r \neq 0, r \notin R[x]^* = R^*$ sodass r zwei Darstellungen hat, die nicht äquivalent sind

$$r(x) = p_1(x) \cdots p_\alpha(x) = q_1(x) \cdots q_\beta(x) \qquad (*)$$

Wir können oBdA einige Annahmen treffen

- $\deg(r(x))$ ist minimal unter allen Polynomen, die nicht äquivalente Darstellungen haben
- die irreduziblen Polynome $p_1, \dots, p_\alpha, q_1, \dots, q_\beta$ sind nach Graden sortiert, also $\deg p_1 \geq \deg p_2 \geq \dots \geq \deg p_\alpha$ und $\deg q_1 \geq \deg q_2 \geq \dots \geq \deg q_\beta$
- $\deg q_1 \geq \deg p_1$

Sei $n := \deg p_1, m := \deg q_1$. Seien a, b die Leitkoeffizienten von p_1 beziehungsweise q_1. Das heißt:

$$p_1 = a \cdot x^n + (\text{lot})$$
$$p_1 = b \cdot x^m + (\text{lot})$$

Beobachtungen:

- $\deg r(x) > 0$, denn sonst wären $r(x)$ und alle $q_i(x), p_j(x)$ konstant, also in R. Per Annahme das R faktoriell ist, müssten die Darstellungen dann äquivalent sein.

  $\Rightarrow n > 0$ und $m > 0$

- Angenommen es gäbe ein j, sodass $p_1 \sim q_j$. Dann könnten wir in $(*)$ auf beiden Seiten p_1 kürzen und erhielten Polynom vom Grad $(\deg r(x)) - n < \deg r(x)$, das zwei nicht äquivalente Darstellungen hat. $\lightning$ zur Minimalität von $\deg r(x)$.

Betrachte Hilfspolynom:

$$s(x) = \underbrace{\left[b \cdot p_1(x) \cdot x^{m-n} - a \cdot q_1(x)\right]}_{\deg(\cdot) < \deg q_1(x)} \cdot q_2 \cdots q_\beta \tag{☼}$$

Wir erhalten zwei offensichtliche Fälle:

1) $s(x) = 0$: Dann ist
$$b \cdot p_1(x) \cdot x^{m-n} - a \cdot q_1(x) = 0$$

2) $s(x) \neq 0$: Wir sehen $\deg s(x) < \deg r(x)$. Also sind je zwei Darstellungen von $s(x)$ äquivalent! Schreibe $s(x)$ um:
$$\begin{aligned} s(x) &= b \cdot p_1(x) x^{m-n} \cdot q_2 \cdots q_\beta - a \underbrace{q_1 \cdots q_\beta}_{r(x)} \\ &= b \cdot p_1 x^{m-n} \cdot q_2 \cdots q_\beta - a \cdot p_1 \cdots p_\alpha \\ &= p_1(x) \left[b \cdot x^{m-n} \cdot q_2(x) \cdots q_\beta(x) - a \cdot p_2(x) \cdots p_\alpha(x)\right] \end{aligned} \tag{☾}$$

Wir können die Ausdrücke (☼) und (☾) verfeinern zu Produkten von Irreduziblen, indem wir die Ausdrücke in $[\dots]$ als Produkt von Irreduziblen schreiben. Diese Darstellungen von $s(x)$ müssen dann per Annahme äquivalent sein.

Konsequenz: In der Darstellung von (☼) muss es einen Faktor geben, der zu p_1 assoziiert ist. Da $p_1 \nsim q_2 \dots p_1 \nsim q_\beta$, muss p_1 ein Primfaktor vom $[\dots]$-Ausdruck in (☼) sein.

$$\Rightarrow \qquad p_1 \mid (bp_1 \cdot x^{m-n} - aq_1) \qquad \Rightarrow p_1 \mid aq_1$$

Insgesamt ergibt sich in jedem der beiden Fälle:

$$\exists h \in R[x]: \quad p_1(x) \cdot h(x) = a \cdot q_1(x) \tag{♠}$$

Beobachte: Wenn $a \in R^*$, dann $p_1 \mid q_1$ und $p_1 \sim q_1$ $\lightning$. Also ist $a \in R \setminus R^*, a \neq 0$.

Zwischenbehauptung (Beweis später): Sei $p \in R$ irreduzibel. Dann ist das konstante Polynom $p \in R[x]$ prim.

Anwendung der Zwischenbehauptung: Schreibe a als Produkt von Irreduziblen. Wenn jetzt p einer der irreduziblen Faktoren ist, dann $p \mid p_1 \cdot h$.

$$\Rightarrow \quad \underbrace{p \mid p_1}_{\substack{\text{kann nicht sein, denn } p_1 \text{ ist irreduzibel,}\\ \text{hat also überhaupt keine echten Teiler.}}} \quad \text{oder } p \mid h.$$

Also können wir p aus ($\spadesuit$) herausteilen und erhalten:

$$p_1 \cdot \frac{h}{p} = \frac{a}{p} \cdot q_1$$

Das geht mit jedem Primfaktor von a, erhalte also am Ende:

$$p_1 \cdot \frac{h}{a} = q_1 \qquad \Rightarrow p_1 \mid q_1 \qquad \Rightarrow p_1 \sim q_1 \qquad \Rightarrow \lightning$$

Zwischenbehauptung (jetzt der Beweis): Sei $p \in R$ irreduzibel. Dann ist das konstante Polynom $p \in R[x]$ prim.

Sei $p \in R$ irreduzibel. Wir zeigen die Kontraposition: wenn $a(x), b(x) \in R[x]$ Polynome sind mit $p \nmid a(x)$ und $p \nmid b(x)$, dann gilt $p \nmid (a \cdot b)(x)$

Seien also $a(x), b(x)$ gegeben. Schreibe

$$\begin{aligned} a(x) &= a_0 + a_1 x + \cdots + a_n x^n \\ b(x) &= b_0 + b_1 x + \cdots + b_m x^m \end{aligned}$$

Erinnere: $p \mid a(x) \Leftrightarrow \forall i : p \mid a_i$

Kann also minimale Indizes i und j wählen, sodass $p \nmid a_i$ und $p \nmid b_j$. Betrachte Produktpolynom $(a \cdot b)(x)$ und rechne den Koeffizienten von x^{i+j} im Produktpolynom aus. Dieser Koeffizient ist

$$\gamma := \sum_{\substack{\alpha+\beta=i+j\\ \alpha,\beta\in\mathbb{N}}} a_\alpha \cdot b_\beta$$

In dieser Summe sind alle Summanden durch p teilbar, weil stets $\alpha < i$ oder $\beta < j$ gilt, mit der Ausnahme des Summanden $\alpha = i, \beta = j, (= a_i \cdot b_j)$.

Weil R per Annahme faktoriell ist, und $p \in R$ deshalb prim ist, folgt $p \nmid a_i \cdot b_j$

$\Rightarrow p \nmid \gamma \qquad \Rightarrow p \nmid (a \cdot b)(x)$ $\square$

Was tun wir mit faktoriellen Ringen?

Sei R ein faktorieller Ring. Betrachte die Äquivalenzrelation $a \sim b \Leftrightarrow a$ assoziiert zu b.

Wähle Repräsentantensystem $P \subset R$ für die irreduziblen Elemente (= zu jedem irreduziblen $a \in R$ gibt es genau ein $b \in P$ mit $a \sim b$).

Wenn dann irgendein $a \in R$ gegeben ist, dann können wir schreiben:

$$a = \varepsilon \cdot \prod_{p \in P} p^{\alpha_p}$$

wobei $\varepsilon \in R^*, \alpha_p \in \mathbb{N}$ und alle bis auf endlich viele $\alpha_p = 0$.

Teilbarkeit wird dann ganz einfach. Seien $a, b \in R$

$$a = \varepsilon_a \cdot \prod_{p \in P} p^{\alpha_{a,p}}, \qquad b = \varepsilon_b \cdot \prod_{p \in P} p^{\alpha_{b,p}}$$

und

$$\begin{aligned} a \mid b &\Leftrightarrow \forall p \in P : \alpha_{a,p} \le \alpha_{b,p} \\ a \parallel b &\Leftrightarrow (\forall p \in P : \alpha_{a,p} \le \alpha_{b,p}) \quad \& \quad (\exists p \in P : \alpha_{a,p} < \alpha_{b,p}) \\ a \sim b &\Leftrightarrow \forall p \in P : \alpha_{a,p} = \alpha_{b,p} \end{aligned}$$

Weiter mit Grundschulstoff:

Sei R ein Integritätsring, seien $a, b \in R \setminus R^*, a \cdot b \neq 0$

1) Ein Element $c \in R$ heißt *größter gemeinsamer Teiler (ggT)*, wenn gilt: $c \mid a$ und $c \mid b$ und wenn für jedes andere c' mit $c' \mid a$ und $c' \mid b$ gilt: $c' \mid c$.

2) Ein Element $c \in R$ heißt *kleinstes gemeinsames Vielfaches (kgV)*, wenn $a \mid c$ und $b \mid c$ ist und für alle $c' \in R$ mit $a \mid c'$ und $b \mid c'$ gilt: $c \mid c'$.

Satz 2.25
Sei R faktoriell. Seien $a, b \in R$ dann existieren ggT und kgV.

Beweis. Wähle Repräsentantensystem $P \subset R$. Schreibe

$$a = \varepsilon_a \cdot \prod_{p \in P} p^{\alpha_{a,p}}, \qquad b = \varepsilon_b \cdot \prod_{p \in P} p^{\alpha_{b,p}}$$

Setze

$$\operatorname{ggT}(a,b) \coloneqq \prod_{p\in P} p^{\min(\alpha_{a,p},\alpha_{b,p})}$$

und

$$\operatorname{kgV}(a,b) \coloneqq \prod_{p\in P} p^{\max(\alpha_{a,p},\alpha_{b,p})}$$

Blick nach oben zeigt, dass dies exakt die Bedingungen erfüllt. □

Satz 2.26
Seien $f, g \in k[x]$ Polynome. Betrachte Divisionsreste

$$f = q_1 \cdot g + r_1 \tag{1}$$
$$g = q_2 \cdot r_1 + r_2 \tag{2}$$

Definiere dann induktiv Polynome r_n als Divisionsrest

$$r_{n-2} = q_n \cdot r_{n-1} + r_n \tag{n}$$

Beobachtung: Die Grade der Polynome $r_1, r_2, \dots$ werden immer kleiner. Der Prozess stoppt also nach endlich vielen Schritten, das heißt irgendwann geht die Division auf. Es existiert also $n \in \mathbb{N}$ sodass

$$r_{n-1} = q_{n+1} \cdot r_n + 0 \tag{n+1}$$

Dann ist $r_n = \operatorname{ggT}(f,g)$.

Beweis. 1) Wenn t ein gemeinsamer Teiler von f, g ist

$$\overset{(1)}{\Longrightarrow} t \mid r_1 \qquad \dots \qquad \overset{(n)}{\Longrightarrow} t \mid r_n$$
$$\overset{(2)}{\Longrightarrow} t \mid r_2$$

2) Andere Richtung analog:

$$\begin{aligned} (n+1) &\Longrightarrow r_n \mid r_{n-1} \\ (n) &\Longrightarrow r_n \mid r_{n-2} \\ &\vdots \\ (2) &\Longrightarrow r_n \mid g \\ (1) &\Longrightarrow r_n \mid f \end{aligned}$$

Da $k[t]$ faktoriell ist genügen 1) + 2) um $r_n = \operatorname{ggT}$ zu zeigen.

□

2.2 Der Quotientenkörper eines Integritätsrings

Ziel: Gegeben ein Ring R, suche einen möglichst kleinen Körper k sodass: $R \subset k$ (besser: sodass es einen injektiven Ringmorphismus $R \hookrightarrow k$ gibt). Wir denken an $\mathbb{Z} \hookrightarrow \mathbb{Q}$.

Beobachtung: So etwas kann es nicht geben, wenn R Nullteiler hat! Betrachte also nur Integritätsringe.

Definition 2.27
Sei R ein Integritätsring. Ein Quotientenkörper *von R ist ein Körper k zusammen mit einem injektiven Ringmorphismus $\varphi : R \to k$, sodass folgende (universelle) Eigenschaft gilt: Wann immer $\Phi : R \to L$ ein injektiver Ringmorphismus in einen Körper ist, dann gibt es genau einen Körpermorphismus $\eta : k \to L$, sodass das folgende Diagramm kommutiert.*

$$\begin{tikzcd} R \arrow[r, "\varphi"] \arrow[d, dash, "\mathbb{1}_R"'] & k \arrow[d, "\exists!\eta"] \\ R \arrow[r, "\Phi"'] & L \end{tikzcd}$$

Bemerkung: Körpermorphismen $k \xrightarrow{\eta} L$ sind immer injektiv! Denn wäre $a \in k \setminus \{0\}, a \in \ker(\eta)$, dann

$$1_L = \eta(1_k) = \eta(a \cdot a^{-1}) = \underbrace{\eta(a)}_{=0_L} \cdot \eta(a^{-1}) = 0_L$$

Widerspruch!

Satz 2.28
Sei R ein Integritätsring. Dann existiert ein Quotientenkörper $(k, \varphi : R \to k)$. Dieser ist eindeutig bis auf kanonische Isomorphie. Das bedeutet: Wenn $(k', \varphi' : R \to k')$ ein weiterer Quotientenkörper ist, dann existiert genau ein Körperisomorphismus $\eta : k \to k'$ sodass das folgende Diagramm kommutiert.

$$\begin{tikzcd} R \arrow[r, "\varphi"] \arrow[d, dash, "\mathbb{1}_R"'] & k \arrow[d, "\exists!\eta"] \\ R \arrow[r, "\varphi'"'] & k' \end{tikzcd}$$

Beweis. Eindeutigkeit: Seien Quotientenkörper $(k, \varphi : R \to k)$ sowie $(k', \varphi' : R \to k')$ gegeben. Nach der universellen Eigenschaft existiert dann genau ein Körpermorphismus $\eta : k \to k'$ sodass das folgende Diagramm kommutiert:

$$\begin{tikzcd}
R \arrow[r, "\varphi"] \arrow[d, dash, "\mathbb{1}_R"'] & k \arrow[d, "\eta"] \\
R \arrow[r, "\varphi'"'] & k'
\end{tikzcd}$$

Wir wissen auch: Weil k' Quotientenkörper ist, existiert genau ein Körpermorphismus $\eta' : k' \to k$ sodass das folgende Diagramm kommutiert:

$$\begin{tikzcd}
R \arrow[r, "\varphi"] \arrow[d, dash, "\mathbb{1}_R"'] & k \arrow[d, "\eta"] \\
R \arrow[r, "\varphi'"'] \arrow[d, dash, "\mathbb{1}_R"'] & k' \arrow[d, "\eta'"] \\
R \arrow[r, "\varphi"'] & k
\end{tikzcd}$$

Die universelle Eigenschaft angewandt auf

$$\begin{tikzcd}
R \arrow[r, "\varphi"] \arrow[d, dash, "\mathbb{1}_R"'] & k \arrow[dd, "\mathbb{1}_k"', "\eta' \circ \eta"] \\
R \arrow[d, dash, "\mathbb{1}_R"'] & \\
R \arrow[r, "\varphi"'] & k
\end{tikzcd}$$

zeigt: $\eta' \circ \eta = \mathbb{1}_k$.

Genauso folgt $\eta \circ \eta' = \mathbb{1}_{k'}$. Also ist der Körpermorphismus η' die Umkehrung von η.

<u>Existenz:</u> Wir konstruieren den Quotientenkörper wie folgt:

1) Betrachte die Menge
$$B = \{(a, b) \in R \times R \mid b \neq 0\}$$
und sage (a, b) ist äquivalent zu (a', b') wenn gilt $ab' = a'b$. Das ist eine Äquivalenzrelation. Symmetrie und Reflexivität sind klar per Definition. Wir müssen also

noch die Transitivität zeigen: Seien also Tupel gegeben, sodass

$$\begin{aligned} & (a,b) \sim (a',b') && (a',b') \sim (a'',b'') \\ \Leftrightarrow \quad & ab' = a'b && a'b'' = a''b' \end{aligned}$$

Und damit dann

$$\Rightarrow \quad ab' \cdot a'b'' = a'b \cdot a''b'$$

Im Integritätsring falls $a' \neq 0$

$$\Rightarrow \quad ab'' = a''b \quad \Leftrightarrow \quad (a,b) \sim (a'',b'')$$

Falls $a' = 0$ ist der Beweis sowieso einfach.

Definiere als Menge

$$k := B/\sim$$

Notation: Die Äquivalenzklasse von (a,b) wird mit $\frac{a}{b}$ bezeichnet.

Betrachte die Abbildung $\varphi : R \to k, a \mapsto \frac{a}{1}$. Diese Abbildung ist injektiv, denn

$$\varphi(a) = \varphi(a') \quad \Leftrightarrow \quad \frac{a}{1} = \frac{a'}{1} \quad \overset{\text{Def.}}{\Leftrightarrow} \quad a \cdot 1 = a' \cdot 1 \quad \Leftrightarrow \quad a = a'$$

2) Definiere auf k die Struktur eines Körpers mit Verknüpfungen

$$\begin{aligned} \cdot : k \times k \to k, \quad & \left(\frac{a}{b}, \frac{c}{d}\right) \mapsto \frac{ac}{bd} \\ + : k \times k \to k, \quad & \left(\frac{a}{b}, \frac{c}{d}\right) \mapsto \frac{ad+cb}{bd} \end{aligned}$$

Muss noch nachrechnen: Wohldefiniertheit

Das bedeutet: Gegeben $\frac{a}{b}$ und $\frac{c}{d}$ sowie $\frac{a'}{b'}$ und $\frac{c'}{d'}$ mit $\frac{a}{b} = \frac{a'}{b'}$ sowie $\frac{c}{d} = \frac{c'}{d'}$, dann gilt $\frac{ad+cb}{bd} = \frac{a'd'+c'b'}{b'd'}$

$$\begin{aligned} \Leftrightarrow \quad & (ad+cb) \cdot b'd' = (a'd'+c'b') \cdot bd \\ \Leftrightarrow \quad & adb'd' + cbb'd' = a'd'bd + c'b'bd \end{aligned}$$

Wir wissen $ab' = a'b$ und $cd' = c'd$

$$\Leftrightarrow \quad 0 = 0$$

Die Addition ist wohldefiniert.

Hausaufgabe: Dasselbe für Multiplikation

Lästige Rechnerei: Diese Verknüpfungen definieren eine Körperstruktur auf k, sodass die Abbildung $\varphi : R \to k$ ein Ringmorphismus ist. Es gilt

$$0_k = \frac{0}{1} \qquad 1_k = \frac{1}{1} \qquad \text{falls } a \neq 0 \text{ dann } \left(\frac{a}{b}\right)^{-1} = \frac{b}{a}$$

3) Beweis der *universellen Eigenschaft*

Sei Körper L gegeben und ein injektiver Ringmorphismus $\Phi : R \to L$, dann müssen wir zeigen $\exists! \eta : k \to L$ sodass ...
<u>Eindeutigkeit:</u> Angenommen wir hätten η sodass das folgende Diagramm kommutiert

$$\begin{tikzcd} R \arrow[r, "\varphi"] \arrow[d, dash, "\mathbb{1}_R"'] & k \arrow[d, "\exists!\eta"] \\ R \arrow[r, "\Phi"'] & L \end{tikzcd}$$

dann gilt für alle $a \in R$

$$\eta(\varphi(a)) = \Phi(\mathbb{1}_R(a)) \Leftrightarrow \eta\left(\frac{a}{1}\right) = \Phi(a)$$

Falls $a \neq 0$ ist gilt

$$\eta\left(\frac{1}{a}\right) = \eta\left(\left(\frac{a}{1}\right)^{-1}\right) \overset{\substack{\text{Körper-}\\\text{morphismus}}}{=} \eta\left(\frac{a}{1}\right)^{-1}$$

also gilt für alle $\frac{a}{b} \in k$

$$\eta\left(\frac{a}{b}\right) = \eta\left(\frac{a}{1} \cdot \frac{1}{b}\right) = \eta\left(\frac{a}{1}\right) \cdot \eta\left(\frac{1}{b}\right) = \Phi(a) \cdot (\Phi(b))^{-1}$$

also ist η eindeutig.

<u>Existenz:</u> Definiere $\eta : k \to L, \quad \frac{a}{b} \mapsto \Phi(a) \cdot \Phi(b)^{-1}$.

Wieder ist auf Wohldefiniertheit zu prüfen: Seien dazu $\frac{a}{b} = \frac{a'}{b'}$. Wir müssen zeigen:

$$\begin{aligned} & & \Phi(a) \cdot \Phi(b)^{-1} &= \Phi(a') \cdot \Phi(b')^{-1} \\ &\Leftrightarrow & \Phi(a) \cdot \Phi(b') &= \Phi(a') \cdot \Phi(b) \\ &\Leftrightarrow (\Phi \text{ ist Ringmorphismus}) & \Phi(ab') &= \Phi(a'b) \\ &\Leftrightarrow & &\text{wahr, wegen Annahme} \end{aligned}$$

Nachrechnen: das ist ein Körpermorphismus.

□

Beispiel 2.29

- *$R = \mathbb{Z}$. Dann ist $Q(\mathbb{Z}) = \mathbb{Q}$*

- *Ist R ein Körper, dann ist $Q(R) = R$*

- *$R = \mathbb{Z}[2+\sqrt{-5}]$, dann ist $Q(R) = \mathbb{Q}(2+\sqrt{-5}) \subset \mathbb{C}$*

  Grund: Wir haben eine Inklusion $R \subset \mathbb{Q}(2+\sqrt{-5})$. Deshalb gibt es einen Körpermorphismus $Q(R) \to \mathbb{Q}(2+\sqrt{-5})$.

  Dieser ist injektiv, denn $Q(R)$ enthält das Element $a = 2+\sqrt{-5}$. Wir wissen aber, dass $\mathbb{Q}(2+\sqrt{-5})$ der kleinste Körper ist, der dieses Element enthält.

- *Sei R faktoriell. Wähle Repräsentantensystem $P \subset R$. Dann können wir alle Elemente von $Q(R)$ auf eindeutige Weise schreiben als $\varepsilon \cdot \prod_{p \in P} p^{\alpha_p}$, wobei $\varepsilon \in R^*, \alpha_p \in \mathbb{Z}$ und fast alle $\alpha_p = 0$.*

<u>Warum das alles?</u>

Wenn R faktoriell ist, können wir manchmal entscheiden, ob Polynome in $R[x]$ irreduzibel sind.

Beispiel: $f(x) = x^3 - 2 \in \mathbb{Z}[x]$

Behauptung: f ist irreduzibel in $\mathbb{Z}[x]$

Angenommen es gäbe einen echten Teiler, dann gäbe es einen linearen Teiler, das heißt

$$\exists a, b \in \mathbb{Z}, a \neq 0 : f(x) = (ax+b)g(x)$$

wobei $g(x)$ quadratisch in $\mathbb{Z}[x]$.

Sehe sofort: $a \in \{\pm 1\}, b \in \{\pm 1, \pm 2\}$

Nachrechnen: keine dieser Möglichkeiten ist ein Teiler

Der folgende Satz zeigt, dass f auch in $\mathbb{Q}[x]$ irreduzibel ist.

Satz 2.30 (Satz von Gauß)
Sei R ein faktorieller Ring. Falls $f(x) \in R[x]$ irreduzibel als Element von $R[x]$, dann ist f auch irreduzibel als Element von $Q(R)[x]$.

<u>Vorbemerkung:</u> Sei $f \in Q(R)[x]$ irgendein Polynom. Dann existiert $a \in Q(R)$, sodass $a \cdot f(x) \subset R[x]$ und ggT(Koeffizienten von $a \cdot f(x)$) $= 1$ (Koeffizienten sind teilerfremd).

Beweis dazu: Auf Hauptnenner bringen und durch größten gemeinsamen Teiler der Koeffizienten teilen.

Beweis. Angenommen wir haben $f(x) \in R[x]$ welches als Polynom in $Q(R)[x]$ reduzibel ist. Das heißt es existieren Polynome $q(x), p(x) \in Q(R)[x]$ mit q, p nicht konstant, sodass $f(x) = q(x) \cdot p(x)$.

Ziel: Schreibe f als Produkt $f = q'(x) \cdot p'(x)$ wobei $q', p' \in R[x]$ echte Teiler sind.

Beobachtung: Wenn $\gamma \in R$ jeden Koeffizienten von f teilt und $\gamma \notin R^*, \gamma \neq 0$, dann ist γ ein echter Teiler von f und wir sind fertig. Wir nehmen also ab sofort an, dass die Koeffizienten von f teilerfremd sind.

Wende Vorbemerkung auf Polynome $p(x), q(x)$ an und erhalte $a, b \in Q(R)$, sodass $a \cdot p(x) \in R[x]$ und $b \cdot q(x) \in R[x]$ und Koeffizienten dieser Polynome jeweils teilerfremd in R sind.

Durch Multiplikation erhalten wir die Gleichung

$$a \cdot b \cdot f(x) = a \cdot p(x) \cdot b \cdot q(x) \in R[x] \tag{$*$}$$

Beachte: die linke Seite ist in $R[x]$, weil beide Faktoren der rechten Seite in $R[x]$ sind.

Behauptung: Es ist $a \cdot b \in R$.

Beweis: Angenommen $a \cdot b \notin R$, das heißt es existiert ein Primelement $p \in R$, welches in der Darstellung von $a \cdot b$ mit negativem Exponenten auftritt. Da aber $a \cdot b \cdot f(x) \in R[x]$, muss die Darstellung jedes Koeffizienten das Element p mit positivem Exponenten enthalten. Also $p \mid$ Koeffizienten $\lightning$ zu ggT(Koeffizienten) $= 1$.

Behauptung: Es gilt sogar $a \cdot b \in R^*$

Beweis: Angenommen $a \cdot b \notin R^*$. Dann hätten wir einen echten irreduziblen Teiler $\gamma \in R$ irreduzibel mit $\gamma \mid a \cdot b$.

$$\Rightarrow \gamma \mid a \cdot b \cdot f(x) \qquad \Rightarrow \gamma \mid [a \cdot p(x)][b \cdot q(x)]$$

Erinnerung: $\gamma \in R$ irreduzibel $\Rightarrow \gamma$ prim in $R[x]$.

Also gilt

$$\gamma \mid a \cdot p(x) \qquad \text{oder} \qquad \gamma \mid b \cdot q(x)$$

oBdA sei $\gamma \mid a \cdot p(x)$ $\lightning$ zur Wahl von a.

Damit können wir $(*)$ umschreiben zu

$$f(x) = \underbrace{\left[(a \cdot b)^{-1} \cdot a \cdot p(x)\right]}_{\in R[x]} \cdot \underbrace{[b \cdot q(x)]}_{\in R[x]}$$

$\square$

<u>Zusammenfassung:</u> Wir sind jetzt in der Lage, für ganzzahlige Polynome zu entscheiden, ob sie in $\mathbb{Q}[x]$ irreduzibel sind. (z.B. $x^3 - 2$ ist irreduzibel in $\mathbb{Q}[x]$, Folgerung: $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$, denn wir wissen jetzt, dass $x^3 - 2$ das Minimalpolynom von $\sqrt[3]{2}$ ist)

<u>Erinnerung:</u> Das geht so:

Lagrangesche Interpolationsformel (= Polynom von Grad $\leq n$ ist durch seine Werte an $n+1$ Stellen festgelegt) Sei k Körper, $f(x) \in k[x]$ Polynome von Grad $\leq n$, seien $a_1, \ldots, a_{n+1} \in k$ unterschiedliche Körperelemente. Dann ist f durch die Werte $f(a_i)$ eindeutig festgelegt, nämlich

$$f(x) = \sum_{j=1}^{n+1} f(a_j) \prod_{k \neq j} \frac{x - a_k}{a_j - a_k} =: h(x) \in k[x]$$

Dann gilt für alle i

$$h(a_i) = \sum_{j=1}^{n+1} f(a_j) \prod_{k \neq j} \frac{a_i - a_k}{a_j - a_k} = f(a_i) \prod_{k \neq i} \frac{a_i - a_k}{a_i - a_k} = f(a_i)$$

$\Rightarrow h - f$ ist Polynom von Grad $\leq n$ mit Nullstellen $a_1, \ldots, a_{n+1}$

$\Rightarrow h - f = 0$

Damit haben wir folgendes Verfahren, um Irreduzibilität in $\mathbb{Z}[x]$ und also auch in $\mathbb{Q}[x]$ zu testen:

Gegeben $f(x) \in \mathbb{Z}[x]$ von Grad $\leq n$ so, dass ggT(Koeffizienten) $= 1$.

Wähle $a_1, \ldots, a_{n+1} \in \mathbb{Z}$ so, dass $f(a_i) \neq 0$ und betrachte $f(a_1), \ldots, f(a_n) \in \mathbb{Z}$.

Wir wissen, wenn $g(x)$ ein Teiler von $f(x)$ in $\mathbb{Z}[x]$ ist, dann gilt für alle $i : q(a_i) \mid f(a_i)$

Für $g(a_i)$ gibt es also nur endlich viele Möglichkeiten.

Nur endlich viele Polynome kommen als Teiler in Frage. Wir müssen also durch Polynomdivision testen, ob die Kandidatenpolynome tatsächlich Teiler sind.

Satz 2.31 (Eisenstein-Kriterium)
Sei R ein faktorieller Ring, sei

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n \in R[x]$$

mit $n > 0$ und $\mathrm{ggT}(a_0, \ldots, a_n) = 1$. Falls es ein irreduzibles $p \in R$ gibt, sodass $p \mid a_0, p \mid a_1, \ldots, p \mid a_{n-1}$ und $p^2 \nmid a_0$, dann ist f irreduzibel in $R[x]$ und also auch in $Q(R)[x]$.

Beweis. Sei f wie im Satz gegeben. Angenommen wir können f schreiben als Produkt

$$f(x) = \alpha(x) \cdot \beta(x)$$

wobei $\alpha, \beta \in R[x], \deg \alpha > 0, \deg \beta > 0$.

Schreibe

$$\begin{aligned} \alpha(x) &= \alpha_0 + \alpha_1 x + \ldots \\ \beta(x) &= \beta_0 + \beta_1 x + \ldots \end{aligned}$$

Beobachte: $a_0 = \alpha_0 \cdot \beta_0$

Per Annahme gilt: $p \mid a_0 \underset{\substack{R \\ \text{faktoriell}}}{\Rightarrow} p \mid \alpha_0$ oder $p \mid \beta_0$.

Per Annahme $p^2 \nmid a_0$ kann p nicht beide Elemente teilen. Wir nehmen also $p \mid \alpha_0$ und $p \nmid \beta_0$ an.

Weil $\mathrm{ggT}(a_0, \ldots, a_n) = 1$, wissen wir: p teilt nicht alle α_i. Sei also i minimal, sodass $p \nmid \alpha_i$. Wir wissen schon mal $i < n$, insbesondere $p \mid a_i$.

Es ist aber

$$a_i = \underbrace{\alpha_0 \beta_i}_{\substack{\text{Vielfaches} \\ \text{von } p}} + \underbrace{\alpha_i \beta_{i-1}}_{\substack{\text{Vielfaches} \\ \text{von } p}} + \underbrace{\alpha_2 \beta_{i-2}}_{\substack{\text{Vielfaches} \\ \text{von } p}} + \cdots + \underbrace{\alpha_i \beta_0}_{\substack{\text{kein} \\ \text{Vielfaches von } p}}$$

↯ zu Teilbarkeitsregeln. □

Bemerkung: Polynome, welche die Annahmen des Satzes erfüllen, heißen Eisensteinpolynome.

Ein Beispiel dafür ist $R = \mathbb{Z}, f(x) = x^3 - 2$.

2.3 Hilfe bei der Anwendung des Eisenstein-Kriteriums

Sei R faktoriell und $\varphi : R[x] \to S$ ein Ringmorphismus in einen Integritätsring S. Angenommen φ hat die Eigenschaft, dass $\forall f \in R[x] : \deg f > 0 \Rightarrow \varphi(f) \notin S^*$.

Wenn jetzt ein $f \in R[x]$ gegeben ist mit $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ mit $n > 0$ und $\mathrm{ggT}(a_0, \ldots, a_n) = 1$ und $\varphi(f)$ irreduzibel ist, dann ist f irreduzibel.

Beweis. Angenommen $f(x)$ sei reduzibel in $R[x] \Rightarrow \exists \alpha(x), \beta(x) \in R[x]$ mit $f(x) = \alpha(x) \cdot \beta(x)$ und $\deg \alpha > 0, \deg \beta > 0$. Dann gilt

$$\varphi(f) = \varphi(\alpha \cdot \beta) = \underbrace{\varphi(\alpha)}_{\notin S^*} \cdot \underbrace{\varphi(\beta)}_{\notin S^*}$$

Also hat $\varphi(f)$ echte Teiler in S und ist damit nicht irreduzibel. □

Wie finden wir φ?: Keine Ahnung, wir müssen rumprobieren.

Beispielhafte Konstruktionen

1) Gegeben ein Ringmorphismus $\phi : R \to S$ (z.B. $\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$, oder $\mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ mit $a \mapsto a^p$)

   Betrachte dann folgenden Morphismus von Polynomringen

   $$\varphi : R[x] \to S[x], \sum a_i x^i \mapsto \sum \phi(a_i) x^i$$

2) Situation wie in 1), zusätzlich sei $s \in S$ gegeben. Betrachte

   $$\varphi^* : R[x] \to S, \sum a_i x^i \mapsto \sum \phi(a_i) s^i$$

3) Situation wie in 2). Betrachte Morphismus

   $$\varphi^{\leftmoon} : R[x] \to s[x], \sum a_i x^i \mapsto \sum \varphi(a_i)(x - s)^i$$

Beispielhafte Nutzanwendung: Betrachte $p \in \mathbb{N}$ prim und

$$f(x) = x^{p-1} + x^{p-2} + \cdots + x + 1 \in \mathbb{Z}[x]$$

Das ist kein Eisenstein-Polynom.

Beobachte aber auch $(x-1)f(x) = x^p - 1$.

Das legt nahe, folgenden Morphismus zu probieren:

$$\varphi : \mathbb{Z}[x] \to \mathbb{Z}[x], g(x) \mapsto g(x+1)$$

was ist $\varphi(f)$?

$$\varphi(x^p - 1) = \varphi((x-1)f) = \underbrace{\varphi(x-1)}_{=x} \cdot \varphi(f)$$

und außerdem:

$$\varphi(x^p - 1) = (x+1)^p - 1 = \sum_{i=1}^{p} \binom{p}{i} x^i - 1$$

$$\Rightarrow \varphi(f) = \sum_{i=1}^{p} \binom{p}{i} \cdot x^{i-1}$$

das ist ein Eisenstein-Polynom.

Also ist $f(x)$ irreduzibel in $\mathbb{Z}[x]$, also auch in $\mathbb{Q}[x]$.

Ernte einfahren: Wir können mit unseren Methoden einige Fragen beantworten!

Erinnerung: Gegeben $M \subset \mathbb{C}$, eine Menge die $0, 1$ enthält. Konst(M) = Menge der aus M konstruierbaren Punkte.

1) Kons(M) ist ein Unterkörper von $\mathbb{C}$

2) Wenn $z \in$ Kons$(M) \subset \mathbb{C}$, dann gibt es $n \in \mathbb{N}$ sodass $[k(z) : k] = 2^n$ wobei $k = \mathbb{Q}(M \cup \overline{M})$ und $M = \{\overline{m} \mid m \in M\}$.

Beispiel 2.32
Das Element $z = \sqrt[3]{2}$ ist nicht aus $M = \{0, 1\}$ konstruierbar, denn in diesem Fall wäre $\overline{M} = M$ und $k = \mathbb{Q}(0, 1) = \mathbb{Q}$ aber $[\mathbb{Q}(\sqrt[3]{2} : \mathbb{Q})] = 3$, denn wir wissen: $x^3 - 2$ ist das Minimalpolynom.

Dieselbe Argumentation liefert mehr!

Satz 2.33
Sei $\varphi \in (0, 2\pi)$ sodass $e^{i\varphi} \in \mathbb{C}$ transzendent ist. Dann ist der Winkel $\angle e^{i\varphi}$, aufgespannt durch x-Achse und $e^{i\varphi}$ nicht durch Zirkel und Lineal 3-teilbar.

Bemerkung: Die Abbildung
$$(0, 2\pi) \to \mathbb{C}, \varphi \mapsto e^{i\varphi}$$
ist injektiv, hat also überabzählbar viele Bildpunkte, es gibt aber nur abzählbar viele algebraische Zahlen. Also ist $e^{i\varphi}$ transzendent für fast alle φ.

Für dieses Problem betrachte bei gegebenem φ die Menge $M = \{0, 1, e^{i\varphi}\}$. Ist $e^{i\frac{\varphi}{3}} \in$ Kons(M)? Also betrachten wir
$$k = \mathbb{Q}(M \cup \overline{M}) = \mathbb{Q}(z) = \mathbb{Q}(e^{i\varphi})$$
Müssen diskutieren: $[k(e^{i\frac{\varphi}{3}}) : k]$ das ist eine 2-er Potenz falls $e^{i\frac{\varphi}{3}}$ konstruierbar ist.

Wir sehen $e^{i\frac{\varphi}{3}}$ ist Nullstelle des Polynoms $f(x) = x^3 - e^{i\varphi} \in k[x]$. Falls f das Minimalpolynom ist, ist $[k(e^{i\frac{\varphi}{3}}) : k] = 3$, also $e^{i\frac{\varphi}{3}} \notin \text{Kons}(M)$.

Um zu sehen, dass $f \in k[x]$ tatsächlich irreduzibel ist, müssen wir k verstehen!

Behauptung: k ist isomorph zum Körper der rationalen Funktionen $\mathbb{Q}(y)$

Beweis. Wir betrachten einen Ringmorphismus
$$\mathbb{Q}[y] \to k = \mathbb{Q}(e^{i\varphi}), f(y) \mapsto f(e^{i\varphi})$$
Die Funktion ist injektiv weil $e^{i\varphi}$ transzendent ist.

Außerdem gilt: $\mathbb{Q}[y] \to Q(\mathbb{Q}[y]) = \mathbb{Q}(y)$

Die universelle Eigenschaft liefert einen Isomorphismus $\eta : \mathbb{Q}(y) \to k$.

η ist surjektiv weil $e^{i\varphi} = \eta(y)$ im Bild liegt und k der kleinste Körper ist, der $e^{i\varphi}$ enthält. $\square$

Wir wollen entscheiden, ob $f(x) = x^3 - e^{i\varphi} \in k[x]$ irreduzibel ist. Wir können also auch untersuchen, ob $x^3 - y$ in $(\mathbb{Q}(y))[x]$ irreduzibel ist.

$\Leftrightarrow$ Ist $x^3 - y \in (\mathbb{Q}[y])[x]$ irreduzibel?

$-y$ ist prim = irreduzibel in $\mathbb{Q}[y]$ und damit ist $x^3 - y$ ein Eisenstein-Polynom.

Beispiel 2.34
Falls p prim ist und das regelmäßige p-Eck konstruierbar ist, ist $p - 1$ von der Form 2^n.

Beweis. Betrachte $M = \overline{M} = \{0, 1\}$ und $k = \mathbb{Q}(M \cup \overline{M}) = \mathbb{Q}$.

Das regelmäßige p-Eck ist konstruierbar $\Leftrightarrow e^{\frac{2\pi i}{p}} \in \text{Kons}(M)$.

Falls das so ist, ist $\left[\mathbb{Q}(e^{\frac{2\pi i}{p}}) : \mathbb{Q}\right] = 2^n$ für ein $n \in \mathbb{N}$.

Wir wissen $e^{\frac{2\pi i}{p}}$ ist Nullstelle von $x^p - 1 \in \mathbb{Q}[x]$.

Aber $x^p - 1 = (x-1)(x^{p-1} + \cdots + 1)$. Das Minimalpolynom ist also $x^{p-1} + \cdots + 1$. Und damit $\left[\mathbb{Q}(e^{\frac{2\pi i}{p}}) : \mathbb{Q}\right] = p - 1$. □

2.4 Ringe und Ideale

Definition 2.35
Sei R ein Ring (kommutativ, mit 1). Sei $I \subset R$ eine nicht-leere Teilmenge. Nenne I ein Ideal, falls gilt:

1) $\forall a, b, \in I : a + b \in I$

2) $\forall a \in I, \forall r \in R : ra \in I$

Bemerkung: Für nicht-kommutative Ringe definiert man Linksideale (wie oben) und Rechtsideale (mit ar statt ra in *2)*).

Bemerkung:
- Die 0 ist in jedem Ideal enthalten
- $\{0\}, R$ sind immer Ideale
- Falls R ein Körper ist, sind $\{0\}$ und R die einzigen Ideale, denn:

  Sei k ein Körper, $I \subset k$ ein Ideal. Angenommen $\exists a \in I \setminus \{0\}$. Sei $b \in k$ gegeben; dann ist $b = (b \cdot a^{-1}) \cdot a \in I$.
- Falls $I \subset R$ ein Ideal und $1 \in I \Rightarrow I = R$

Beispiel 2.36
- *$R = \mathbb{Z}, a \in \mathbb{Z}$ ein Element $I = \{$alle Vielfachen von $a\}$*
- *Besonders einfache Ideale: sei R ein Ring, $I \subset R$ ein Ideal. Nenne I ein Hauptideal falls $\exists a \in I : I = (a)$. Nenne R Hauptidealring falls alle Ideale Hauptideale sind. z.B. $\mathbb{Z}$ ist ein Hauptidealring.*

  Sei $I \subset \mathbb{Z}$ ein Ideal, $I \neq (0)$. Wir wissen: I enthält positive Elemente. Sei $a \in I$ das kleinste positive Element. Will zeigen: $I = (a)$. Inklusion $\supset$ ist klar. Sei also

$b \in I \setminus \{0\}$ irgendein Element. oBdA sei $b > 0$. Division mit Rest:

$$\underbrace{b}_{\in I} = \underbrace{* \cdot a}_{\in I} + c, \quad \textit{wobei } 0 \le c < a.$$

Damit ist $c \in I$ aber auch $c < a \Rightarrow c = 0$ und damit $b \in (a)$.

Das gleiche gilt, falls k ein Körper und $R = k[x]$ ist.

$R = k[x, y]$ ist kein Hauptidealring, denn $I = (x, y)$ ist kein Hauptideal, denn

1) *$I \neq R$ genauer $1 \notin I$, denn alle Elemente von I außer 0 haben positiven Grad.*

2) *Wenn I ein Hauptideal wäre, $I = (a)$, dann $a \mid x$ und $a \mid y$, Aber $\mathrm{ggT}(x, y) = 1$. Also wäre a Einheit, $I = R$ ↯.*

Einige Rechenregeln

- $(a) \subset (b) \quad \Leftrightarrow \quad b \mid a$
- $(a) = (b) \quad \Leftrightarrow \quad a \sim b$

- *R beliebiger Ring, $(a_\lambda)_{\lambda \in \Lambda}$ eine Familie von Elementen*

$$I = \{r_1 \cdot a_{\lambda_1} + \cdots + r_n \cdot a_{\lambda_n} \mid n \in N, r_1, \ldots, r_n \in R, \lambda_1, \ldots, \lambda_n \in \Lambda\}$$

Wir sagen das Ideal ist von $(a_\lambda)_{\lambda \in \Lambda}$ erzeugt und schreibe

$$I = ((a_\lambda)_{\lambda \in \Lambda}) = (a_\lambda \mid \lambda \in \Lambda)$$

Falls die Familie endlich ist, schreibt man auch

$$I = (a_1, \ldots, a_n)$$

Definition 2.37
Sei R ein Ring und $I \subset R$ ein Ideal. Nenne I endlich erzeugt, falls es endlich viele $a_1, \ldots, a_n \in I$ gibt, sodass

$$I = (a_1, \ldots, a_n)$$

Bemerkung: Die Ähnlichkeit zwischen Erzeugendensystemen von Idealen und Untervektorräumen geht nicht sehr weit!

Beispiel 2.38
Sei k ein Körper (z.b. $\mathbb{R}$) und $X \subset k^n$ eine Teilmenge (z.B. X = Einheitskreis in $\mathbb{R}^2$)

Betrachte $R = k[x_1, \dots, x_n]$ und

$$I = \left\{ f \in k[x_1, \dots, x_n] \mid f(x_1, \dots, x_n) = 0 \; \forall \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in X \right\}$$

Diese Konstruktion ist besonders interessant, falls X die Lösungsmenge eines polynomiellen Gleichungssystems ist.

Definition 2.39
Sei R ein Ring. Sage „in R gilt der Teilerkettensatz für Ideale“, falls jede aufsteigende Kette von Idealen

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \dots$$

nach endlich vielen Schritten konstant wird.

Satz 2.40
Sei R ein Ring, dann sind äquivalent:

1) *Jedes Ideal ist endlich erzeugt*

2) *In R gilt der Teilerkettensatz für Ideale*

3) *In jeder nicht-leeren Menge von Idealen gibt es ein Element, das bezüglich Inklusion maximal ist*

Falls diese Eigenschaften gelten, nenne R Noethersch.

Beweis. 1) $\Rightarrow$ 2) Sei $I_1 \subseteq I_2 \subseteq \dots$ eine Folge von Idealen. Beachte:

$$I = \bigcup_{i=0}^{\infty} I_i$$

ist ein Ideal, also per Annahme endlich erzeugt: $I = (a_1, \dots, a_n)$ für geeignete $a_1, \dots, a_n \in \bigcup I_i$. Dann gibt es also $i_1, \dots, i_n$ sodass $a_i \in I_{i_1}, a_2 \in I_{i_2}$ wenn $m = \max\{i_1, \dots, i_n\}$. Dann gilt $a_1 \in I_m, a_2 \in I_m, \dots$ und somit:

$$(a_1, \dots, a_n) \subset I_m \subset I = (a_1, \dots, a_m)$$

also auch $I_m = I_{m+1} = I_{m+2} = \dots$

2) $\Rightarrow$ 3) Sei M eine nicht-leere Menge von Idealen ohne maximales Element. Sei $I_i \in M$ irgendein Element. Finde dann $I_2 \in M$ mit $I_1 \subsetneq I_2$. Da I_2 auch nicht maximal ist finde also $I_3 \in M$ mit $I_2 \subsetneq I_3$. Erhalte so eine Kette

$$I_1 \subsetneq I_2 \subsetneq I_3 \subsetneq \dots$$

$\Rightarrow$ Teilerkettensatz für Ideale gilt nicht!

$\underline{3) \Rightarrow 1)}$ Sei $I \subset R$ ein Ideal, $I \neq (0)$. Sei $M = \{J \subset I \mid J \text{ ein Ideal, } J \text{ endlich erzeugt}\}$

Wir wissen es gibt ein maximales $m \in M$. Behauptung $m = I$

Denn sonst wäre $m = (a_1, \dots, a_n) \subsetneq I$ und es gäbe $a_{n+1} \in I \setminus m$. Dann ist $m' = (a_1, \dots a_n, a_{n+1})$ endlich erzeugt, also in M und $m' \supsetneq m$ ↯ □

Satz 2.41 (Hilbert)
Sei R Noethersch. Dann ist auch $R[x]$ Noethersch.

Beweis. Angenommen $R[x]$ nicht Noethersch. Wir müssen zeigen R ist nicht Noethersch.

Wir wissen: Es gibt in $R[x]$ ein Ideal I, das nicht endlich erzeugt ist.

Wähle in I ein Element f von minimalem Grad. Dann ist $I \subsetneq (f_1)$, also $I \setminus (f_1) \neq \emptyset$, wähle $f_2 \in I \setminus (f_1)$ von minimalem Grad. $I \supsetneq (f_1, f_2)$ wähle $f_3 \in I \setminus (f_1, f_2)$ von minimalem Grad.

Erhalte Folge von Polynomen $f_1, f_2, f_3, \dots$ sodass $\deg f_1 \leq \deg f_2 \leq \deg f_3 \leq \dots$

Setze $n_i = \deg f_i$, $a_i =$ Leitkoeffizient von $f_i \in R$.

Wir wollen zeigen, dass folgende Kette von Idealen in R nicht stationär wird:

$$(a_1) \subseteq (a_1, a_2) \subseteq (a_1, a_2, a_3) \subseteq \dots$$

Denn dann wird klar sein, dass R nicht Noethersch war.

Angenommen es gäbe k mit $(a_1, \dots, a_k) = (a_1, \dots, a_{k+1}) \Leftrightarrow a_{k+1} \in (a_1 \dots, a_k)$

Dann gibt es also eine Linearkombination

$$a_{k+1} = \sum_{i=1}^{k} r_i a_i$$

für geeignete $r_i \in R$. Betrachte Polynom

$$s(x) = \sum_{i=1}^{k} r_i \cdot x^{n_{k+1} - n_i} \cdot f_i(x)$$

Wesentliche Eigenschaften von s:

1) $\deg s = n_{k+1} = \deg f_{k+1}$

2) Leitkoeffizient $(s) = a_{k+1}$

3) $s \in (f_1, \dots, f_k)$

Betrachte $\underbrace{f_{k+1}(x)}_{\notin (f_1,\dots,f_k)} - \underbrace{s(x)}_{\in (f_1,\dots,f_k)} = t(x)$.

Damit ist $t(x) \notin (f_1, \dots, f_k)$ und $\deg t(x) < n_{k+1}$.

$\lightning$ zur Wahl von f_{k+1} als Element von $I \setminus (f_1, \dots, f_k)$ von minimalem Grad. $\square$

Satz 2.42
Sei R ein Integritätsring, der Hauptidealring ist. Dann ist R faktoriell.

Beweis. Sei p irreduzibel, seien $a, b \in R$, sowie $p \nmid a, p \nmid b$. Dann müssen wir zeigen: $p \nmid a \cdot b$.

Wir wissen: (p, a) ist ein Hauptideal, also $\exists c \in R$ sodass $(p, a) = (c)$. Also p ist Vielfaches von c, also $c \mid p$. Aber p ist irreduzibel, hat also keine echten Teiler. Also $c \in R^*$ oder $c \sim p$.

Aber $c \sim p \Leftrightarrow p \mid a$, was wir per Annahme ausschließen!

Also $c \in R^* \quad \Rightarrow (a, p) = (1)$. Es gibt also eine Linearkombination

$$1 = \alpha_1 a_1 + \alpha_2 p \tag{$*$}$$

Analog finde $\beta_1, \beta_2 \in R$

$$1 = \beta_1 b + \beta_2 p \tag{☾}$$

Es folgt

$$1 = \alpha_2 \beta_2 p^2 + (\alpha_1 \beta_2 a + \alpha_2 \beta_1 b) p + \alpha_1 a \beta_1 b$$

$\Rightarrow p \nmid \alpha_1 \beta_1 ab$, denn sonst würde p die Summe teilen, also auch $p \mid 1$.

$\Rightarrow p \nmid a \cdot b$ $\square$

Quotienten: Sei R ein Ring, $I \subset R$ ein Ideal. Dann definiere $r, s \in R$ als äquivalent, falls $r - s \in I$.

Satz 2.43
Es gibt auf Quotientenmengen eindeutige Verknüpfungen + und ·, sodass die Quotientenabbildung

$$q : R \to R/I$$

ein Ringmorphismus ist.

Beispiel 2.44
$R = \mathbb{Z}, I = (p)$ *das von einer Primzahl* p *erzeugte Hauptideal. Dann gilt*

$$R/I = \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p = \underline{F}_p$$

Beispiel 2.45
Sei k *ein Körper,* $R = k[x]$, $f \in R$ *ein Polynom, sowie* $I = (f)$. *Dann betrachte* $R/(f)$.

Beobachtung: Sei $n = \deg f$. *Polynomdivison zeigt: die Polynome von* $\deg < n$ *bilden vollständiges Repräsentantensystem. Insbesondere* $\dim_k R/(f) = n$.

Multiplikation und Addition ist sehr einfach zu beschreiben: Wenn a, b *Polynome von* $\deg < n$

$$[a] \cdot [b] = [c]$$

wobei c *der Divisionsrest von* $a \cdot b$ *bei Division durch* f *ist.*

Beispiel 2.46
Sei k *ein Körper,* $X \subset k^n$ *eine Teilmenge (z.B. Lösungsmenge eines algebraischen Gleichungssystems).*

Dann setze $R = k[x_1, \dots, x_n]$

$$I = \{f \in R \mid f_{|X} \equiv 0\}$$

und $R/I = \{$*Funktionen* $X \to k$, *die sich zu Polynomen* $k^n \to k$ *fortsetzen lassen*$\}$ = *Polynomiale Funktionen = algebraische Funktionen*

Satz 2.47 (Universelle Eigenschaft)
Sei R *ein Ring, sei* $I \subset R$ *ein Ideal. Sei* $q : R \to R/I$ *die Restklassenabbildung. Dann gilt folgende universelle Eigenschaft: Für jeden surjektiven Ringmorphismus* $\varphi : R \to S$ *mit* $\ker(\varphi) \supseteq I$ *gibt es genau einen Ringmorphismus* $\eta : R/I \to S$ *sodass das folgende Diagramm kommutiert:*

$$\begin{tikzcd}
R \arrow[r, "q"] \arrow[d, dash, "\mathbb{1}_R"'] & R/I \arrow[d, "\exists!\eta"] \\
R \arrow[r, "\varphi"'] & S
\end{tikzcd}$$

Beweis.

Eindeutigkeit: Angenommen wir haben zwei Morphismen η_1, η_2. Sei $[a] \in R/I$ gegeben. Weil die Diagramme kommutieren, muss dann $\eta_1([a]) = \eta_1(q(a)) = \varphi(a) = \eta_2([a])$.

Existenz: Setze $\eta : R/I \to S, [a] \mapsto \varphi(a)$. Dabei ist die Wohldefiniertheit zu zeigen. Sei also $[a] = [a']$ d.h. $a - a' \in I \subset \ker(\varphi)$. Dann ist $\varphi(a) - \varphi(a') = \varphi(a - a') = 0$, also $\varphi(a) = \varphi(a')$ und die Wohldefiniertheit ist klar. Muss noch nachrechnen: η ist Ringmorphismus, bin aber zu faul. $\square$

Beispiel 2.48
Sei $\varphi : R \to S$ ein surjektiver Ringmorphismus. Dann ist $S \simeq R/\ker(\varphi)$.

Beweis. Nach universeller Eigenschaft gibt es genau eine Abbildung $\eta : R/\ker(\varphi) \to S$ sodass das folgende Diagramm kommutiert.

$$\begin{tikzcd}
R \arrow[r] \arrow[d, no head, "\mathbb{1}_R"'] & R/\ker(\varphi) \arrow[d, "\exists!\eta"] \\
R \arrow[r, "\varphi"'] & S
\end{tikzcd}$$

Behauptung: η ist Isomorphismus. Muss zeigen: η bijektiv also injektiv und surjektiv. Surjektivität folgt sofort aus Kommutativität des Diagramms und der Surjektivität von φ. Noch zu zeigen η injektiv bzw. $\ker(\eta) = 0_{R/\ker(\varphi)}$.

Sei also $[a] \in \ker(\eta)$. Wegen der Kommutativität des Diagramms:

$$0_S = \eta([a]) = \eta(q(a)) = \varphi(a) \Rightarrow a \in \ker(\varphi),$$

also $[a] = 0_{R/\ker(\varphi)}$. $\square$

Warum das Bohei um Quotienten?

Wir betrachten Körpererweiterung L/k und algebraische Elemente $a \in L$.

Wir wissen: a hat das Minimalpolynom $f \in k[x]$. Jedes andere Polynom $g \in k[x]$ mit $g(a) = 0$ ist Vielfaches von f. $(g(a) = 0 \Leftrightarrow g \in (f))$.

Betrachte Abbildung:

$$\begin{aligned} k[x] &\to k(a) \\ g &\mapsto g(a) \end{aligned}$$

Wir wissen:

- $\ker(\varphi) = (f)$
- Die Elemente von $k(a)$ können wir schreiben als $\lambda_1 + \lambda_2 a + \cdots + \lambda_n a^{n-1}$ mit $\lambda_i \in k$
  $\Rightarrow \varphi$ ist surjektiv!

Insgesamt:

$$k(a) \cong k[x]/(f)$$

Satz 2.49
Sei $\varphi : R \to S$ ein Ringmorphismus. Dann gilt

1) *Für jedes Ideal $I \subset S$ ist $\varphi^{-1}(I)$ ein Ideal, das $\ker(\varphi)$ enthält.*

2) *Wenn φ surjektiv ist, dann ist die Abbildung*

$$\begin{aligned}\{\textit{Ideale in } S\} &\xrightarrow{\alpha} \{\textit{Ideale in } R\textit{, die } \ker(\varphi) \textit{ enthalten}\}\\ I &\mapsto \varphi^{-1}(I)\end{aligned}$$

   bijektiv.

3) *Wenn φ surjektiv ist, $J \subset R$ ein Ideal, dann ist $\varphi(J) \subset S$ ein Ideal.*

4) *Wenn φ surjektiv ist, und $I \subset S$ ein Ideal ist, dann betrachte die Komposition ψ von*

$$R \underset{\varphi}{\to} S \to S/I$$

   und es ist $\ker(\psi) = \varphi^{-1}(I)$. Also ist $S/I \simeq R/\varphi^{-1}(I)$.

Beweis. 1) Hausaufgabe!

2) Weil φ per Annahme surjektiv ist, ist die Abbildung α injektiv. Also noch Surjektivität zu zeigen. Sei also $J \subset R$ ein Ideal, das $\ker(\varphi)$ enthält. Wir wissen: $S \simeq R/\ker(\varphi)$. Also gibt es nach universeller Eigenschaft ein Diagramm

$$\begin{tikzcd} R \arrow[r, "\varphi"] \arrow[d, dash, "\mathbb{1}_R"'] & R/\ker(\varphi) \arrow[d, "\exists!\eta"] \\ R \arrow[r, "q"'] & R/J \end{tikzcd}$$

und $J = q^{-1}((0)) = \varphi^{-1}(\eta^{-1}(0))$, setze $I = \eta^{-1}(0)$, fertig.

3) Sei $J \subset R$ ein Ideal. Wir müssen zeigen

   C1: Wenn $a, b \in \varphi(J)$, dann ist $a + b \in \varphi(J)$. $\exists a', b' \in J$ mit $a = \varphi(a'), b = \varphi(b')$ und dann $a + b = \varphi(\underbrace{a' + b'}_{\in J})$

   C2: Sei $a \in \varphi(J)$, sei $b \in S$ beliebig. Dann ist $s \cdot a \in \varphi(J)$. Weil φ surjektiv ist, $\exists s' \in R : s = \varphi(s')$. Außerdem $\exists a' \in J : a = \varphi(a')$ und $\varphi(\underbrace{s'a'}_{\in J}) = \varphi(s')\varphi(a') = sa$

4) Sei $r \in R$. Es gilt

$$\begin{aligned} r \in \ker(\psi) &\Leftrightarrow q(\varphi(r)) = 0_{S/I} \\ &\Leftrightarrow \varphi(r) \in I \\ &\Leftrightarrow r \in \varphi^{-1}(I) \end{aligned}$$

□

Folgerung 2.50
Sei R noethersch (bzw. Hauptidealring). Sei $I \subset R$ ein Ideal. Dann ist R/I Noethersch (bzw. Hauptidealring).

Notation: Sei R Ring. Seien $I \subseteq J \subseteq R$ Ideale. Dann betrachte $q_I : R \to R/I$.

Das Ideal $q_I(J) \subseteq R/I$ wird mit J/I bezeichnet.

Satz 2.51 (Noetherscher Isomorphiesatz)
Situation wie oben. Dann

$$R/J \simeq (R/I)/(J/I)$$

Beweis. Wir haben Ringmorphismen

$$R \xrightarrow{q_I} R/I \xrightarrow{q_{J/I}} (R/I)/(J/I)$$

Wir wissen $\ker(\eta) = q_I^{-1}(J/I) = J$. Also folgt die Aussage. □

Wir haben 2 wichtige Typen von Idealen

- Primideale: R ein Ring, $I \subseteq R$ ein Ideal. Nenne I prim, falls $\forall a, b \in R : a \cdot b \in I \Rightarrow a \in I \vee b \in I$

- Maximale Ideale: R ein Ring. Ein Ideal $I \subset R$ heißt maximal, falls gilt

1) $I \neq R$

2) Wenn $J \supsetneq I$ ein echt größeres Ideal ist, dann ist $J = R$.

Beispiel 2.52 • *Sei R ein Ring, $p \in R$ ein prim-Element. Dann ist (p) ein Primideal.*

- *Sei k ein Körper, $R = k[x_1, \dots, x_n]$ und*

$$I = (x_1, x_2, \dots, x_n) = \{ \underbrace{x_1 f_1 + x_2 f_2 + \cdots + x_n f_n}_{\text{haben stets Nullstelle am Ursprung!}} \mid f_i \in k[x_1, \dots, x_n]\}$$

Wir wissen $1 \notin I$, denn 1 hat keine Nullstelle.

Beobachte: Ein Polynom liegt genau dann in I, wenn der konstante Teil gleich Null ist (d.h. wenn $f(0) = 0_k$).

Sei jetzt $J \supsetneq I$ echt größer! Sei $f \in J \setminus I$. Dann

$$\underbrace{f}_{\in J} = const^{\neq 0} + (\underbrace{\text{Polynom ohne konstanten Teil}}_{\in I \subset J})$$

$\Rightarrow const^{\neq 0} \in J \Rightarrow J = R$

Variante: Seien $a_1, \dots, a_n \in k$. Dann ist $I' = (x_1 - a_1, x_2 - a_2, \dots, x_n - a_n)$ auch maximal.

Zurück zu Beispiel ohne Variante

$$\begin{aligned} R/I = k[x_1, \dots, x_n]/(x_1, \dots, x_n) &\xrightarrow{\simeq} k \\ [f] &\longmapsto f(0) \end{aligned}$$

Beispiel 2.53
Sei k ein Körper, $f \in k[x]$ irreduzibel. Dann ist (f) maximal.

Beweis. Sei $J \supsetneq (f)$ größer, sei $g \in J \setminus (f)$ ein Element (g kein Vielfaches von f).

Wissen (Euklidischer Algorithmus): $\mathrm{ggT}(f, g) \in J$. Aber f ist irreduzibel hat also keine echten Teiler d.h. $\mathrm{ggT}(f, g) = 1$ □

Satz 2.54
Sei R ein Ring, $I \subset R$ ein Ideal. Dann gilt

1) I ist prim $\Leftrightarrow$ R/I ist Integritätsring

2) I ist maximal $\Leftrightarrow$ R/I ist ein Körper

<u>Insbesondere:</u> *maximale Ideale sind prim (denn Körper sind Integritätsringe)*

Beweis. <u>1) $\Rightarrow$</u>: Sei I prim. Seien $[a], [b] \in R/I$ Äquivalenzklassen von Elementen $a, b \in R$ sodass $[a] \neq 0_{R/I}$ und $[b] \neq 0_{R/I}$. Dann gilt $a \notin I$ und $b \notin I$.

Da I prim $a \cdot b \notin I \Rightarrow [a \cdot b] \neq 0_{R/I}$

<u>1) $\Leftarrow$</u>: Sei R/I ein Integritätsring. Seien $a, b \in R \setminus I$. Dann $[a] \neq 0_{R/I}$ und $[b] \neq 0_{R/I}$ und $[a \cdot b] \neq 0_{R/I}$.

$\Rightarrow ab \notin I$

<u>2) $\Rightarrow$</u>: Sei I maximal. Sei $a \in R$ mit $[a] \neq 0_{R/I}$ d.h. $a \notin I$.

Dann betrachte $J = (I, a)$. Wir wissen $J \supsetneq I$ also $(1) = J$. Also können wir schreiben:

$$1 = f + g \cdot a \qquad \text{mit } f \in I, g \in R$$

$$\Rightarrow \underbrace{[1]}_{=1_{R/I}} = \underbrace{[f]}_{0_{R/I}} + [g] \cdot [a]$$

also ist $[g] = [a]^{-1}$ in R/I

<u>2) $\Leftarrow$</u>: Sei R/I ein Körper, sei $J \supsetneq I$ ein echtes Oberideal. Dann gibt es $a \in J \setminus I$.

Wir wissen $[a] \neq 0_{R/I}$, per Annahme $\exists b \in R$ mit $[a] \cdot [b] = [1]$. Das bedeutet $\exists f \in I$ sodass

$$\underbrace{a \cdot b}_{\in J} + \underbrace{f}_{\in I \subset J} = 1$$

das heißt $1 \in J$ d.h. $J = R$. □

Bemerkung: Teil 2) des Satzes liefert neuartige Methode, um Beispiele von Körpern zu konstruieren!

<u>Weitere Beobachtungen/Konstruktionen mit Idealen</u>

Sei R ein Ring, seien $I_1, \ldots, I_n$ Ideale in R

- Dann ist $I_1 \cap I_2 \cap \cdots \cap I_n$ ein Ideal
- Dann ist $I_1 + \cdots + I_n = \{f_1 + \cdots + f_n \in R \mid \forall i f_i \in I_i\}$ ein Ideal

Beispiel 2.55
$R = \mathbb{Z}$ $I_1 = (a)$ $I_2 = (b)$

$I_1 \cap I_2 = (\text{kgV}(a, b))$

$I_1 + I_2 = (\text{ggT}(a, b))$

Definition 2.56
Zwei Ideale I_1, I_2 heißen teilerfremd, wenn $I_1 + I_2 = (1)$.

Nutzanwendung: Manchmal hat man Aufgaben der Form: gegeben ein Ring R, Ideale $I_1, \dots, I_n$ und Elemente $r_1, \dots, r_n \in R$. Finde ein/alle $r \in R$

$$\begin{aligned} r &\equiv r_1 \mod I_1 \\ r &\equiv r_2 \mod I_2 \\ &\vdots \\ r &\equiv r_n \mod I_n \end{aligned}$$

Antwort ist Chinesischer Restsatz: Situation wie oben. Fall $\forall\ i \neq j$ die Ideale I_i und I_j stets teilerfremd sind, dann ist die Abbildung:

$$\begin{aligned} \varphi : R &\to R/I_1 \times R/I_2 \times \dots \times R/I_n \\ r &\mapsto ([r]_{R/I_1}, [r]_{R/I_2}, \dots, [r]_{R/I_n}) \end{aligned}$$

surjektiv und $\ker(\varphi) = I_1 \cap \dots \cap I_n$.

Beweis. Aussage über $\ker(\varphi)$ ist trivial. Müssen surjektiv zeigen!

Seien $k \neq l$ gegeben. Wir wissen $(1) = I_k + I_l$. Also existieren Elemente $a_{kl} \in I_k$ und $b_{kl} \in I_l$ sodass $1 = a_{kl} + b_{kl}$

Setze

$$s_l = \prod_{k \neq l} a_{kl} = \prod_{k \neq l} (1 - b_{kl}) \in R$$

Beobachtung: Seien $k \neq l$ gegeben. Dann $s_l \equiv 0 \mod I_k$, denn der Faktor a_{kl} aus dem 1. Produkt ist $\equiv 0 \mod I_k$.

$s_l \equiv 1 \mod I_l$, denn es ist stets $b_k l \equiv 0 \mod I_l$, also jeder Faktor des rechten Produktes $\equiv 1 \mod I_l$.

Seien $r_1, \dots, r_n \in R$ gegeben.

Setze: $r = \sum r_i \cdot s_i$ dann gilt $\forall i : r \equiv r_i \mod I_i$, also

$$\varphi(r) = [r_1] \times [r_2] \times \cdots \times [r_n]$$

□

Einschub Mengenlehre

Definition 2.57
Sei M eine Menge. $\leq$ sei eine Relation. Wie nennen $\leq$ eine Halbordnung, falls gilt:

1) $\forall a \in M : a \leq a$

2) Wenn $a, b, c \in M$ gegeben sind mit

$$a \leq b, b \leq c \Rightarrow a \leq c$$

3) $\forall a, b \in M : a \leq b$ *und* $b \leq a \Rightarrow a = b$

Wir fordern nicht, dass $\forall a, b \in M : a \leq b$ oder $b \leq a$ gilt. (Falls das gilt nenne $\leq$ vollständig)

Beispiel 2.58
Betrachte $S =$ Studierende, $M = \mathrm{Pot}(S)$.

Gegeben $m_1, m_2 \in M$, schreibe $m_1 \leq m_2$ falls $m_1 \subseteq m_2$ ist.

Definition 2.59
Sei $(M, \leq)$ eine Menge mit Halbordnung. Eine Kette ist eine Teilmenge $N \subset M$, sodass die auf N induzierte Halbordnung vollständig ist. Ein Element $m \in M$ heißt obere Schranke der Kette N, falls gilt: $\forall n \in N : n \leq m$.

Beispiel 2.60
Sei $(M, \leq)$ gegeben. Sei $(n_i)_{i \in \mathbb{N}}$ eine Folge von Elementen sodass $n_1 \leq n_2 \leq \ldots$ ist. Dann ist $N = \{n_i \mid i \in \mathbb{N}\}$ eine Kette.

Beispiel 2.61
Sei $M = \mathbb{R}$ und $\leq$ wie üblich definiert. Dann ist jede Teilmengen eine Kette, denn $\leq$ ist sowieso vollständig. Obere Schranken existieren genau dann wenn N nach oben beschränkt ist.

Satz 2.62 (Lemma von Zorn)
Sei $(M, \leq)$ eine halbgeordnete Menge, $M \neq \emptyset$. Falls jede Kette eine obere Schranke besitzt, dann gibt es in M ein maximales Element.

Bemerkung: Dies ist äquivalent zum Auswahlaxiom. Sei $(M_\alpha)_{\alpha \in A}$ eine Familie von Mengen. Dann gibt es eine Abbildung

$$A \to \bigcup_{\alpha \in A} M_\alpha$$

sodass $\forall \alpha \in A : \varphi(\alpha) \in M_\alpha$.

Satz 2.63
Sei R ein Ring, $I \subset R$ ein Ideal. Dann gibt es ein maximales Ideal $m \subset R$, das I enthält

Beweis. Sei

$$M = \{\text{Ideale } J \subset R \text{ mit } I \subseteq J \subsetneq R\}$$

wähle $\subseteq$ als Halbordnung.

Beachte: Wenn $N \subset M$ eine Kette ist, dann ist $s = \bigcup_{n \in N} n$ eine obere Schranke.

- Ketteneingenschaft garantiert, dass s ein Ideal ist
- $1 \notin s$, denn für alle $m \in M : 1 \notin m$. Also $s \subsetneq R$, also $s \in M$

Zorn: Es existiert in M ein maximales Element m.

Nachrechnen: Dies ist ein maximales Ideal in R, welches I enthält. $\square$

3 Körpertheorie

3.1 Grundbegriffe

Beobachtung: Sei k ein Körper, sei 1_k das neutrale Element der Multiplikation. Dann betrachte Ringmorphismus

$$\begin{aligned} \eta : \mathbb{Z} &\to k \\ n &\mapsto \begin{cases} \underbrace{1_k + \cdots + 1_k}_{n \text{ mal}} & \text{falls } n \geq 0 \\ \underbrace{-(1_k + \cdots + 1_k)}_{n \text{ mal}} & \text{falls } n < 0 \end{cases} \end{aligned}$$

Beobachte: Wenn $k' \subset k$ ein Unterkörper ist, dann $\text{Bild}(\eta) \subseteq k'$.

Beobachtung: Wenn $(k_\lambda)_{\lambda\in\Lambda}$ eine Familie von Unterkörpern ist, dann ist

$$k' := \bigcap_{\lambda\in\Lambda} k_\lambda$$

wieder ein Unterkörper.

Definition 3.1
Gegeben ein Körper k, betrachte

$$k' := \bigcap_{\substack{k''\subseteq k\\ \text{Unterkörper}}} k''$$

Dieser Unterkörper heißt Primkörper von k.

Mit der Beobachtung von eben: $\mathrm{Bild}(\eta) \subseteq$ Primkörper

Beachte: η ist entweder injektiv oder nicht.

Fall η ist injektiv:

$$\begin{tikzcd}
\mathbb{Z} \arrow[r, "\varphi"] \arrow[d, dash, "\mathbb{1}_R"'] & Q(\mathbb{Z}) = \mathbb{Q} \arrow[d, hook, "\exists!\varphi"] \\
\mathbb{Z} \arrow[r, hook, "\eta"'] & \text{Primkörper von } k
\end{tikzcd}$$

Beachte: $\mathrm{Bild}(\varphi)$ ist Unterkörper des Primkörpers, welcher der kleinste Unterkörper von k ist, also $\mathrm{Bild}(\varphi) =$ Primkörper. Also insgesamt: Falls η injektiv ist, ist der Primkörper kanonisch isomorph zu $\mathbb{Q}$.

Fall η nicht injektiv: Dann ist $\ker(\eta) \subseteq \mathbb{Z}$ ein nicht-triviales Ideal.

Weil $\eta(1_\mathbb{Z}) = 1_k \neq 0_k$, ist $\ker(\eta) \subsetneq \mathbb{Z}$ also Hauptideal der Form (p) für ein $p \in \mathbb{N}$. Weil k nullteilerfrei ist, ist p eine Primzahl und nach universeller Eigenschaft von Quotienten haben wir ein Diagramm.

$$\begin{tikzcd}
\mathbb{Z} \arrow[r, "\varphi"] \arrow[d, dash, "\mathbb{1}_R"'] & \mathbb{Z}/(p) \arrow[d, hook, "\exists\varphi"] \\
\mathbb{Z} \arrow[r, "\eta"'] & \text{Primkörper von } k
\end{tikzcd}$$

Argumentiere wie oben, erhalte einen kanonischen Isomorphismus zwischen dem Primkörper und $\mathbb{Z}/p\mathbb{Z}$.

Zusammenfassung/Notation: Sei k ein Körper. Sei $k' \subseteq k$ der Primkörper. Dann entweder

- $k' \simeq \mathbb{Q}$ und man sagt: k hat Charakteristik $0, \operatorname{char}(k) = 0$
- $k' \simeq \mathbb{Z}/p\mathbb{Z}$ für eine Primzahl p und man sagt k hat die Charakteristik p

Bemerkung zum Gruseln: Sei $\operatorname{char}(k) = p > 0$. Dann ist $(x+y)^p = x^p + y^p$. Insbesondere ist

$$\begin{aligned} \text{Frob}\colon k[x] &\to k[x] \\ f &\mapsto f^p \end{aligned}$$

ein Ringmorphismus. Außerdem ist die Ableitung von $f(x) = x^p$ gegeben als $f'(x) = px^{p-1} \equiv 0$.

$f(x) = x^p + x^{p+2}$ und $f'(x) = (p+2) \cdot x^{p+1} = 2 \cdot x^{p+1}$

Schlussbeobachtung: Sei k ein endlicher Körper, dann ist $\operatorname{char}(k) = p > 0$. Beobachte: k ist ein Vektorraum über dem Primkörper $\simeq \mathbb{Z}/p\mathbb{Z}$.

Sei $n = \dim_{\text{Prim}} k$. Dann $n < \infty$ und $\#k = p^n$.

3.2 Der algebraische Abschluss

Beobachtung: Das Polynom $x^2 + 2$ hat in $\mathbb{Q}$ keine Nullstelle, aber im Oberkörper $\mathbb{C}$. Es gilt sogar: jedes nicht konstante $f \in \mathbb{C}[x]$ hat in $\mathbb{C}$ eine Nullstelle.

Ziel: Wir wollen Ähnliches für beliebige Körper konstruieren. Gegeben Körper k, konstruiere einen Oberkörper $\overline{k}$, sodass alle nicht konstanten Polynome $f \in \overline{k}[x]$ in $\overline{k}$ eine Nullstelle haben.

Aber: $\overline{k}$ erfüllt keine gute universelle Eigenschaft $\rightsquigarrow$ Galois-Theorie: Symmetrie von Erweiterungen

Spielwiese: Betrachte $\mathbb{Q}$ und $k = \mathbb{Q}[x]/(x^2+1)$.

Wir können $\mathbb{Q}$ in k einbetten durch

$$\begin{aligned}\mathbb{Q} &\hookrightarrow k\\ q &\mapsto [q]\end{aligned}$$

Also ist k Oberkörper von $\mathbb{Q}$.

Betrachte das Element $a := [x] \in k$

Beobachte: $a^2 + 1_k = a \cdot a + 1_k = [x][x] + [1_{\mathbb{Q}}] = [x \cdot x + 1_{\mathbb{Q}}] = [x^2 + 1_{\mathbb{Q}}] = 0_k$.

Einsicht: $a \in k$ ist Nullstelle des Polynoms $x^2 + 1_k \in k[x]$

Wie soll die Konstruktion von $\overline{k}$ gehen? Grundidee: so wie in der Spielwiese.

Satz 3.2
Sei k ein Körper, sei $f \in k[x]$ nicht konstant. Dann gibt es einen Oberkörper $L \supseteq k$, sodass f als Polynom in $L[x]$ eine Nullstelle in L hat.

Beweis. Sei $p(x)$ ein irreduzibler Faktor von f. Setze $L := k[x]/(p)$. Das ist ein Körper, weil (p) ein maximales Ideal ist.

Bette k mit Hilfe des injektiven Körpermorphismuses

$$\begin{aligned}k &\to L\\ a &\mapsto [a]\end{aligned}$$

in L ein. Beachte, dass $a := [x] \in L$ eine Nullstelle von p und also auch von f ist. □

Beobachtung: Wir wissen schon: wenn wir diese Konstruktion anwenden auf $k = \mathbb{R}, f = x^2 + 1$, dann erhalten wir $\mathbb{C}$. Wir sehen schon an diesem Beispiel, dass die so erhaltene Erweiterung Symmetrien besitzt, nämlich die komplexe Konjugation. Also ist es nicht richtig, dass $\mathbb{C}$ bis auf kanonische Isomorphie eindeutig ist.

Satz 3.3
Sei k ein Körper. Dann ist äquivalent:

1) *Jedes nicht-konstante Polynom in $k[x]$ hat eine Nullstelle in k.*

2) *Jedes nicht-konstante Polynom zerfällt in Linearfaktoren.*

3) *Jedes irreduzible Polynom ist linear.*

4) *Wenn L/k eine algebraische Körpererweiterung ist, dann ist $L = k$.*

Nenne k algebraisch abgeschlossen, falls diese Bedingungen erfüllt sind.

Beweis. 1) $\Rightarrow$ 2): Polynomdivision: wenn f bei a eine Nullstelle hat dann ist f ein Vielfaches von $(x-a)$.

2) $\Rightarrow$ 3): trivial

3) $\Rightarrow$ 4): Sei L/k eine algebraische Körpererweiterung. Sei $a \in L$ gegeben. Dann ist a algebraisch über k. Sei $f \in k[x]$ das Minimalpolynom. Dann ist f irreduzibel, also linear, also $f(x) = x - a \in k[x] \Rightarrow a \in k$.

4) $\Rightarrow$ 1): Sei $f \in k[x]$ nicht konstant. Sei $p(x)$ ein irreduzibler Faktor von f. Setze

$$L = k[x]/(p)$$

Das ist eine endliche Erweiterung, denn $\dim_k L = \deg p < \infty$, also ist L algebraisch. Außerdem gilt: f hat in L eine Nullstelle. Nach 4) ist $L = k$, also hat f bereits in k eine Nullstelle. $\square$

Definition 3.4
Sei k ein Körper. Ein Oberkörper $\overline{k}/k$ heißt algebraischer Abschluss von k, falls gilt:

1) $\overline{k}$ ist algebraisch abgeschlossen

2) $\overline{k}/k$ ist algebraisch

Achtung: $\mathbb{C}$ ist kein algebraischer Abschluss von $\mathbb{Q}$!

Nicht verwechseln mit algebraischer Abschluss von k in einem Oberkörper $L = \{l \in L \mid l \text{ ist algebraisch über } k\}$.

Definition 3.5
Seien R, S Ringe (später meistens Körper) die beide den Ring T als Unterring besitzen. Ein Ringmorphismus $\varphi : R \to S$ heißt T-Morphismus, falls $\varphi\mid_T = id_T$.

Beispiel 3.6
$R = S = \mathbb{C}$, $T = \mathbb{R}$. Dann ist die Konjugation

$$\begin{aligned} \varphi : \mathbb{C} &\to \mathbb{C} \\ z &\mapsto \overline{z} \end{aligned}$$

ein $\mathbb{R}$-Morphismus.

Satz 3.7
Sei k ein Körper, $\overline{k}$ ein algebraischer Abschluss von k. Sei L/k algebraisch, sei L_0 ein Zwischenkörper $k \subseteq L_0 \subseteq L$. Sei weiter ein k-Morphismus $\varphi_0 : L_0 \to \overline{k}$ gegeben.
Dann existiert eine Fortsetzung $\varphi : L \to \overline{k}$ (d.h. ein Körpermorphismus φ, sodass $\varphi \mid_T L_0 = \varphi_0$).

Insbesondere ($L_0 = k$): jede algebraische Körpererweiterung von k bettet in $\overline{k}$ ein.

Typische Anwendung: Sei k ein Körper, seien $\overline{k}$ und $\overline{k}'$ zwei algebraische Abschlüsse von k. Dann $\overline{k} \simeq \overline{k}'$.

Beweis. Wende den Satz 3.7 an mit $L = \overline{k}', L_0 = k$ und $\varphi_0 = Id_k$. Der Satz sagt dann, dass es einen Körpermorphismus (sogar k-Morphismus) gibt

$$\varphi : \overline{k}' \to \overline{k}$$

Wir wissen: φ ist injektiv. Wir behaupten: φ ist sogar surjektiv. Der Grund dafür ist: Wir haben eine Kette von Körpern $k \subseteq \operatorname{Bild}(\varphi) \subseteq \overline{k}$.

Wir wissen auch: $\operatorname{Bild}(\varphi) \simeq \overline{k}'$ ist algebraisch abgeschlossen. $\overline{k}/k$ ist algebraisch $\Rightarrow$ $\overline{k}/\operatorname{Bild}(\varphi)$ ist algebraisch.

Insgesamt: $\overline{k} = \operatorname{Bild}(\varphi)$, denn algebraisch abgeschlossene Körper haben keine echten algebraischen Erweiterungen. □

Beweis. (zu Satz 3.7) Verwende Zorns Lemma und betrachte

$$\begin{aligned} M = \{(L', \varphi') \mid & L' \text{ ist Zwischenkörper } L_0 \subseteq L' \subseteq L \text{ und} \\ & \varphi' : L' \to \overline{k} \text{ ist Körpermorphismus mit } \varphi'_{|L_0} = \varphi_0\} \end{aligned}$$

Definiere eine Halbordnung durch $(L', \varphi') \leq (L'', \varphi'')$ falls gilt:

1) $L' \subseteq L''$

2) $\varphi''_{|L'} = \varphi'$

Fakt ohne Beweis: Das ist tatsächlich eine Halbordnung.

Zwischenbehauptung: In $(M, \leq)$ hat jede Kette eine obere Schranke.

Sei $(L_\lambda, \varphi_\lambda)_{\lambda\in\Lambda}$ eine Kette. Dann ist $L' := \bigcup_{\lambda\in\Lambda} L_\lambda$ ein Unterkörper von L (sogar Zwischenkörper: $L_0 \subseteq L' \subseteq L$). Sei $a \in L'$ und seien $\lambda_1, \lambda_2 \in \Lambda$ sodass $a \in L_{\lambda_1}$ und $a \in L_{\lambda_2}$ ist. Dann gilt:

$$\varphi_{\lambda_1}(a) = \varphi_{\lambda_2}(a)$$

Auswahlaxiom sagt: finde Abbildung $\eta : L' \to \Lambda$ sodass für alle a $L_{\eta(a)} \ni a$.

Definiere dann:

$$\begin{aligned} \varphi' : & L' \to \overline{k} \\ & a \to \varphi_{\eta(a)}(a) \end{aligned}$$

Das ist ein Körpermorphismus, der φ_0 fortsetzt. Also ist (L', φ') eine obere Schranke für die Kette.

Insgesamt sagt Zorns Lemma: Es gibt ein maximales Element $(L_{\max}, \varphi_{\max}) \in M$. Wir sind fertig, wenn wir zeigen: $L_{\max} = L$.
Angenommen es gibt $a \in L \setminus L_{\max}$.

Wir wissen: a ist algebraisch über $L_{\max}$, mit Minimalpolynom

$$f(x) = \sum \lambda_i x^i \in L_{\max}[x]$$

Wir wissen auch:

$$L_{\max}(a) \simeq L_{\max}[x]/(f)$$

Betrachte das Polynom

$$\overline{f} = \sum \varphi_{\max}(\lambda_i) \cdot x^i \in \operatorname{Bild}(\varphi_{\max})[x] \subset \overline{k}[x]$$

Wir wissen: $\overline{f}$ hat eine Nullstelle $\overline{a} \in \overline{k}$ und

$$\operatorname{Bild}(\varphi_{\max})(\overline{a}) \simeq \operatorname{Bild}(\varphi_{\max})[x]/(\overline{f}) \simeq L_{\max}[x]/(f) \simeq L_{\max}(a)$$

Insgesamt haben wir also einen Morphismus

$$L_{\max} \subsetneq L_{\max}(a) \overset{\varphi_{\mathrm{mmax}}}{\hookrightarrow} \operatorname{Bild}(\varphi_{\eta(a)}\mathrm{max})(\overline{a}) \subseteq \overline{k}$$

Per Konstruktion ist $\varphi_{\mathrm{mmax}} |_{L_{\max}} = \varphi_{\max}$

Insgesamt: $(L_{\max}, \varphi_{\max}) \lneq (L_{\max}(a), \varphi_{\mathrm{mmax}})$, $\lightning$ zur Maximalität von $(L_{\max}, \varphi_{\max})$. $\square$

Definition 3.8 (Polynomringe in ∞ vielen Variablen)
Sei $(x_\lambda)_{\lambda\in\Lambda}$ eine Menge von Variablennamen, sei R ein Ring. Dann betrachte:

$$R[(x_\lambda)_{\lambda\in\Lambda}] = \bigcup_{\{x_{\lambda_1},\ldots,x_{\lambda_n}\}\ \mathit{endl.}} R[x_{\lambda_1},\ldots,x_{\lambda_n}]$$

Bemerkung: Polynome enthalten immer nur endlich viele Terme und endlich viele Variablen!

Fakt: (universelle Eigenschaft) Gegeben sei ein Ringmorphismus $\varphi : R \to S$ und eine beliebige Abbildung: $\alpha : \Lambda \to S$. Dann gibt es genau einen Ringmorphismus $\Phi : R[(x_\lambda)_{\lambda\in\Lambda}] \to S$ sodass $\Phi_{|R} = \varphi$

$$\exists\lambda \in \Lambda : \Phi(x_\lambda) = \alpha(\lambda)$$

Idee:

$$\Phi(x_{\lambda_1}^2 + x_{\lambda_2} + r \cdot x_{\lambda_3}^7 \cdot x_{\lambda_4}) = \alpha(\lambda_1)^2 + \alpha(\lambda_2) + \varphi(r) \cdot \alpha(\lambda_3)^7 \cdot \alpha(\lambda_4)$$

Satz 3.9 (Steinitz)
Sei k ein Körper. Dann existiert ein algebraischer Abschluss.

Beweis. (Mike Artin) Betrachte:

- $\Lambda = \{$nicht-konstante Polynome in $k[x]\}$
- Polynomring $k[(x_\lambda)_{\lambda\in\Lambda}] =: P$
- Für jedes $f \in \Lambda$ das Element $f(x_f)$
- Das Ideal $I = (f(x_f) \mid f \in \Lambda)$

Behauptung 1: $I \subsetneq P$ d.h. $1 \notin I$

Beweis: Angenommen es wäre $1 \in I$. Dann können wir schreiben:

$$1 = \sum_{i=1}^{n} g_i \cdot f_i(x_{f_i})$$

für geeignete $f_1, \ldots, f_n \in \Lambda, g_1, \ldots, g_n \in P$. Das kann nicht sein!

Erinnerung: Es gibt eine Körpererweiterung k_1/k sodass f_1 eine Nullstelle $a_1 \in k_1$ hat.

Wiederholte Anwendung: Es gibt eine Körpererweiterung k'/k sodass für alle i gilt: f_i hat in k' eine Nullstelle $a_i \in k'$.

Universelle Eigenschaft: Es gibt Ringmorphismus $\Phi : P \to k'$ sodass für alle i gilt $x_{f_i} \mapsto a_i$.

Dann ist

$$\Phi(1_{k'}) = \Phi(1_P) = \sum_{i=1}^{n} \underbrace{\Phi(g_i) f_i(a_i)}_{=0} = 0$$

Widerspruch! Damit ist Behauptung 1 bewiesen.

Erinnerung: I ist vielleicht nicht maximal, aber Zorn sagt: Es gibt ein maximales Ideal $I \subseteq m \subsetneq P$.

Erinnerung: $E_1 := P/m$ ist ein Körper.

Wesentliche Eigenschaften dieses Körpers.

1) Haben Abbildung $k \to P \to E_1 = P/m, a \mapsto$ konst. Pol. a. Diese Abbildung ist injektiv, deshalb Inklusion von Körpern. Fasse ab sofort k als Unterkörper von E_1 auf.

2) Die Polynome $f \in \Lambda$ haben Nullstellen in E_1, nämlich $f(x_f) \in I \subset m$, also $f([x_f]) = 0$ in $E_1 = P/m$

3) Die Körpererweiterung E_1/k ist algebraisch. Sei $a \in E_1$ irgendein Element. Schreibe $a = [g]$, wobei $g \in P$ ein Polynom in den endlich vielen Variablen $x_{\lambda_1}, \dots, x_{\lambda_n}$ ist. Dann $a \in k([x_{\lambda_1}], \dots, [x_{\lambda_n}]) \subset E_1$.

   Wir wissen aber: für alle i ist $[x_{\lambda_i}]$ Nullstelle des Polynoms $\lambda_i \in \Lambda$.

Beobachtung: Es ist nicht klar, dass E_1 ein algebraischer Abschluss von k ist.

Wir wissen: Polynome mit Koeffizienten in k haben in E_1 eine Nullstelle.

Wir wissen nicht: Polynome mit Koeffizienten in E_1 haben in E_1 eine Nullstelle.

Wir wiederholen diese Konstruktion und erhalten die Erweiterungen

$$k \subseteq E_1 \subseteq E_2 \subseteq \dots$$

sodass für alle $i \in \mathbb{N}$ jedes nicht-konstante Polynom in $E_i[x]$ eine Nullstelle in E_{i+1} hat und E_{i+1}/E_i algebraisch ist. Insbesondere ist E_i/k algebraisch.

Setze

$$E := \bigcup_i E_i$$

dann gilt:

1) Weil wir eine Kette haben, ist E ein Körper

2) Gegeben $a \in E$. Dann $\exists x : a \in E_i$, also ist a algebraisch über k. $\Rightarrow E/k$ ist algebraisch.

3) Sei $f \in E[x]$ ein Polynom, $f(x) = \sum_{j=1}^n e_j x^j$. Dann gibt es ein $i \in \mathbb{N} : \forall j : e_j \in E_i$. Das Polynom $f \in E_i[x]$ hat also eine Nullstelle in $E_{i+1} \subseteq E$.

$\square$

Definition 3.10
Sei k ein Körper, f ein nicht konstantes Polynom, $f \in k[x]$. Eine Erweiterung L/k heißt Zerfällungskörper von f, falls gilt:

1) f zerfällt in $L[x]$ in ein Produkt von linearen Polynomen

$$f = \mathrm{const} \cdot \prod (x - a_i) \in L[x]$$

2) $L = k(a_1, \dots, a_n)$

<u>Wesentliches Problem:</u> Gegeben k und f, finde ein L.

Satz 3.11
Sei k ein Körper, dann gilt:

1) Jedes nicht-konstante f hat einen Zerfällungskörper

2) Gegeben f, dann sind je zwei Zerfällungskörper von f isomorph

3) Gegeben f und ein Zerfällungskörper L, dann ist

$$[L : k] \leq (\deg f)!$$

Beweis. <u>1)</u> Sei f gegeben. Seien $a_1, \dots, a_n \in \overline{k}$ die Nullstellen, dann setze $L = k(a_1, \dots, a_n) \subseteq \overline{k}$.

<u>2)</u> Sei f gegeben. Wähle L wie in Schritt 1), sei L' ein weiterer Zerfällungskörper, seien $a_1', \dots, a_n'$ die Nullstellen von f in L'.

Wir wissen: L'/k ist algebraisch. Nach universeller Eigenschaft haben wir einen k-Morphismus

$$\varphi : L' \to \overline{k} \supseteq L$$

Banale Beobachtung: Die Abbildung φ bildet Nullstellen von f auf Nullstellen von f in $\overline{k}$ ab. Sei $a_i \in L$ eine Nullstelle. Dann schreibe $f(x) = \sum f_i \cdot x^i$, wobei $f_i \in k$. Dann ist

$$0_{\overline{k}} = \varphi(f(a)) = \varphi\left(\sum f_i \cdot a^i\right) = \sum \varphi(f_i) \cdot \varphi(a)^i = \sum f_i \varphi(a)^i = f(\varphi(a))$$

Also: $\forall i : \varphi(a_i') = a_j$ für geeignetes j.

$$\Rightarrow \mathrm{Bild}(\varphi) = \varphi(k(a_1', \ldots, a_n')) \subseteq \underbrace{k(a_1, \ldots, a_n)}_{=L} \subseteq \overline{k}$$

Andererseits: $\mathrm{Bild}(\varphi)$ ist ein Zerfällungkörper, enthält alle n Nullstellen $\Rightarrow \mathrm{Bild}(\varphi) = L$.

$\Rightarrow \varphi$ ist Isomorphismus

3) Sei f gegeben, seien $a_1, \ldots, a_n \in L$ die Nullstellen. Dann ist $L = k(a_1, \ldots, a_n)$ und wir haben eine Kette

$$k \subseteq k(a_1) \subseteq k(a_1, a_2) \subseteq \ldots$$

Dann:

- f ist Polynom in k, das a_1 als Nullstelle hat
$$[k(a_1) : k] \leq \deg f$$
- $f/(x - a_1)$ ist Polynom in $k(a_1)$, das a_2 als Nullstelle hat
$$[k(a_1, a_2) : k(a_1)] \leq n - 1$$
- Wiederholte Anwendung liefert:
$$[L : k] \leq n!$$

□

Beispiel 3.12
$k = \mathbb{Q}$, $f = x^2 - 2$.
Dann ist $L = \mathbb{Q}(-\sqrt{2}, \sqrt{2})$ der Zerfällungskörper und

$$[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$$

sowie

$$[\mathbb{Q}(\sqrt{2}, -\sqrt{2}) : \mathbb{Q}(\sqrt{2})] = 1$$

$\Rightarrow \deg[L : \mathbb{Q}] = 2.$

Beispiel 3.13
$k = \mathbb{Q}$, $f = x^3 - 2$. Dann:

$$L = \mathbb{Q}(\sqrt[3]{2}, \xi\sqrt[3]{2}, \xi^2\sqrt[3]{2})$$

wobei $\xi = e^{\frac{2\pi i}{3}}$, und

$$[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$$

und

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

weil $\mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{R}$, $\xi \notin \mathbb{R}$

$\Rightarrow [L : \mathbb{Q}] = 6$

Nächstes Ziel: Zerfällungskörper verstehen. Dazu Nullstellenmengen von (irreduziblen) Polynomen verstehen.

Dazu Sprache: Sei $S \supseteq R$ eine Erweiterung von Ringen und sei $(a_\lambda)_{\lambda\in\Lambda}$ eine Familie von Elementen aus S. Betrachte dann:

$$\bigcap_{\substack{\text{Zwischenringe} R \subseteq A \subseteq S \\ \forall \lambda \in \Lambda, a_\lambda \in A}} A = R[(a_\lambda)_{\lambda\in\Lambda}]$$

Fakt:

- $R[(a_\lambda)_{\lambda\in\Lambda}]$ ist ein Unterring von S, der alle a_λ enthält.
- $R[(a_\lambda)_{\lambda\in\Lambda}]$ ist der kleinste Unterring von S der alle $(a_\lambda)_{\lambda\in\Lambda}$ enthält.
- Sei $\varphi : R[(x_\lambda)_{\lambda\in\Lambda}] \to S$ die eindeutige Abbildung, die $\forall\lambda$ x_λ auf a_λ abbildet. Dann ist $R[(a_\lambda)_{\lambda\in\Lambda}] = \text{Bild}(\varphi)$

Auf Deutsch: Elemente von $R[(a_\lambda)_{\lambda\in\Lambda}]$ sehen aus wie Polynome in a_λ.

$$r_1 a_{\lambda_1}^7 a_{\lambda_2} + r_2 a_{\lambda_3}^8 \cdot a_{\lambda_4} \cdot a_{\lambda_1}$$

Spezialfall: Die Ringe R, S sind Körper. Gegeben also eine Körpererweiterung L/k und Familie von Elementen aus L, $A := (a_\lambda)_{\lambda\in\Lambda} \subseteq L$. Dann haben wir Ringe/Körper

$$k \subseteq k[A] \overset{i}{\hookrightarrow} k(A) \subseteq L$$

und wir haben $k[A] \hookrightarrow Q(k[A])$. Zudem erhalten wir genau ein $\eta : Q(k[A]) \to k(A)$ wobei η durch die universelle Eigenschaft des Quotientenkörpers gegeben ist.

Klar: $\text{Bild}(\eta)$ ist Unterkörper von $k(A)$, der $k[A]$ enthält $\Rightarrow \text{Bild}(\eta) = k(A)$. Also η ist isomorph.

Satz 3.14
Situation wie oben. Dann

$$k(A) \cong Q(k(A))$$

mit kanonischer Isomorphie.

Beispiel 3.15
$k = \mathbb{R}$, $L = \mathbb{C} = \mathbb{R}(i)$

Wir wissen: jede komplexe Zahl können wir schreiben als $r_1 + ir_2$, also $\mathbb{R}[i] = \mathbb{R}(i) = \mathbb{C}$.

Allgemein: Sei L/k eine Körpererweiterung, sei $a \in L$ algebraisch über k. Dann können wir alle Elemente von $k(a)$ schreiben als $k_0+k_1\cdot a+k_2a^2+\cdots+k_{n-1}a^{n-1}$, wobei $n = [a : k]$. Also $k(a) = k[a]$.

Beispiel 3.16
L/k Körpererweiterung, $a \in L$ sei transzendent über k. Dann haben wir eine Abbildung

$$\varphi : k[x] \to k[a] \subseteq k(a), \quad f(x) \mapsto f(a)$$

Per Definition ist φ surjektiv. Per Annahme a transzendent ist φ injektiv. $\Rightarrow k[a] \cong k[x]$. Insbesondere ist $k[a]$ kein Körper, also $\neq k(a)$. Induktiv beweist man:

Satz 3.17
Sei L/k eine Körpererweiterung, seien $a_1, \ldots, a_n \in L$ endlich viele Elemente, dann sind äquivalent

1) *alle a_i sind algebraisch*

2) $k[a_1, \ldots, a_n] = k(a_1, \ldots, a_n)$

Bemerkung: Achtung: für ∞ viele Elemente ist das falsch! z.B. sei L/k beliebig, $A = L$. Dann ist $k[A] = k(A)$.

3.3 Separable und Inseparable Körpererweiterungen

Frage: Sei L/k Erweiterung, $a \in L$ sei algebraisch über k und $f \in k[x]$ das Minimalpolynom. Kann f mehrfache Nullstellen in L haben?

Teilantwort: Wenn $k = \mathbb{Q}$ ist, geht das nicht! Denn wenn f die Zahl $a \in L$ als mehrfache Nullstelle hat, dann $f'(a) = 0$. $\lightning$ zur Annahme f Minimalpolynom.

Ziel: Argument erweitern zu beliebigen Körpern

Definition 3.18
Sei k ein Körper, $f \in k[x]$ ein Polynom. Dann schreibe

$$f(x) = \sum_{i=0}^{n} a_i \cdot x^i$$

und setze

$$f'(x) = \sum_{i=1}^{n} \underline{i} \cdot a_i \cdot x^{i-1}$$

wobei $\underline{i} = \underbrace{1 + \cdots + 1}_{i-mal} \in k$

Satz 3.19
Alle bekannten Ableitungsregeln gelten.

Zurück zur Frage: Wenn k ein beliebiger Körper der Charakteristik 0 ist, und a eine mehrfache Nullstelle von f ist (d.h. in $L[x]$), können wir schreiben:

$$f = (x-a)(x-a) \cdot \text{rest}$$

Dann sagt die Ketten-/Produkt-Regel dass f' das Element a immer noch als Nullstelle hat, wegen $\text{char}(k) = 0$ und $f' \not\equiv 0$. Also $\lightning$ wie oben.

Bemerkung: In $\text{char}(k) = p > 0$ ist immer noch wahr, dass $f'(a) = 0$ ist, aber es könnte sein, dass $f' \equiv 0$.

Definition 3.20
Ein irreduzibles Polynom f heißt separabel, wenn f in $\overline{k}$ keine mehrfache Nullstelle hat. Ein beliebiges Polynom f ist separabel, wenn alle irreduziblen Faktoren separabel sind. Ansonsten nenne f inseparabel.

Bemerkung: Falls $\text{char}(k) = 0$, sind alle Polynome separabel.

Bemerkung: (Nicht-irreduzible) separable Polynome können mehrfache Nullstellen haben.

Konstruktion mit Frobenius-Morphismus: Sei R ein Ring sowie $R \to S$ ein Ringmorphismus. Dieser induziert einen Ringmorphismus $R[x] \to S[x]$. Für $S = R$ und den Frobenius-Morphismus erhalten wir den Ringmorphismus

$$\eta : R[x] \to R[x], \quad \sum a_i x^i \mapsto a_i^p x^i$$

Falls R Integritätsring ist, ist η injektiv.

$\text{Bild}(\eta) = (R^p)[x] \subseteq R[x]$ und die Abbildung $\eta : R[x] \to R^p[x]$ ist ein Isomorphismus.

Satz 3.21 (Charakterisierung inseparabler Polynome)
Sei k ein Körper, sei $f \in k[x]$ irreduzibel. Dann sind äquivalent

1) f *ist inseparabel*

2) $f' \equiv 0$

3) $p = \mathrm{char}(k)$ *ist eine Primzahl. Es gibt ein irreduzibles separables* $g \in k[x]$ *und* $n \in \mathbb{N}$ *sodass* $f(x) = g(x^{p \cdot n}) = g((x^p)^n)$.

Beweis. $\underline{1) \Rightarrow 2)}$: Sei f inseparabel, d.h. f hat in $\overline{k}$ eine mehrfache Nullstelle a, dann ist auch $f'(a) = 0$. Widerspruch zur Irreduzibilität falls $f \not\equiv 0$. Also $f' \equiv 0$.

$\underline{2) \Rightarrow 3)}$: Sei $f(x) = \sum_{i=0}^{n} a_i x^i$. Dann:

$$f'(x) = \sum_{i=1}^{n} a_i \cdot i \cdot x^{i-1}$$

wobei i hier $\varphi(i) = \underbrace{1 + \cdots + 1}_{i\text{-mal}}$.

Falls $\mathrm{char}(k) = 0$ wäre, dann wäre $\forall i$ mit $a_i \neq 0$ auch $i \cdot a_i \neq 0$, also $f'(x) \not\equiv 0$ $\lightning$. Somit ist $\mathrm{char}(k) = p > 0$. Die Zahl p ist prim weil k ein Körper ist.

Beobachtung: Falls i kein Vielfaches von p ist, dann $\varphi(i) \neq 0$. Es ist aber $a_i \cdot \varphi(i) = 0 \Rightarrow a_i = 0$ für alle i, die kein Vielfaches von p sind. Also

$$f(x) = \sum_{j=0}^{n/p} a_{j \cdot p} x^{j \cdot p}$$

Setze $g_1(x) = \sum_{j=0}^{n/p} a_{j \cdot p} x^j$. Dann $f(x) = g_1(x^p)$.

Idee: Falls g_1 inseparabel ist, wiederhole Prozedur, finde $g_2(x)$ sodass $g_1(x) = g_2(x^p)$ ($\Rightarrow f(x) = g_2(x^{2p})$). Weil der Grad der Polynome dabei sinkt, endet diese Prozedur nach endlich vielen Schritten, finde $g = g_n$ sodass $f(x) = g(x^{n \cdot p})$ und g separabel ist.

Damit das funktioniert, müssen wir zeigen, dass g_1 irreduzibel ist (per Induktion sind dann auch $g_2, \ldots, g_n = g$ irreduzibel).

Erinnerung: hatten Morphismen

$$\varphi_1 : k[x] \to (k^p)[x], \quad \sum h_i \cdot x^i \mapsto \sum h_i^p \cdot x_i$$

$$\mathcal{F} : k[x] \to (k^p)[x^p] \subseteq (k^n)[x] \subseteq k[x], \quad \sum h_i \cdot x^i \mapsto \sum h_i^p \cdot x^{i \cdot p}$$

Nachrechnen: es ist $\varphi(f) \in (k^p)[x^p]$ weil $f \in k[x^p]$ und $g = \mathcal{F}^{-1}(\varphi(f))$. Da $\varphi, \mathcal{F}$ Isomorphismen sind folgt aus f irreduzibel g_1 irreduzibel.

3) $\Rightarrow$ 1): Angenommen f hat folgende Eigenschaft: $\exists g(x) \in k[x] : f(x) = g(x^p)$. Sei $a \in \overline{k}$ eine Nullstelle von g, d.h. $g(x) = (x - a) \cdot \text{rest}$ in $\overline{k}[x]$. Wähle $b \in \overline{k}$ mit $b^p = a$ (das geht, weil $\overline{k}$ algebraisch abgeschlossen ist). Dann

$$g(x^p) = (x^p - b^p) \cdot \text{rest} = (x - b)^p \cdot \text{rest}$$

$\Rightarrow b \in \overline{k}$ ist p-fache Nullstelle von f, also f inseparabel. □

Warum diese Diskussion von Inseparabilität? Antwort kommt jetzt!

Lemma 3.22
Sei L/k eine Körpererweiterung und $a \in L$, sei algebraisch über k. Setze $M = k(a)$. Sei $f(x) \in k[x]$ das Minimalpolynom von a. Angenommen f hat exakt m unterschiedliche Nullstellen in $\overline{k}$. Dann gibt es genau m unterschiedliche k-Morphismen

$$\varphi : M \to \overline{k}$$

Bemerkung: Falls f separabel ist, $m = \deg f$. Falls f inseparabel ist, ist $m < \deg f$.

Beweis. Beobachtung 1: Wir wissen schon: Die Elemente von M können wir schreiben als

$$\lambda_0 + \lambda_1 a + \lambda_2 a^2 + \cdots + \lambda_{n-1} a^{n-1}$$

mit $\lambda_i \in k$ wobei $n = \deg f$. Insbesondere ist für alle solche Elemente

$$\varphi(\lambda_0 + \lambda_1 a + \cdots + \lambda_{n-1} a^{n-1}) = \sum \lambda_i \varphi(a)^i$$

Das bedeutet: φ ist durch $\varphi(a)$ eindeutig festgelegt!

Beobachtung 2: Gegeben einen k-Morphismus φ, dann ist $\varphi(a)$ eine Nullstelle des Polynoms $f(x) \in k[x]$, wir haben aber nur m unterschiedliche Nullstellen!

Insgesamt also höchstens m unterschiedliche Morphismen!

Noch zu zeigen: Wenn $b \in \overline{k}$ eine Nullstelle von f ist, dann existiert ein k-Morphismus $\varphi : M \to \overline{k}$ sodass $\varphi(a) = b$ ist.

Erinnerung: Wir wissen $M \simeq k[x]/(f)$, wobei a mit $[x]$ identifiziert wird.

Haben Morphismus:

$$\Omega : k[x] \to \overline{k}, \quad g \mapsto g(b)$$

Dann $f \in \mathrm{Ker}(\Omega)$, der Kern ist ein Hauptideal und f irreduzibel, also: $(f) = \ker(\Omega)$. Also erhalte (nach universeller Eigenschaft) einen Morphismus $k[x]/(f) \to \overline{k}$ wobei $[x] \mapsto b$.

Erhalte $M \to \overline{k}$ durch Komposition der Morphismen.

Varianten mit völlig analogem Beweis

Lemma 3.23
Sei L/k eine Körpererweiterung. $a \in L$ algebraisch mit Minimalpolynom $f \in k[x]$. f hat m unterschiedliche Nullstellen in L. Dann gibt es genau m unterschiedliche k-Morphismen $\varphi : M \to L$, wobei $M = k(a)$ ist.

Lemma 3.24
Seien L_1 und L_2 Körper und $\sigma : L_1 \to L_2$ Körpermorphismen. $a \in L_2$ sei algebraisch über $\mathrm{Bild}(\sigma)$ *mit Minimalpolynom f. Angenommen f hat m unterschiedliche Nullstellen in L_2. Dann gibt es genau m unterschiedliche Fortsetzungen von σ zu Morphismen $\Sigma : M \to L_2$, wobei $M \supseteq L$, der Körper $\sigma(L_1)(a)$.*

□

Spezialfall: $M = \overline{k}$. Dann hat f (mit Vielfachheit) genau $n = \deg f$ Nullstellen. Beachte f separabel $\Leftrightarrow$ n unterschiedliche Nullstellen $\Leftrightarrow$ n unterschiedliche Fortsetzungen von φ zu $k(a)$.

Definition 3.25
Sei L/k Körpererweiterung. Nenne algebraisches $a \in L$ separabel, wenn das zugehörige Minimalpolynom separabel ist. Nenne L/k separabel, falls alle $a \in L$ algebraisch und separabel über k sind. Nenne L/k inseparabel falls algebraisches $a \in L$ existiert, das nicht separabel über k ist.

Satz 3.26
Sei L/k eine endliche Körpererweiterung und $n := [L : k]$. Dann gilt:

1) *Es gibt höchstens n k-Morphismen $L \to \overline{k}$*

2) *L/k ist genau dann separabel, wenn es exakt n solche Morphismen gibt*

Beweis. Vorbereitung: Wegen der Endlichkeit, finde $a_1, \dots, a_l \in L$ sodass $L = k(a_1, \dots, a_l)$. Betrachte Kette von Erweiterungen

$$k \subseteq k(a_1) \subseteq k(a_1, a_2) \subseteq \cdots \subseteq k(a_1, \dots, k_l) = L$$

Sei $k_0 = k$ und $k_l = k_{l-1}(a_l)$.

1) *Erinnerung:* es gibt höchstens $[a_1 : k_0]$ viele unterschiedliche k-Morphismen $\sigma_1 : k_1 \to \overline{k}$.

Erinnerung: Gegeben $\sigma_1 : k_1 \to \overline{k}$, dann gibt es maximal $[a_2 : k_1]$ viele Fortsetzungen von σ_1 zu Morphismen $\sigma_2 : k_2 \to \overline{k}$.

Erinnerung: Gegeben $\sigma_i : k_i \to \overline{k}$, dann gibt es höchstens $[a_{i+1} : k_i]$ viele Fortsetzungen von σ_i zu $\sigma_{i+1} : k_{i+1} \to \overline{k}$.

Insgesamt: Maximal

$$[a_1 : k_0] \cdot [a_1 : k_2] \cdot \dots \cdot [a_l : k_{l-1}] = [L : k]$$

viele Fortsetzungen von $Id_k : k \to \overline{k}$ zu Morphismen $L \to \overline{k}$.

2) Angenommen L/k ist separabel. Wir wissen: die maximale Zahl von Erweiterungen existiert, falls für alle i gilt a_{i+1} ist separabel über k_i. Per Annahme: a_{i+1} ist separabel über k.

Aber: $f_{k_i} \mid f_k$ also klar, dass f_{k_i} keine mehrfachen Nullstellen hat.

b) $\Leftarrow$ Angenommen L/k nicht separabel. Wir können die a_i so wählen, dass bereits a_1/k nicht separabel ist.

$\Rightarrow$ wir haben weniger als $[a_1 : k_0]$ viele k-Morphismen $\sigma_i : k_1 \to \overline{k}$.

$\Rightarrow$ wir haben insgesamt weniger als $[L : k]$ viele k-Morphismen $\sigma_l : L \to \overline{k}$. □

Folgerung 3.27
Sei L/k endlich. $n = [L : k]$. Sei M/k algebraisch. Dann gibt es höchstens n unterschiedliche k-Morphismen $L \to M$.

Beweis. Bette M in $\overline{k}$ ein. Dann liefert jeder k-Morphismus $L \to M$ automatisch einen k-Morphismus $L \to \overline{k}$. □

Folgerung 3.28
Sei L/k endlich. $L = k(a_1, \dots, a_l)$. Falls für alle i gilt, dass a_{i+1} separabel über $k(a_1, \dots, a_i)$ ist, dann gibt es genau $[L : k]$-viele k-Morphismen $L \to \overline{k}$.

Folgerung 3.29
Sei L/K eine Körpererweiterung. Seien $a_1, \dots, a_n \in L$. Wenn a_{i+1} separabel über $K(a_1, \dots, a_i)$ ist, dann ist $K(a_1, \dots, a_n)$ eine separable Erweiterung von K.

Folgerung 3.30
Sei $k \subseteq L \subseteq M$ eine Kette von Körpererweiterungen sodass L/k und M/L jeweils separabel sind, dann ist M/k separabel.

Beweis. Sei $m \in M$ gegeben. Betrachte das Minimalpolynom $f_L(x) \in L[x]$ von m. Schreibe $f_L(x) = \sum_{i=1}^n a_i x^i$, wobei $a_i \in L$ geeignete Koeffizienten sind.

Betrachte den Zwischenkörper

$$L' = k(a_0, \dots, a_{n-1})$$

und schreibe

$$L'' = k(a_0, \dots, a_{n-1}, m)$$

Wir wenden die letzte Folgerung auf L'' an, somit erhalten wir mit dem vorherigen Satz, dass L''/k separabel ist. Also ist m/k separabel. □

Folgerung 3.31
Sei L/k eine Körpererweiterung. Sei

$$L_{Sep} = \{l \in L \mid l \text{ ist separabel über } k\}$$

Dann ist L_{Sep} ein Unterkörper von L.

Notation: Nenne L_{Sep} den separablen Abschluss (separable Hülle) von k in L ist.

Beweis. Gegeben $a, b \in L_{\text{Sep}}$, müssen zeigen dass $a+b, a \cdot b, a-b$ und gegebenenfalls a/b in L_{Sep} liegen.

Wissen: all diese Elemente liegen in $k(a, b)$, das nach obiger Folgerung separabel ist. □

Notation: Sei L/k Körpererweiterung. Nenne $[L_{\text{Sep}} : k]$ den Sepearabilitätsgrad von L/k.

Definition 3.32
Nenne Körper k vollkommen, falls jede algebraische Körpererweiterung automatisch separabel ist.

Bemerkung: Trivial: Körper der char $= 0$ und algebraisch abgeschlossene Körper sind vollkommen.

Satz 3.33
Sei k ein Körper mit positiver Charakteristik. Dann ist äquivalent:

1) *k ist vollkommen*

2) *Der Frobenius-Morphismus $F : k \to k$ ist surjektiv*

Beweis. 1) $\Rightarrow$ 2) Beweis der Kontraposition: Sei F nicht surjektiv. Sei also $k \in k \setminus k^p$. Sei $b \in \overline{k}$ sodass $b^p = a$. (Erinnerung $F : \overline{k} \to \overline{k}$ ist injektiv, das heißt b ist eindeutig).

Betrachte die Erweiterung $k(b)/k$. Das Minimalpolynom von b ist Teiler von $x^p - a$ (das hat lediglich b als Nullstelle), hat also nur eine Nullstelle, nämlich b.

2) $\Rightarrow$ 1) Angenommen F wäre surjektiv, $k = k^p$. Angenommen k wäre nicht vollkommen, dann gäbe es ein inseparables, irreduzibles Prolynom $f(x) \in k[x]$.

Erinnerung: Es gibt $g \in k[x]$ sodass $f(x) = g(x^p)$. Schreibe $g(x) = \sum_{i=0}^n g_i \cdot x^i$.

Per Annahme $\forall i \exists h_i \in k$ mit $g_i = (h_i)^p$. Also

$$g(x) = \sum (h_i)^p x^i$$
$$g(x^p) = \sum (h_i x^i)^p = \left(\sum h_i x^i\right)^p$$

also ist $\sum h_i x^i$ ein echter Teiler von $f(x)$ in $k[x]$. $\lightning$ zur Irreduzibilität von f. $\square$

3.4 Galoissche Körpererweiterungen

Definition 3.34
Sei L/k eine Körpererweiterung. Betrachte die Menge

$$\mathrm{Gal}(L/k) = \{k\text{-}Morphismen\ L \to L\ die\ surjektiv,\ also\ isomorph\ sind\}$$

Beobachtung: $\mathrm{Gal}(L/k)$ ist eine Gruppe mit Einheit Id_L und der Hintereinanderausführung als Gruppenverknüpfung. Die Inversen sind die Umkehrabbildungen.

Diese Gruppe heißt Galoisgruppe

Variante: Sei k ein Körper, $f \in k[x]$ ein Polynom, L der Zerfällungskörper. Dann bezeichne $\mathrm{Gal}(L/k)$ auch als $\mathrm{Gal}(f)$ (Galoisgruppe von f).

Zentrale Beobachtung: Falls L/k endlich ist dann ist $\mathrm{Gal}(L/k)$ endlich und $\#\,\mathrm{Gal}(L/k) \leq [L : k]$.

Analog
$$\#\,\mathrm{Gal}(f) \leq [\text{Zerfällungskörper von } f : k] \leq (\deg f)!$$

Beispiel 3.35 *1) $k = \mathbb{Q}, L = \mathbb{Q}(\sqrt{2})$ Wissen: die Elemente von L schreiben sich als $a + b\sqrt{2}$ mit $a, b \in \mathbb{Q}$.*

Die Elemente der Galoisgruppe sind durch die Bilder von $\sqrt{2}$ festgelegt, und $\sqrt{2}$ kann nur auf andere Nullstellen von $x^2 - 2$ abgebildet werden. Es gibt aber nur eine andere Nullstelle, nämlich $-\sqrt{2}$.

$\Rightarrow \mathrm{Gal}(L/k) = \{Id, a + b\sqrt{2} \mapsto a - b\sqrt{2}\} \simeq (\mathbb{Z}/2\mathbb{Z}, +)$

2) *Analog* $\mathrm{Gal}(\mathbb{C}/\mathbb{R}) = \{Id_{\mathbb{C}}, \textit{Konjugation}\}$

3) $k = \mathbb{Q}, L = \mathbb{Q}(\sqrt[3]{2})$ *Wieder: Elemente der Galoisgruppe sind durch das Bild von $\sqrt[3]{2}$ bestimmt und als Bilder kommen nur die Nullstellen von $x^3 - 2$ in Frage. In L ist $\sqrt[3]{2}$ aber die einzige Nullstelle.*

$\Rightarrow \mathrm{Gal}(L/\mathbb{Q}) = \{Id_L\}$

4) *Sei k ein endlicher Körper, sei $\mathbb{F}_p$ der Primkörper von k. Betrachte $k/\mathbb{F}_p$. Betrachte den Frobenius-Morphismus $F : k \to k$.*

Beobachtung:

$$\begin{aligned} F(1) &= 1^p = 1 \\ F(1+1) &= 1+1 \\ &\vdots \\ F(1+\cdots+1) &= 1+\cdots+1 \end{aligned}$$

Das heißt für alle $a \in \mathbb{F}_p$ gilt $F(a) = a$.

Beobachte auch: Die $a \in k$, für die $F(a) = a$ gilt, sind exakt die Nullstellen des Polynoms $x^p - x$. Dieses Polynom hat höchstens p Nullstellen. Also für alle $a \in k$ gilt $F(a) = a \Leftrightarrow a \in \mathbb{F}_p$.

Insgesamt: Der Frobenius-Morphismus ist ein $\mathbb{F}_p$-Automorphismus von k. $F \in \mathrm{Gal}(k/\mathbb{F}_p)$.

Fakt: Die Galoisgruppe ist von F erzeugt, d.h. alle Elemente sind von der Form

- Id_k
- $\underbrace{F \circ \cdots \circ F}_{n\text{-mal}}$
- $\underbrace{F^{-1} \circ \cdots \circ F^{-1}}_{n\text{-mal}}$

Ziel: Die Galois-Gruppe ausrechnen!

Falls L/k algebraisch:

Beobachtung: Wir können stets L in $\overline{k}$ einbetten. Jedes $\sigma \in \operatorname{Gal}(L/k)$ ist dann automatisch ein Morphismus

$$L \to L \subseteq \overline{k}$$

Falls L/k endlich ist, wissen wir: Es existieren höchstens $[L : k]$ viele k-Morphismen $L \to \overline{k}$. Also

$$\# \operatorname{Gal}(L/k) \leq [L : k] \tag{1}$$

Frage: Haben wir Gleichheit?

Antwort: Im Allgemeinen nein!

- Falls L/k inseparabel ist, dann weniger als $[L : k]$ viele k-Morphismen $L \to \overline{k}$.
- Es kann passieren, dass für gegebenes $\sigma : L \to \overline{k}$, $\operatorname{Bild}(\sigma) \neq L$ ist. $\Rightarrow$ dieses σ liefert kein Element von $\operatorname{Gal}(L/k)$.

Definition 3.36
Sei L/k eine Körpererweiterung. Nenne L/k normal, wenn L/k algebraisch ist und wenn jedes irreduzible Polynom $f \in k[x] \setminus \{0\}$, das in L überhaupt eine Nullstelle hat, bereits über L in Linearfaktoren zerfällt.

Beispiel 3.37
- $\mathbb{C}/\mathbb{R}$ *ist normal*
- $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ *ist nicht normal, denn $x^3 - 2$ hat Nullstelle, zerfällt aber nicht.*
- $\overline{k}/k$ *ist immer normal*
- *Werden gleich sehen: Zerfällungskörper sind normal!*

Satz 3.38
Sei L/k eine algebraische Körpererweiterung. Dann sind folgende Aussagen äquivalent:

1) L/k ist normal

2) Es gibt eine Familie $(f_\lambda)_{\lambda \in \Lambda}$ von Polynomen in $k[x]$, sodass L durch Adjunktion sämtlicher Nullstellen der f_λ in $\overline{L}$ aus k entsteht.

3) Jeder k-Morphismus $\sigma : L \to \overline{L}$ hat $\operatorname{Bild}(\sigma) = L$

Beweis. L/k ist algebraisch. Wir betrachten L daher als Unterkörper von $\overline{k}$.

<u>1) $\Rightarrow$ 2) :</u> Finde Elemente $(a_\lambda)_{\lambda\in\Lambda}$ von L, sodass $L = k(a_\lambda \mid \lambda \in \Lambda)$. Die a_λ sind algebraisch über k und haben Minimalpolynome f_λ. Jedes der f_λ hat eine Nullstelle in L (nämlich a_λ), zerfällt also über L (da L/k normal). Sei jetzt $(b_\mu)_{\mu\in M}$ die Familie der Nullstellen aller f_λ. Per Annahme: alle $b_\mu \in L$ und $L = k(b_\mu \mid \mu \in M)$, da $L \subseteq \{b_\mu \mid \mu \in M\} \supseteq \{a_\lambda \mid \lambda \in \Lambda\}$.

<u>2) $\Rightarrow$ 3) :</u> Sei L wie in 2) gegeben. Das heißt es gibt Familie $(f_\lambda)_{\lambda\in\Lambda}$ von Polynomen, sodass $L = k(b_\mu \mid \mu \in M)$wobei $(b_\mu)_{\mu\in M}$ die Familie der Nullstellen der f_λ in $\overline{k}$ ist. Weiter sei ein k-Morphismus $\sigma : L \to \overline{k}$ gegeben. Wir müssen zeigen: $\mathrm{Bild}(\sigma) = L$.

Schritt 1: Zeige: $\mathrm{Bild}(\sigma) \subseteq L$. Da $L = k(b_\mu \mid \mu \in M)$ ist, genügt es zu zeigen dass für alle μ $\sigma(b_\mu) \in L$. Sei μ gegeben, per Definition finden wir ein λ sodass $f_\lambda(b_\mu) = 0$. Erinnerung: σ ist ein k-Morphismus und $f_\lambda \in k[x]$. Das bedeutet $\sigma(b_\mu)$ ist wieder eine Nullstelle von f_λ. Also $\sigma(b_\mu) \in L$.

Schritt 2: Zeige: $\mathrm{Bild}(\sigma) \supseteq L$. Es genügt zu zeigen: Für alle μ gilt $b_\mu \in \mathrm{Bild}(\sigma)$. Sei also ein μ gegeben. Wieder finde λ sodass $f_\lambda(b_\mu) = 0$. Das f_λ hat weitere Nullstellen $b_\mu, b_{\mu_1}, \ldots, b_{\mu_d}$ wobei $d = \deg(f_\lambda)-1$. Wir wissen: σ bildet die d Nullstellen $b_\mu, b_{\mu_1}, \ldots, b_{\mu_d}$ injektiv auf die Nullstellen von f_λ ab. $\Rightarrow \sigma(b_\mu) = b_\mu$, oder es gibt $1 \leq i \leq d$ sodass $\sigma(b_{\mu_i}) = b_\mu$.

<u>3) $\Rightarrow$ 1) :</u> Wir Müssen zeigen: jedes irreduzible $f \in k[x]$, das in L eine Nullstelle hat, zerfällt über L in Linearfaktoren. Sei also $f \in k[x]$ wie oben gegeben, sei $a \in L$ eine Nullstelle von f, sei $b \in \overline{k}$ eine weitere Nullstelle. Wir müssen zeigen: $b \in L$. Wir wissen: es gibt k-Isomorphismen

$$k(a) \longleftarrow k[x]/(f) \longrightarrow k(b)$$

sodass für die Komposition φ gilt $\varphi(a) = b$. Insgesamt haben wir

$$L \supseteq k(a) \xrightarrow{\varphi} k(b) \subseteq \overline{k}$$

Universelle Eigenschaft von $\overline{k}$. Wir können Morphismus φ fortsetzen zu $\sigma : L \to \overline{k}$. Per Annahme: $\mathrm{Bild}(\sigma) = L$, aber $b \in \mathrm{Bild}(\sigma)$. □

Folgerung 3.39
Sei L/k endlich. Dann ist äquivalent:

1) *L/k ist normal*

2) *L ist Zerfällungskörper eines einzigen Polynoms*

Beweis. <u>2) $\Rightarrow$ 1) :</u> folgt aus dem Satz

1) $\Rightarrow$ 2) : L/k ist endlich, also gibt es $a_1, \dots, a_n \in L$ sodass $L = k(a_1, \dots, a_n)$. Seien $f_1, \dots, f_n$ die Minimalpolynome. Behauptung: L ist Zerfällungskörper von $f = f_1 \cdot \ldots \cdot f_n$.

Seien $(b_\mu)_{\mu \in M}$ die Nullstellen von f. Weil L/k normal ist, folgt

$$L = k(a_1, \dots, a_n) = k(b_\mu \mid \mu \in M)$$

Also ist L der Zerfällungskörper. □

Folgerung 3.40
Sei L/k eine algebraische Körpererweiterung. Dann gibt es einen Oberkörper $k \subseteq L \subseteq N \subseteq \overline{k}$ sodass gilt

1) *N/k ist normal*

2) *Wenn wir einen Zwischenkörper $k \subseteq L \subseteq N' \subseteq N$ haben, sodass N'/k normal ist, so folgt: $N = N'$*

Wenn $\tilde{N}$ ein weiterer Oberkörper ist mit Eigenschaften 1) und 2) $\Rightarrow$ $\tilde{N}$ und $\tilde{N}$ sind k-Isomorph.

Nenne N/k die normale Hülle von L/k.

Beweis. Schreibe $L = k(a_\lambda \mid \lambda \in \Lambda)$. Seien f_λ die Minimalpolynome der a_λ. Sei $(b_\mu)_{\mu \in M}$ die Familie aller Nullstellen. Setze $N := k(b_\mu \mid \mu \in M)$. Mit Satz folgt N ist normal.

Sei N' ein Zwischenkörper. Um zu zeigen $N = N'$ müssen wir zeigen: alle $b_\mu \in N'$. Sei also μ gegeben, wähle λ sodass $f_\lambda(b_\mu) = 0$. Dann f_λ hat Nullstelle in N' (nämlich a_λ) also zerfällt f_λ über N', das heißt $b_\mu \in N' \Rightarrow N = N'$

Sei jetzt $\tilde{N}$ gegeben. Finde Einbettung $\sigma : \tilde{N} \to \overline{k}$. Es ist $\tilde{N} \simeq \mathrm{Bild}(\sigma)$. Also genügt es, den Fall zu betrachten, wo $\tilde{N} \subseteq \overline{k}$ und für jedes solche $\tilde{N}$ zu zeigen: $N = \tilde{N}$.

Beobachte: $N \cap \tilde{N}$ ist ein Oberkörper von L, der wieder normal ist.

Also haben wir

$$k =\subseteq L \subseteq N' \subseteq N$$

Da $N' = N \cap \tilde{N}$ folgt $N' = N$ daraus folgt $N \subseteq \tilde{N}$.

Die andere Inklusion $N \supseteq \tilde{N}$ folgt analog. □

Satz 3.41
Sei L/K eine endliche Körpererweiterung. Dann sind folgende Aussagen äquivalent

1) *L/K ist normal und separabel*

2) *L ist Zerfällungskörper eines separablen Polynoms $f \in K[x]$*

3) *$|\mathrm{Gal}(L/K)| = [L : K]$*

solche Körpererweiterungen heißen Galoissche Körpererweiterung.

Beweis. 1) $\Rightarrow$ 2) L ist der Zerfällungskörper eines $f \in K[x]$. Die irreduziblen Faktoren von f können keine mehrfache Nullstelle haben, denn ein solcher Faktor ist das Minimalpolynom eines separablen Elements $\in L$.

2) $\Rightarrow$ 1) L ist separabel, weil f separabel ist. L ist normal, denn es ist ein Zerfällungskörper über K.

1) $\Leftrightarrow$ 2) Sei $\overline{L}$ ein algebraischer Abschluss von L. $\sigma \in \mathrm{Gal}(L/K)$ kann zu einem K-Morphismus $L \to \overline{L}$ fortgesetzt werden.

Angenommen $[L : K] = n$, dann gibt es maximal n K-Morphismen $L \to \overline{L}$ und es gibt genau n weil L separabel ist. Außerdem ist L/K genau dann normal, wenn für jeden K-Morphismus $\tau : L \to \overline{K}$ gilt $\tau(L) = L$; deshalb ist τ ein Element von $\mathrm{Gal}(L/K)$. □

Folgerung 3.42
Sei K ein Körper der Charakteristik 0, dann ist jeder Zerfällungskörper über K Galois-Erweiterung.

Bemerkung: Wenn $K \subset L \subset M$ Körpererweiterungen sind und M/K Galois ist, dann ist M/L Galois, aber L/K muss nicht Galois sein.

Bemerkung: Sei $f \in K[x]$ ein separables Polynom mit Zerfällungkörper L. Dann notiere $\mathrm{Gal}(f) = \mathrm{Gal}(L/K)$.

1) Seien $\alpha_1, \ldots, \alpha_n$ die Nullstellen von f. Dann permutiert $\sigma \in \mathrm{Gal}(f)$ die $\alpha_1, \ldots, \alpha_n$, und σ wird durch diese Permutation eindeutig bestimmt. Wir können also $\mathrm{Gal}(f)$ als Untergruppe von S_n betrachten.

   Für $f(\alpha_i) = 0$ gilt

$$c_n \alpha_i^n + \cdots + c_1 \alpha_i + c_0 = 0 \qquad c_i \in K$$

   und damit

$$\begin{aligned} & \sigma(c_n \alpha_i^n + \cdots + c_1 \alpha_i + c_0) = \sigma(0) \\ \Rightarrow \quad & \sigma(c_n)\sigma(\alpha_i)^n + \cdots + \sigma(c_1)\sigma(\alpha_i) + \sigma(c_0) = 0 \\ \Rightarrow \quad & f(\sigma(\alpha_i)) = c_n \sigma(\alpha_i)^n + \cdots + c_1 \sigma(\alpha_i) + c_0 = 0 \end{aligned}$$

2) Die Nullstellen der irreduziblen Faktoren werden untereinander permutiert.

3) Wenn f irreduzibel ist, dann operiert $\mathrm{Gal}(f)$ transitiv auf der Menge der Nullstellen. (siehe Definition 4.3)

4) Sei $n = \deg(f)$ und f irreduzibel, dann gilt $n \mid |\mathrm{Gal}(f)|$

Beweis. 3) Seien a und b Nullstellen von f. Dann ist

$$L \supset K(a) \cong K[x]/(f) \cong K(b) \subset L$$

Und damit: ein Isomorphismus $\sigma : K(a) \to L$. σ kann zu einem K-morphismus $L \hookrightarrow \overline{L}$ erweitert werden. Da L/K normal ist, gilt $\sigma(L) = L$, also $\sigma \in \mathrm{Gal}(L/K)$. □

Definition 3.43
Sei L/K eine Galoissche Körpererweiterung und $\alpha \in L$ ein beliebiges Element. Dann nennen wir die Elemente $\sigma(\alpha), \sigma \in \mathrm{Gal}(L/K)$, die Konjugierten von α. Die Menge $\{\sigma(\alpha) \mid \sigma \in \mathrm{Gal}(L(K))\}$ ist die Menge der Nullstellen des Minimalpolynoms von α.

Beispiel 3.44
$f = X^3 - 3 \in \mathbb{Q}[X]$, hat Nullstellen $\sqrt[3]{2} \in \mathbb{R}$ und $\sqrt[3]{2} \cdot \zeta_3, \sqrt[3]{2} \cdot \zeta_3^2 \in \mathbb{C}$ mit $\zeta_3 = e^{2\pi i/3}$.

$\mathbb{Q}(\alpha)/\mathbb{Q}$ ist nicht Galois.

$L = \mathbb{Q}(\alpha, \zeta_3)$ ist der Zerfällungskörper von f.

$[L : \mathbb{Q}]$ ist 6. Denn $\mathrm{Gal}(f) \subset S_3$ und $\#S_3 = 6$ und damit $\mathbb{Q} \underset{3}{\subsetneq} \mathbb{Q}(\alpha) \underset{2}{\subsetneq} L$. Also $\mathrm{Gal}(f) = S_3$.

Satz 3.45
Sei K ein Körper und $G \subset \mathrm{Aut}(K)$ eine endliche Untergruppe. Dann ist

$$\mathrm{Fix}(G) = \{\alpha \in K \mid \sigma(\alpha) = \alpha, \forall \sigma \in G\}$$

ein Unterkörper von K, genannt der Fixkörper von G.

Satz 3.46 (E. Artin)
Sei G eine endliche Untergruppe von $\mathrm{Aut}(L)$ für einen beliebigen Körper L. Schreibe $K = \mathrm{Fix}(G)$. Dann ist L/K Galois, und $G = \mathrm{Gal}(L/K)$.

Insbesondere $[L : K] = \#G$.

Satz 3.47
Sei K ein endlicher Körper, mit q Elementen. Dann ist $q = p^m$ für eine Primzahl p und $m \in \mathbb{Z}_{>0}$. Außerdem ist K isomorph zu dem Zerfällungskörper von

$$x^q - x \in \mathbb{F}_p[x]$$

Umgekehrt, für jedes $q = p^m$, hat der Zerfällungskörper $\mathbb{F}_q$ von $x^q - x \in \mathbb{F}_p[x]$ q Elemente.

Die Galois Gruppe ist $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p) = (\mathbb{Z}/m\mathbb{Z}, +)$ *und wird erzeugt vom Frobenius-Morphismus:* $F : \mathbb{F}_q \to \mathbb{F}_q, a \mapsto a^p$.

Beweis. Sei $\mathbb{F}_p \subset K$ mit $m = [K : \mathbb{F}_p]$ und damit $q = p^m$.

Wir haben gesehen dass $\mathbb{F}_p = \{\alpha \in K \mid F(\alpha) = \alpha\} = \mathrm{Fix}(F)$.

Also gibt es $\tilde{m} \in \mathbb{Z}_{>0}$ sodass $F^{\tilde{m}} = Id_K$. Also ist

$$G = \{Id, F, F^2, \dots, F^{\tilde{m}-1}\} \subset \mathrm{Aut}(K)$$

Also ist $\mathrm{Fix}(G) = \mathbb{F}_p$. Mit dem Satz von Artin folgt $K/\mathrm{Fix}(G)$ ist Galois mit Gruppe G.

Also ist $K/\mathbb{F}_p$ ist Galois. $m = [K : \mathbb{F}] = \#G \Rightarrow \tilde{m} = m$.

Es gilt $F^m : K \to K = Id_k$. Also ist $x^{p^m} = x$, oder auch $x^q - x = 0, \forall x \in K$. Also gilt $X^q - X = \prod_{x \in K}(X - x)$. Insbesondere ist K isomorph zu einem Zerfällungskörper von $X^q - X$.

Umgekehrt, wenn $q = p^m$ eine Primzahlpotenz ist. Betrachte $\{x \in \overline{\mathbf{F}_p} \mid x^q = x\} = \mathrm{Fix}(F^m)$. Das ist ein Körper. Außerdem ergibt $X^q - X$ abgeleitet $qX^{q-1} - 1 = -1 \neq 0$. Also gilt $\#\,\mathrm{Fix}(F^m) = q$. □

Definition 3.48
Sei H eine Gruppe, und L ein Körper. Sei L^* die Gruppe der Einheiten in L, also $L^* = L \setminus \{0\}$.

Ein (L-wertiger) Charakter von H ist ein Gruppenmorphismus

$$H \to L^*$$

Beachte: Wenn $\sigma : K \to L$ ein Körpermorphismus ist erhalten wir einen Charakter $K^* \to L^*$ der Gruppe K^*.

Satz 3.49
Seien $\sigma_1, \dots, \sigma_n$ paarweise verschiedene Charakter eine Gruppe H mit Werten in einem Körper L. Seien $a_1, \dots, a_n \in L$ sodass die Linearkombination

$$\sum_{i=1}^{n} a_i\sigma_i : H \to L, h \mapsto \sum_{i=1}^{n} a_i\sigma_i(h)$$

die Nullabbildung ist. Dann gilt $a_1 = a_2 = \cdots = a_n = 0$.

Beweis. Induktion über n.

Fall $n = 1$: $a_1 \cdot \sigma_1(h) = 0, \sigma_1(h) \in L^* \Rightarrow a_1 = 0$

Fall $n > 1$:

$$\sum_{i=1}^{n} a_i \sigma_i(h) = 0 \qquad \forall h \in H$$

Da $\sigma_1 \neq \sigma_n$, also gibt es $g \in H$ sodass $\sigma_1(g) \neq \sigma_n(g)$.

$$\sum_{i=1}^{n} a_i \sigma_n(g) \sigma_i(h) = 0 \qquad \forall h \in H \tag{$*$}$$

$$\sum_{i=1}^{n} a_i \sigma_i(g) \sigma_i(h) = \sum_{i=1}^{n} a_i \sigma_i(gh) = 0 \qquad \forall h \in H \tag{$**$}$$

Wir betrachten die Differenz von $(*)$ und $(**)$.

$$\sum_{i=1}^{n} (a_i \sigma_i(g) \sigma_i(h) - a_i \sigma_n(g) \sigma_i(h)) = 0 \qquad \forall h \in H$$

oder

$$\sum_{i=1}^{n-1} a_i (\sigma_i(g) - \sigma_n(g)) \sigma_i(h) = 0$$

Mit der Induktionsvoraussetzung folgt für alle $i < n$ $a_i(\sigma_i(g) - \sigma_n(g)) = 0$ und da $\sigma_1(g) \neq \sigma_n(g)$ gilt $a_1 = 0$.

Also erhalten wir

$$\sum_{i=2}^{n} a_i \sigma_i(h) = 0 \qquad \forall h \in H$$

und durch Induktion $a_2 = a_3 = \cdots = a_n = 0$. $\square$

Satz 3.50 (E. Artin (wdh.))
Sei G eine endliche Untergruppe von $\mathrm{Aut}(L)$ für einen beliebigen Körper L. Schreibe $K = \mathrm{Fix}(G)$. Dann ist L/K Galois, und $G = \mathrm{Gal}(L/K)$.

Insbesondere $[L : K] = \#G$.

Beweis. Betrachte $\sigma \in G$, dann gilt für alle $a \in K, b \in L$ $\sigma(a \cdot b) = \sigma(a) \cdot \sigma(b) = a\sigma(b)$.

Also ist $\sigma \in G$ K-linear und damit $G \subset \mathrm{Gal}(L/K)$. Damit also $\#G \leq \# \mathrm{Gal}(L/K) \leq [L : K]$. Wir wollen zeigen $[L : K] \leq \#G$.

Setze $n = \#G$ und schreibe $G = \{\sigma_1, \ldots, \sigma_n\}$.

Für jedes $y \in L$ betrachte
$$S(y) = \sum_{i=1}^{n} \sigma_i(y)$$
und
$$\sigma_j(S(y)) = \sigma_j\left(\sum_{i=1}^{n} \sigma_i(y)\right) = \sum_{i=1}^{n} \sigma_j(\sigma_i(y)) = \sum_{i=1}^{n} (\sigma_j \circ \sigma_i)(y) = \sum_{\sigma \in G} \sigma(y) = S(y)$$
$\Rightarrow S(y) \in K$.

Mit der linearen Unabhängigkeit der Charaktere folgt $\exists y \in L^*, S(y) \neq 0$.

Außerdem gilt $\forall z_1, z_2 \in L : S(z_1 + z_2) = S(z_1) + S(z_2)$

und $\forall x \in K, z \in L : S(xz) = xS(z)$.

Seien $a_1, \dots, a_{n+1} \in L$ beliebig. Betrachte das Gleichungssystem
$$\sum_{k=1}^{n+1} \sigma_i^{-1}(a_k)x_k = 0 \text{ für } i = 1, \dots, n$$
Also haben wir n Gleichungen in den Variablen $x_1, x_2, \dots, x_{n+1}$. Also haben wir eine nicht-triviale Lösung $(y_1, \dots, y_{m+1}) \in L^{n+1}$. Wir können (durch umsortieren) annehmen dass $y_1 \neq 0$.

Wenn $(y_1, \dots, y_{n-1})$ eine Lösung ist und $z \in L^*$ dann ist $(zy_1, \dots, zy_{n+1})$ eine weitere Lösung.

Wir wählen $z = y/y_1$, dann könne wir annehmen dass $S(y_1) \neq 0$. Anwenden von σ_i auf die Gleichung i ergibt
$$\sum_{k=1}^{n+1} a_k \sigma_i(y_k) = 0$$
Summieren über i ergibt
$$0 = \sum_{i=1}^{n} \sum_{k=1}^{n+1} a_k \sigma_i(y_k) = \sum_{k=1}^{n+1} a_k \sum_{i=1}^{n} \sigma_i(y_k) = \sum_{k=1}^{n+1} a_k S(y_k) = \sum_{k=1}^{n+1} \underbrace{S(y_k)}_{\in K} \underbrace{a_k}_{\in L}$$
Also sind $a_1, \dots, a_{n+1} \in L$ linear abhängig über K. Also $\dim_K(L) \leq n$ und damit $[L : K] \leq \#G$. $\square$

Satz 3.51 (Hauptsatz der Galois-Theorie)
Sei L/K eine Galois-Erweiterung mit Galois-Gruppe $G = \mathrm{Gal}(L/K)$.

1) *Für jeden Zwischenkörper $K \subset Z \subset L$, ist die Gruppe $\mathrm{Gal}(L/Z)$ eine Untergruppe von G.*

   Für jede Untergruppe $H \subset G$ ist der Fixkörper $\mathrm{Fix}(H)$ ein Zwischenkörper $K \subset \mathrm{Fix}(H) \subset L$.

2) *Schreibe $\mathcal{Z}$ für die Menge der Zwischenkörper $K \subset Z \subset L$ und $\mathcal{H}$ für die Menge der Untergruppen $H \subset G$. Dann sind die Abbildungen*

$$\begin{aligned} \mathrm{Gal}(L/\_) : \mathcal{Z} &\to \mathcal{H} \\ z &\mapsto \mathrm{Gal}(L/Z) \end{aligned}$$

   und

$$\begin{aligned} \mathrm{Fix}(\_) : \mathcal{H} &\to \mathcal{Z} \\ H &\mapsto \mathrm{Fix}(H) \end{aligned}$$

   bijektiv und invers zueinander.

3) *Die Abbildungen sind umgekehrte Inklusionen und erhalten Indizes.*

   $Z_1 \subset Z_2 \Rightarrow \mathrm{Gal}(L/Z_1) \supset \mathrm{Gal}(L/Z_2)$ *und* $[Z_2 : Z_1] = [\mathrm{Gal}(L/Z_1) : \mathrm{Gal}(L/Z_2)]$.

   $H_1 \subset H_2 \Rightarrow \mathrm{Fix}(H_1) \supset \mathrm{Fix}(H_2)$ *und* $[H_2 : H_1] = [\mathrm{Fix}(H_1) : \mathrm{Fix}(H_2)]$

4) *Für jedes $\sigma \in G, Z \in \mathcal{Z}$ ist $\sigma(Z)$ ein Zwischenkörper und $\mathrm{Gal}(L/\sigma(Z)) = \sigma \circ \mathrm{Gal}(L/Z) \circ \sigma^{-1} = \{\sigma\tau\sigma^{-1} \mid \tau \in \mathrm{Gal}(L/K)\} \subseteq \mathrm{Gal}(L/K)$.*

5) *Für $Z \in \mathcal{Z}$ ist Z/K Galois genau dann wenn $G(L/Z) \subset G$ eine normale Untergruppe ist, in anderen Worten wenn $\sigma \circ \mathrm{Gal}(L/Z) \circ \sigma^{-1} = \mathrm{Gal}(L/Z)$ für alle $\sigma \in G$.*

   In dem Fall gilt
$$\mathrm{Gal}(Z/K) = \mathrm{Gal}(L/K)/\,\mathrm{Gal}(L/Z)$$

Bemerkung: Sei G eine endliche Gruppe, Sei $H \subseteq G$ eine Untergruppe. Dann gilt $\#H \mid \#G$. Den Quotienten bezeichnet man als Grad der Gruppenerweiterung $[G : H]$.

Beispielanwendung: Sei $k = \mathbb{Q}$, sei L der Zerfällungskörper von $x^3 - 2$.

Erinnerung: Wir wissen: $L = \mathbb{Q}(\underbrace{\sqrt[3]{2}}_{a_1}, \underbrace{\xi\sqrt[3]{2}}_{a_2}, \underbrace{\xi^2\sqrt[3]{2}}_{a_3})$ wobei $\xi = e^{\frac{2\pi i}{3}}$.

Wir wissen auch $[L : \mathbb{Q}] = 6$

Zudem wissen wir $L = \mathbb{Q}(\sqrt[3]{2}, i \cdot \sqrt[2]{3})$

Frage: Welche Zwischenkörper gibt es? Welche sind Galois?

Gegenfrage: Was ist $\mathrm{Gal}(L/K)$?

Antwort: Jedes Element von $\mathrm{Gal}(L/K)$ permutiert $\{a_1, a_2, a_3\}$ erhalte also Abbildung:

$$\mathrm{Gal}(L/K) \overset{\alpha}{\to} \mathrm{Perm}(\{a_1, a_2, a_3\}) = S_3$$

Wissen auch: die Elemente von $\mathrm{Gal}(L/K)$ sind durch die Permutation eindeutig bestimmt. Also ist α injektiv.

Wissen auch: L/K ist Galois, also

$$6 = [L : k] = \# \mathrm{Gal}(L/K) = \# S_3$$

α ist also bijektiv.

Wie viele Elemente hat S_3? Wie sehen die aus?

$$\{Id, (123), (12)(3), (13)(2), (23)(1), (132)\} = S_3$$

Untergruppen sind

$$\{Id\}$$
$$\{Id, (12)(3)\}, \{Id, (13)(2)\}, \{(23)(1)\}$$
$$\{Id, (123), (132)\}$$
$$S_3$$

Wir sehen die normalen Untergruppen sind exakt $\{Id\}, \{Id, (123), (132)\}, S_3$.

Welche Körpererweiterungen gibt es also?

$\mathrm{Fix}(Id) = L$

$\mathrm{Fix}(Id, (12)(3) = k(a_3)$

Denn: Klar ist, dass Elemente von k und a_3 fix sind, also $k(a_3) \subseteq \mathrm{Fix}(Id, (12)(3))$. Wende 3) an mit $H_2 = S_3, H_1 = (Id, (12)(3))$ also

$$\Rightarrow [\mathrm{Fix}(H_1) : \mathrm{Fix}(H2)] = [H_2 : H_1] = 3$$

Aber $[k(a_3), k] = 3$ also Gleichheit.

Außerdem

$\mathrm{Fix}(Id,(13)(2)) = k(a_2)$ und $\mathrm{Fix}(Id,(23)(1)) = k(a_1)$ sind nicht Galois.

$\mathrm{Fix}(S_3) = k$

$\mathrm{Fix}(Id,(123),(132)) = k(i \cdot \sqrt[2]{3})$. Warum ist $i \cdot \sqrt[2]{3}$ überhaupt invariant? Wir wissen

$$i \cdot \sqrt[2]{3} = \frac{a_2 - a_3}{a_1} = \frac{\xi\sqrt[3]{2} - \xi^2\sqrt[3]{2}}{\sqrt[3]{2}} = \xi - \xi^2$$

aber

$$\frac{a_3 - a_1}{a_2} = \frac{\xi^2\sqrt[2]{3} - \sqrt[2]{3}}{\xi\sqrt[2]{3}} = \xi - \overline{\xi} = \xi - \xi^2$$

Beweis des Hauptsatzes. 1) ist bereits bewiesen

2) Wir müssen zeigen: Für jeden Zwischenkörper Z ist $\mathrm{Fix}(\mathrm{Gal}(L/Z)) = Z$

Und für jede Untergruppe H ist

$$\mathrm{Gal}(L/\,\mathrm{Fix}(H)) = H$$

Letztere Aussage ist Satz von Artin, also fertig.

Sei Z gegeben. Klar per Definition $\mathrm{Fix}(\mathrm{Gal}(L/Z)) \supseteq Z$. Will Gleichheit zeigen mit Hilfe des Gradargumentes.

Artin $L/\,\mathrm{Fix}(\mathrm{Gal}(L/Z))$ ist Galois'sch, $[L : \mathrm{Fix}(\mathrm{Gal}(L/Z))] = \#\,\mathrm{Gal}(L/Z)$

Wir L/Z ist auch Galois'sch, also $[L : Z] = \#\,\mathrm{Gal}(L/Z)$.

Also: $[\mathrm{Fix}(\mathrm{Gal}(L/Z)) : Z] = 1$

3) Wir beweisen nur die zweite Aussage. Seien also Gruppen $H_1 \subseteq H_2 \subseteq \mathrm{Gal}(L/K)$ gegeben. Klar ist: jedes $l \in L$, das fix ist unter H_2 ist auch fix unter $H_1 \Rightarrow \mathrm{Fix}(H_2) \subseteq \mathrm{Fix}(H_1)$ Inklusionsumkehr ist also bewiesen.

Artin $[L : \mathrm{Fix}(H_1)] = \#H_1$ und $[L : \mathrm{Fix}(H_2)] = \#H_2$

$$\Rightarrow [\mathrm{Fix}(H_1) : \mathrm{Fix}(H_2)] = \frac{[L : \mathrm{Fix}(H_2)]}{[L : \mathrm{Fix}(H_1)]} = \frac{\#H_2}{\#H_1} = [H_2 : H_1]$$

4) Sei σ und Z gegeben. Klar ist $\sigma(Z)$ ist ein Zwischenkörper. Behaupte

$$\mathrm{Gal}(L/\sigma(Z)) \supseteq \sigma\,\mathrm{Gal}(L/Z)\sigma^{-1} \tag{$*$}$$

Beweis der Behauptung: Sei $\tau \in \sigma\,\mathrm{Gal}(L/Z)\sigma^{-1}$ und sei $z \in \sigma(Z)$. Muss zeigen, dass $\tau(z) = z$ ist. Schreibe dazu $\tau = \sigma\tau'\sigma^{-1}$ und $z = \sigma(z')$ für geeignete $\tau \in \mathrm{Gal}(L/Z), z' \in Z$. Dann ist

$$\tau(z) = \sigma\tau\sigma^{-1}\sigma(z') = \sigma\tau' z' = \sigma(z') = z$$

Noch zu zeigen: Wir haben Gleichheit in $(*)$

Beobachte: Die Gruppen $\mathrm{Gal}(L/Z)$ und $\sigma\,\mathrm{Gal}(L/Z)\sigma^{-1}$ sind isomorph, haben also gleich viele Elemente.

Isomorphie ist

$$\begin{aligned} \mathrm{Gal}(L/Z) &\to \sigma\,\mathrm{Gal}(L/Z)\sigma^{-1} \\ \tau &\mapsto \sigma\tau\sigma^{-1} \end{aligned}$$

Beobachtung: L/Z ist Galois'sch

$$\#\,\mathrm{Gal}(L/Z) = [L : Z] = [\sigma(L) : \sigma(Z)] = [L : \sigma(Z)] = \#\,\mathrm{Gal}(L/\sigma(Z))$$

Insgesamt: Die beiden Gruppen in $(*)$ haben gleich viele Elemente!

5) Sei Z ein Zwischenkörper.

Beobachtung 1: Z/K ist separabel. Also: Z/K ist Galois'sch $\Leftrightarrow$ Z/K ist normal $\Leftrightarrow$ für jede k-Morphismus $\sigma : Z \to \overline{L}$ ist $\sigma(Z) = Z$.

Beobachtung 2: Jeder Morphismus $\sigma : Z \to \overline{L}$ setzt sich fort zu Morphismus $\overline{\sigma} : L \to \overline{L}$. Weil L/K per Annahme Galois'sch, also normal ist, gilt: $\overline{sigma}(L) = L$.

Zusammenfassung: Z/K ist Galois'sch $\Leftrightarrow \forall\sigma \in \mathrm{Gal}(L/K)\sigma(Z) = Z$.

$\overset{2)}{\Rightarrow} \forall\sigma \in \mathrm{Gal}(L/K) : \mathrm{Gal}(L/\sigma(Z)) = \mathrm{Gal}(L/Z)$

$\overset{4)}{\Rightarrow} \forall\sigma \in \mathrm{Gal}(L/K) : \sigma\,\mathrm{Gal}(L/Z)\sigma^{-1} = \mathrm{Gal}(L/Z)$

$\Leftrightarrow \mathrm{Gal}(L/Z)$ ist normale Untergruppe von $\mathrm{Gal}(L/K)$

Falls Z/K Galois'sch ist, haben wir Einschränkung

$$r : \mathrm{Gal}(L/K) \to \mathrm{Gal}(Z/K)$$

die Abbildung r ist surjektiv, weil wir Morphismen fortsetzen können. $\ker(r) = \mathrm{Gal}(L/Z)$.

$\square$

4 Gruppentheorie

4.1 Grundbegriffe

Definition 4.1
Sei G eine Gruppe, M eine Menge. Eine Gruppenwirkung ist eine Abbildung

$$\alpha : G \times M \to M$$

sodass

1) $\forall m \in M : \ \alpha(e, m) = m$

2) $\forall m \in M, \forall g, h \in G \ \alpha(h, \alpha(g, m)) = \alpha(h \cdot g, m)$

Bemerkung: Gegeben eine Gruppenwirkung $\alpha : G \times M \to M$ und $g \in G$ betrachte oft die Abbildung

$$\begin{aligned} \alpha_g : M &\longrightarrow M \\ m &\longmapsto \alpha(g, m) \end{aligned}$$

(Translation). Die Axiome 1) und 2) sagen:

$$\alpha_e = id_M, \forall g, h : \alpha_h \circ \alpha_g = \alpha_{h \cdot g}$$

Insbesondere: Alle α_g sind bijektiv, $(\alpha_g)^{-1} = \alpha_{g^{-1}}$.

Insbesondere: erhalte Gruppenmorphismus

$$\begin{aligned} \underbrace{\alpha} : G &\longrightarrow \mathrm{Perm}(M) \\ g &\longmapsto \alpha_g \end{aligned}$$

Andersherum: Gegeben Gruppenmorphismus

$$\underline{\beta} : G \to \mathrm{Perm}(M)$$

dann liefert

$$\begin{aligned} \beta : G \times M &\longrightarrow M \\ (g, m) &\longmapsto (\underline{\beta}(g))(m) \end{aligned}$$

eine Gruppenwirkung.

Beispiel 4.2

- *k ein Körper. Dann wirkt $\mathrm{Gl}_n(k)$ auf k^n*
- *$(\mathbb{R}, +)$ wirkt auf $\mathbb{R}$.*

$$\begin{aligned} a : \mathbb{R} \times \mathbb{R} &\longrightarrow \mathbb{R} \\ (a, b) &\longmapsto a + b \end{aligned}$$

$$\begin{aligned} m : \mathbb{R} \times \mathbb{R} &\longrightarrow \mathbb{R} \\ (a, b) &\longmapsto \exp(a)b \end{aligned}$$

- *k ein Körper, f ein Polynom mit Zerfällungskörper L. Sei $G = \mathrm{Gal}(L/K)$. Dann haben wir natürliche Wirkungen*
  - *G wirkt auf L*
  - *G wirkt auf die Nullstellenmenge von f*
  - *G wirkt auf die Menge der Zwischenkörper $k \subseteq \cdot \subseteq L$*
- *Sei G eine Gruppe. Dann wirkt G auf sich selbst $(M = G)$*

$$\begin{aligned} l : G \times G &\longrightarrow G \\ (g, m) &\longmapsto g \cdot m \\ r : G \times G &\longrightarrow G \\ (g, m) &\longmapsto m \cdot g^{-1} \\ c : G \times G &\longrightarrow G \\ (g, m) &\longmapsto g \cdot m \cdot g^{-1} \end{aligned}$$

- *Variante: Sei $H \subseteq G$ eine Untergruppe. Dann:*

$$\begin{aligned} l : H \times G \to G \quad & (h, m) \mapsto hm \\ r : H \times G \to G \quad & (h, m) \mapsto mh^{-1} \\ c : H \times G \to G \quad & (h, m) \mapsto hmh^{-1} \end{aligned}$$

- *Sei ODE auf M gegeben, sodass Anfangswertprobleme für alle Zeilen lösbar sind. Dann ist die Lösungsabbildung*

$$\begin{aligned} \mathbb{R} \times M &\longrightarrow M \\ (t, m) &\longmapsto \text{Lösung des AWP zum Wert } m \text{ und Zeit } t \end{aligned}$$

  Wirkung von $\mathbb{R}$ auf M.

Definition 4.3
Sei $\alpha : G \times M \to M$ eine Gruppenwirkung.

1) Wir schreiben statt $\alpha(g, m)$ oft $g \cdot m$.

2) Gegeben $m \in M$. Dann betrachte alle Elemente, die wir von m erreichen können

$$G \cdot m = \{g \cdot m \mid g \in G\}$$

Dies heißt die Bahn von m.

3) Gegeben Teilmenge $N \subseteq M$, betrachte Untergruppen

$$\mathrm{Fix}(N) = \{g \in G \mid \forall n \in N : g \cdot n = n\}$$

$$\mathrm{Stab}(N) = \{g \in G \mid g \cdot N = N\}$$

Spezialfall: $m \in M$ gegeben. Dann nenne $\mathrm{Fix}(\{m\})$ die Isotropiegruppe von m.

4) Ein Element $m \in M$ sodass $\forall g \in G : g \cdot m = m$ heißt Fixpunkt der Gruppenwirkung.

5) Eine Gruppenwirkung heißt transitiv, falls es nur eine Bahn gibt.

Zentrale Beobachtung: Sei $\alpha : G \times M \to M$ eine Gruppenwirkung, seien $m_1, m_2 \in M$ gegeben. Betrachte Bahnen $G \cdot m_1$ und $G \cdot m_2$. Falls die Bahnen einen Schnittpunkt haben, sind sie gleich!

Beweis. Sei m_3 ein Schnittpunkt. Das heißt finde $g_1, g_2 \in G : m_3 = g_1 \cdot m_1 = g_2 \cdot m_2$.

Sei $n \in Gm_1$ jetzt irgendein Element, also $n = h \cdot m_1$, dann $n = hg_1^{-1}g_2m_2$ also $n \in G \cdot m_2$.

$\Rightarrow G \cdot m_1 \subseteq G \cdot m_2$. Andere Inklusion analog! □

Die Relation auf M

$$a \sim b \Leftrightarrow \exists g \in G : a = g \cdot b \Leftrightarrow \text{Bahnen von } a \text{ und } b \text{ sind gleich}$$

ist eine Äquivalenzrelation! Die Gruppenwirkung zerlegt den Raum in eine disjunkte Vereinigung von Bahnen.

Besonders relevanter Fall: Sei G eine Gruppe, $H \subseteq G$ eine Untergruppe, Wirkung: l. Die Bahnen heißen Rechtsnebenklassen. Die Anzahl der Bahnen wird mit $[G : H]$ bezeichnet und heißt Index von H in G.

Satz 4.4
Sei G eine endliche Gruppe, die auf M wirkt. Sei $m \in M$ gegeben. Dann ist

$$\#G = \#\operatorname{Iso}(m) \cdot \#(G \cdot m)$$

Beweis. Betrachte Bahnabbildung

$$\begin{aligned} b : G &\longrightarrow M \\ g &\longmapsto g \cdot m \end{aligned}$$

Bild der Bahnabbildung ist die Bahn $G \cdot m$. Was sind die Fasern?

$$b^{-1}(m) = \{g \in G \mid g \cdot m = m\} = \operatorname{Iso}(m)$$

Gegeben $h \in G$

$$b^{-1}(h \cdot m) = \{g \in G \mid g \cdot m = h \cdot m\} = h^{-1} \cdot \operatorname{Iso}(m)$$

Also alle Urbildmengen enthalten stets $\#\operatorname{Iso}(m)$ Elemente. Es gibt exakt $\#(G \cdot m)$ Urbildmengen.

$\Rightarrow$ hat $\#\operatorname{Iso}(m) \cdot \#(G \cdot m)$ viele Elemente. $\square$

<u>Anwendung auf Spezialfall:</u> $H \subseteq G$ wirkt auf $M = G$ durch Linksmultiplikation.

Satz 4.5 (Kleiner Satz von Lagrange)
Sei G eine endliche Gruppe, sei $H \subseteq G$ eine Untergruppe. Dann $\#G = [G : H] \cdot \#H$.

Beweis. Die Menge G ist disjunkte Vereinigung von $[G : H]$ vielen Bahnen. Müssen also zeigen: alle Bahnen enthalten exakt $\#H$ viele Elemente. Wegen Satz 4.4 genügt es zu zeigen $\forall g \in G : \operatorname{Iso}(g) = \{e\}$.

Erinnerung: $\operatorname{Iso}(g) = \{h \in H \mid h \cdot g = g\}$ $\square$

Folgerung 4.6
$[G : H] = \#G/\#H$. *Insbesondere ist* $[G : H]$ *Teiler von* $\#G$. *Insbesondere ist* $\#H$ *Teiler von* $\#G$.

Folgerung 4.7
Sei G endlich. G wirke auf Menge M. Sei $m \in M$ dann $\#(G \cdot m) = [G : \operatorname{Iso}(m)]$.

Wesentliches weiteres Beispiel

G wirkt auf sich selbst durch Konjugation. Die Bahnen heißen Konjugationsklassen. Gegeben Untergruppe $H \subseteq G$, betrachte $\mathrm{Fix}(H) = \{g \in G \mid ghg^{-1} = h, \forall h \in H\} = Z(H) \subseteq G$ diese Untergruppe heißt Zentralisator von H.

$\mathrm{Stab}(H) = \{g \in G \mid gHg^{-1} = H\} \subseteq G$

Beobachtung: $H \subseteq \mathrm{Stab}(H)$ ist normale Untergruppe.

Klassengleichung: Die Gruppe G zerlegt sich in Konjugationsklassen. Wenn wir aus jeder Klassen einen Vertreter wählen $h_1, \ldots, h_n \in G$. Dann

$$\#G = \sum_{i=1}^{n} H \cdot h_i = \sum_{i=1}^{n} [G : Z(h_i)] = \#Z(H) + \sum_{\substack{i=1\ldots n \\ h_i \notin Z(H)}} [G : Z(h_i)]$$

4.2 Zyklische Gruppen

Gegeben sei eine Gruppe G und ein Element $g \in G$. Dann gibt es einen Gruppenmorphismus

$$\begin{aligned} \varphi_g : \mathbb{Z} &\longrightarrow G \\ n &\longmapsto \begin{cases} g^n & \text{falls } n > 0 \\ e & \text{falls } n = 0 \\ (g^{-1})^n & \text{falls } n < 0 \end{cases} \end{aligned}$$

Bild ist eine Untergruppe von G, genannt $\langle g \rangle$ die von g erzeugte Zyklische Untergruppe.

- Falls φ_g injektiv ist, dann ist $\langle g \rangle$ isomorph zu $\mathbb{Z}$.

- Falls φ_g nicht injektiv ist, beachte $\ker(\varphi_g)$ enthält positive Zahlen. Sei also $n = \min(\ker(\varphi_g) \cap \mathbb{N})$. Wie immer ist

$$\langle g \rangle \simeq (\mathbb{Z}/(n), +)$$

Beispiel 4.8
Sei G eine endliche Gruppe. Sei $\#G = p$ eine Primzahl. Sei $g \in G$ gegeben. Dann ist $\langle g \rangle \subseteq G$ also: $\#\langle g \rangle \mid \#G$.

$\Rightarrow$ *entweder $\langle g \rangle = \{e\}$ oder $\langle g \rangle = G$.*

Konsequenz:

1) *G hat überhaupt keine echten Untergruppen.*

2) *G ist zyklisch.*

Definition 4.9
Sei G eine Gruppe und $g \in G$, definiere:

$$\mathrm{ord}(g) = \min\{n \in \mathbb{N} : g^n = e\} \in \mathbb{N} \cup \{\infty\}$$

$\mathrm{ord}(g) = \#\langle g \rangle$, *falls endlich ist* $\mathrm{ord}(g) \mid \#G$

Beispiel 4.10 1) *Falls $\#G$ eine Primzahl ist, dann ist G zyklisch.*

2) *Gegeben $n \in \mathbb{N}$ betrachte $G = \{\xi \in \mathbb{C} \mid \xi^n = 1\}$.*

3) *Sei R ein Integritätsring, sei $G \subset (R^*, \cdot)$ endlich. Dann ist G zyklisch.*

   Beweis. Weil $R \hookrightarrow Q(R)$ eingebettet ist, können wir ohne Einschränkung annehmen. $R = k$ ist ein Körper. Sei $m = \max\{\mathrm{ord}(h) \mid h \in G\}$. Dann gilt $\forall g \in G$

$$g^m = \underbrace{\left(g^{\mathrm{ord}(g)}\right)}_{=e}{}^{m/\mathrm{ord}(g)} = e$$

   Also: alle $g \in G$ sind Nullstellen des Polynoms $x^m - 1$. Dieses Polynom hat maximal m Nullstellen $\Rightarrow \#G \leq m$. Wenn wir $g \in G$ nehmen, mit $\mathrm{ord}(g) = m$, dann ist $\#(g) = m$. Insbesondere $G = (g)$, G ist zyklisch. □

4.3 Die Sätze von Sylow

Frage: Wenn G endliche Gruppe ist, $H \subseteq G$ eine Untergruppe, dann $\#H \mid \#G$. Wenn wir $n \in \mathbb{N}$ haben, mit $n \mid \#G$, gibt es dann auch eine Untergruppe H mit $\#H = n$?

Sylow-Sätze geben Teilantwort. Die Zentrale Beobachtung ist einfach!

Lemma 4.11
Sei G eine Gruppe, sei $\#G = p^n$ für p Primzahl, $n \in \mathbb{N}$. G wirke auf endliche Menge M. Setze $M_0 = \mathrm{Fix}(G)$. Dann ist $\#M \equiv \#M_0 \mod p$.

Beweis. M ist disjunkte Vereinigung der Bahnen. Bahnen mit einem Element sind exakt die Fixpunkte. Wenn B eine Bahn mit mehr als einem Element ist, dann $1 < \#B \mid p^n$ $\Rightarrow \#B \equiv 0 \mod p$. □

Satz 4.12 (Satz von Cauchy)
Sei G endliche Gruppe und sei p eine Primzahl sodass $p \mid \#G$. Dann gibt es ein $g \in G$: $\operatorname{ord}(g) = p$.

Beweis. Betrachte $(\mathbb{Z}/p\mathbb{Z}, +)$. Diese Gruppe wirkt auf $\underbrace{G \times \cdots \times G}_{p-\text{mal}}$ durch zyklische Vertauschung:

$$1 : (g_1, \ldots, g_p) \mapsto (g_p, g_1, \ldots, g_{p-1})$$

Beobachte: Die Menge $M = \{(g_1, \ldots, g_p) \in G^p \mid g_1 \cdot \cdots \cdot g_p = e\}$ ist stabil unter der Wirkung von $\mathbb{Z}/p\mathbb{Z}$.

Beobachte: $\#M = (\#G)^{p-1}$

Beobachte: Fixpunkte der $\mathbb{Z}/p\mathbb{Z}$-Wirkung auf M sind Elemente der Form $\underbrace{(g, \cdots, g)}_{p-\text{mal}}$ mit $g^p = e$.

$\Rightarrow g = e$ oder $\operatorname{ord}(g) = p$.

Wir wissen:

1) $\#\operatorname{Fix}(\mathbb{Z}/p\mathbb{Z}) \geq 1$, denn $(e \ldots e) \in \operatorname{Fix}(\ldots)$

2) Lemma: $\#\operatorname{Fix}(\mathbb{Z}/p\mathbb{Z}) \equiv 0 \mod p$

$\Rightarrow \#Fix(\mathbb{Z}/p\mathbb{Z}) \geq p$. Also existiert ein Element der Ordnung p. □

Definition 4.13
Sei p eine Primzahl. Eine Gruppe heißt p-Gruppe, wenn $\forall g \in G \exists n \in \mathbb{N} : \operatorname{ord}(g) = p^n$.

Satz 4.14
Sei G eine endliche Gruppe, sei p eine Primzahl. Dann sind äquivalent:

1) G ist p-Gruppe

2) $\#G = p^m$ für geeignetes $m \in \mathbb{N}$

Beweis. $\underline{2) \Rightarrow 1)}$ Klar, denn wir wissen:

$$\forall g \in G : \operatorname{ord}(g) \mid \#G = p^m$$

$\Rightarrow \operatorname{ord}(g)$ ist Potenz von p

1) $\Rightarrow$ 2) Beweis der Kontraposition!

Angenommen $\#G$ ist keine Potenz von p.

$\Rightarrow$ Es gibt Primzahl $q \neq p$ mit $q \mid \#G$.

Cauchy: Es gibt ein Element $g \in G$ mit $\operatorname{ord}(g) = q$.

$\Rightarrow G$ ist keine p-Gruppe. $\square$

Lemma 4.15
Sei G eine endliche p-Gruppe. Dann: G hat nicht triviales Zentrum

$$Z(G) \supsetneq \{e\}$$

Beweis. Betrachte die Wirkung von G auf $M = G$ durch Konjugation. Dann $Z(G) = \operatorname{Fix}(G)$.

Wieder gilt: $\{e\} \subseteq \operatorname{Fix}(G)$

$\# \operatorname{Fix}(G) \equiv 0 \mod p \Rightarrow \# \operatorname{Fix}(G) \geq p$. $\square$

Definition 4.16
Sei G eine Gruppe, p eine Primzahl. Eine p-Sylowgruppe ist eine maximal große p-Untergruppe von G.

Satz 4.17 (ohne Beweis)
Mit Zorns Lemma existieren Sylowgruppen.

Lemma 4.18
Sei G eine Gruppe, sei $G_p \subseteq G$ eine p-Sylowgruppe, sei $g \in G$ ein Element $\Rightarrow gG_pg^{-1}$ ist eine Sylowgruppe.

Beweis. Klar ist $\#G_p = \#gG_pg^{-1}$ also ist gG_pg^{-1} schon mal eine p-Gruppe. Angenommen gG_pg^{-1} wäre nicht maximal, das heißt p-Gruppe U mit $gG_pg^{-1} \subsetneq U \Rightarrow G_p \subsetneq g^{-1}Ug$ und $g^{-1}Ug \simeq U$ also p-Gruppe.

$\Rightarrow G_p$ nicht Sylow! $\square$

Lemma 4.19
Sei G endlich, sei $U \subseteq G$ eine p-Untergruppe dann gilt:

$$[G : U] = [N(U) : U] \mod p$$

(Erinnerung: $N(U) = \{g \in G \mid gUg^{-1} = U\}$. Das ist eine Untergruppe von G und U ist normal in $N(U)$)

Beweis. Betrachte die Wirkung von U auf G durch Linkstranslation. Sei $M =$ Quot. Anders gesagt $M =$ Menge der Bahnen also

$$M = \{U \cdot g \mid g \in G\}$$

Nachrechnen: U wirkt auf der Menge M durch:

$$\begin{aligned} U \times M &\longrightarrow M \\ (u, U \cdot g) &\longmapsto U \cdot g \cdot u^{-1} \end{aligned}$$

Betrachte wieder $M_0 \subseteq M$, die Fixpunktmenge dieser Wirkung.

Beobachte:

$$\begin{aligned} Z \cdot g \in M_0 &\Leftrightarrow \forall u \in U : U \cdot g \cdot u^{-1} = Ug \\ &\Leftrightarrow \forall u \in U : Ugu^{-1}g^{-1} = U \Leftrightarrow g \in N(U) \end{aligned}$$

Wir wissen:

$$[G : U] = \#M = \#M_0 \mod p$$

wobei $\#M_0 = \#$Bahnen der Wirkung von U auf Gruppe $N(U) = [N(U) : U]$ $\square$

<u>Zusatz:</u> Falls gilt $p \mid [G : U]$, dann $[N(U) : U] = 0 \mod p$

$\Rightarrow [N(U) : U] \neq 1 \Rightarrow N(U) \subsetneq U$

Satz 4.20 (Sylow-Satz 1)
Sei G eine endliche Gruppe, sei p eine Primzahl. Schreibe $\#G = p^n \cdot m$ wobei $p \nmid m$. Dann gilt:

1) *$\forall 0 \leq i \leq n$ gilt: Es existiert eine p-Untergruppe von G mit p^i-Elementen.*

2) *$\forall 0 \leq i < n$ und alle p-Untergruppen $U \subseteq G$ mit p^i Elementen: Es gibt eine p-Untergruppe $U' \subseteq G$ mit p^{i+1} Elementen. $U \subseteq U'$ und U ist normal in U'.*

Beweis. Banal: $\{e\}$ hat p^0 Elemente

Cauchy: Es existiert eine Untergruppe mit p Elementen. Per Induktion genügt es also Teil 2) zu zeigen.

Sei also $0 \leq i < n$ gegeben, sei U mit p^i Elementen gegeben. Wissen dann (Lemma und Zusatz) $N(U) \supsetneq U$. Weil U normal ist in $N(U)$ können wir Quotientengruppe betrachten!

$$\pi : N(U) \longrightarrow N(U)/U$$

Lemma: $[N(U) : U] = [G : U] \equiv 0 \mod p$

$\Rightarrow \#N(U)/U \equiv 0 \mod p$

$\Rightarrow p \mid \#N(U)/U$

Cauchy: Finde in $N(U)/U$ eine Untergruppe $\underline{U}' \subseteq N(U)/U$ von Ordnung $\#\underline{U}' = p$. Setze $U' := \pi^{-1}(\underline{U}')$. Diese Gruppe hat dann p^{i+1} viele Elemente und $U' \subseteq N(U)$, also $U \subseteq U'$ normal. □

Satz 4.21 (Sylow-Satz 2)
Sei G eine endliche Gruppe: Zu jeder p-Untergruppe $H \subseteq G$ und jeder p-Sylowgruppe $P \subseteq G$ gibt es $g \in G : gHg^{-1} \subseteq P$.

Insbesondere: je zwei p-Sylowgruppen sind zueinander konjugiert!

Beweis. H wirkt auf die Menge $G/P =: M$.

$\#G = p^n \cdot m$ wobei $p \nmid m$ und $\#P = p^n$

$\Rightarrow \#M = m \not\equiv 0 \mod p$

Mit Lemma 4.11 folgt $M_0 \neq \emptyset$.

Also gibt es $g \in G$ sodass $gP \in G/P$ Fixpunkt von H ist.

Für alle $h \in H$ gilt $h \cdot g \cdot P = g \cdot P$.

$\Rightarrow g^{-1}hg \cdot P = P \forall h \in H$.

$\forall h \in H : g^{-1}hg \in P \Rightarrow g^{-1}Hg \subset P$ □

Satz 4.22 (Sylow-Satz 3)
Sei G eine endliche Gruppe $s_p = \#p$-Sylowgruppen

$\Rightarrow s_p \mid \#G$ und $s_p \equiv 1 \mod p$

Beweis. Betrachte die Wirkung von G auf subgrp$(G) = \{H \subset G \mid H \text{ Untergruppe}\}$ durch Konjugation: $(g, H) \mapsto g^{-1}Hg$.

Alle p-Sylow Untergruppen bilden eine Bahn mit Länge s_p.

Die Länge einer Bahn teilt $\#G$, also teilt s_p $\#G$.

Sei $P \subset G$ eine p-Sylow Untergruppe. P wirkt durch Konjugation auf die Menge der p-Sylow Untergruppen.

Die Fixpunkte dieser Wirkung sind

$$M_0 = \{Q \mid g^{-1}Qg = Q \; \forall g \in P\}$$

oder auch $Q \in M_0 \Leftrightarrow P \subset N(Q) = \{g \in G \mid g^{-1}Qg = Q\} \subseteq G$

Beobachte: P und Q sind p-Sylow Untergruppen von $N(Q)$.

Nach Sylow-Satz 2 sind beide zueinander konjugiert: Es gibt also $h \in N(Q)$ sodass $P = h^{-1}Qh = Q$. $\Rightarrow M_0 = \{P\}$. Mit Lemma 4.11 folgt $s_p \equiv \#M_0 = 1 \mod p$. □

4.4 Abelsche Gruppen

Sei G eine abelsche Gruppe. Für $n \in \mathbb{N}$ und $g \in G$ schreibe $n \cdot g = \underbrace{g + \cdots + g}_{n\text{-mal}}$ und $(-n) \cdot a = -(n \cdot a)$.

Beachte: Für $n \in \mathbb{Z}$, und $g, h \in G$ gilt $n(a + b) = na + nb$.

Definition 4.23
Eine abelsche Gruppe G ist endlich erzeugt, falls es eine endliche Liste von Elementen $g_1, \ldots, g_n \in G$ gibt, sodass jedes $g \in G$ als Linearkombination geschrieben werden kann.

$$g = \sum_{i=1}^{n} n_i g_i, \quad n_i \in \mathbb{Z}$$

Definition 4.24
Ein Erzeugendensystem $\{g_1, \ldots, g_n\}$ heißt Basis falls gilt

$$0 = \sum_{i=1}^{n} n_i g_i \Rightarrow n_i = 0 \; \forall i$$

Wenn G eine Basis hat, heißt G frei.

Lemma 4.25
Wenn G frei ist, haben je zwei Basen dieselbe Länge. Die Länge heißt dann Rang von G.

Satz 4.26
Sei G eine endlich erzeugte abelsche Gruppe. Dann gibt es $r \in \mathbb{Z}_{\geq 0}$ und $a_1, \dots, a_n \in \mathbb{Z}_{>0}$ mit $a_i \mid a_{i+1}$ $\forall i \in \{1, \dots, n-1\}$ sodass

$$G \cong \mathbb{Z}^r \oplus \mathbb{Z}/(a_1) \oplus \cdots \oplus \mathbb{Z}/(a_n)$$

$r, a_1, \dots, a_n$ sind durch G eindeutig bestimmt.

Bemerkung: 1) Wir nennen r den Rang von G und $a_1, \dots, a_n$ die Elementarteiler von G.

2) Die Summe $\mathbb{Z}/(a_1) \oplus \cdots \oplus \mathbb{Z}/(a_n)$ ist der Torsionsanteil von G und $\mathbb{Z}^r$ der freie Anteil von G.

3) Der Torsionsteil ist eindeutig bestimmte Untergruppe von G und ist $\operatorname{Tors}(G) = \{g \in G \mid \operatorname{ord}(g) < \infty\}$.

4) Der freie Anteil von G ist nicht notwendigerweise eindeutig bestimmt als Untergruppe, aber es gilt $\mathbb{Z}^r \cong G/\operatorname{Tors}(G)$

4.5 Auflösbare Gruppen

Sei G eine Gruppe. Wir versuchen G zu verstehen.

Finde eine normale Untergruppe $N \subset G, i \neq N \neq G$. Wir betrachten N und G/N.

Definition 4.27
Eine Gruppe G heißt auflösbar, wenn es eine endliche Kette

$$G = N_k \supset N_{k-1} \supset N_{k-2} \supset \cdots \supset N_1 \supset N_0 = \{e\}$$

gibt, sodass N_i normal in N_{i+1} ist und dass N_{i+1}/N_i abelsch ist für alle i.

Satz 4.28
Jede endliche p-Gruppe ist auflösbar.

Beweis. Sei G eine endliche p-Gruppe. Angenommen $G \neq \{e\}$. Dann ist $Z(G)$ ebenso nicht trivial.

Betrachte jetzt $G/Z(G)$ und beweise durch Induktion wie folgt:

Nehme an wir haben eine Auflösungskette

$$G/Z(G) = \tilde{N}_k \supset \tilde{N}_{k-1} \supset \cdots \supset \tilde{N}_1 \supset \tilde{N}_0 = \{e\}$$

Sei $\varphi : G \to G/Z(G)$ die Quotientenabbildung und setze $N_i = \varphi^{-1}(\tilde{N}_i)$. Damit erhalten wir die Kette

$$G = N_k \supset N_{k-1} \supset \cdots \supset N_1 \supset N_0 = Z(G) \subset N_{-1} = \{e\}$$

$\ker(q_i) = N_i \subset \underbrace{N_{i+1} \twoheadrightarrow \tilde{N}_{i+1} \twoheadrightarrow \tilde{N}_{i+1}/\tilde{N}_i}_{q_i}$

$\Rightarrow N_i \subset N_{i+1}$ ist normal

$\Rightarrow N_{i+1}/N_i \cong \tilde{N}_{i+1}/\tilde{N}_i$ ist abelsch □

Satz 4.29
Sei G eine endliche auflösbare Gruppe. Dann ist jede Untergruppe und jeder Quotient auflösbar.

Satz 4.30
Sei G eine auflösbare Gruppe, and sei $N \subset G$ eine normale Untergruppe.

Dann gibt es eine Auflösungskette

$$\{e\} \subset N_1 \subset \cdots \subset N_k \subset G$$

sodass

1) $N \in \{\{e\}, N_1, \ldots, N_k, G\}$

2) N_{i+1}/N_i *ist zyklisch mit primer Ordnung*

Beweis. 1) Sei $\{e\} \subset \tilde{N}_1 \subset \tilde{N}_2 \subset \cdots \subset \tilde{N}_l = N$ eine Auflösungskette für N.

Sei $N/N = \tilde{N}_l \subset \tilde{N}_{l+1} \subset \cdots \subset \tilde{N}_k = G/N$ eine Auflösungskette für G/N. Sei $q : G \to G/N$ dann is

$$\{e\} \subset \tilde{N}_1 \subset \cdots \subset \tilde{N}_l = N = q^{-1}(\tilde{N}_l) \subset q^{-1}(\tilde{N}_{l+1}) \subset \cdots \subset q^{-1}(\tilde{N}_k) = G$$

eine Auflösungskette für G.

2) Wenn $\{N_i\}$ eine Auflösungskette ist, dann ist $N_{i+1}/N_i = \mathbb{Z}/(a_1) \oplus \cdots \oplus \mathbb{Z}/(a_m)$ abelsch.

Sei p eine Primzahl die $|N_{i+1}/N_i|$ teilt. Dann sagt der Satz von Cauchy dass N_{i+1}/N_i eine zyklische Untergruppe H der Ordnung p hat sodass $\{e\} \subset H \subset N_{i+1}/N_i$.

$$\{e\} \subset N_1 \subset N_2 \subset \cdots \subset N_i \subset q^{-1}(H) \subset N_{i+1} \subset \cdots \subset N_k$$

□

Definition 4.31
Eine Gruppe G ist einfach, wenn die einzige normalen Untergruppen $\{e\}$ und G sind.

Satz 4.32
Wenn G eine endliche einfache abelsche Gruppe ist, dann ist

$$G \cong \mathbb{Z}/(p)$$

für eine Primzahl p.

Satz 4.33
Für $n \geq 5$ ist S_n nicht auflösbar.

Beweis. Nutze den nächsten Satz. □

Satz 4.34
Für $n \geq 5$ ist A_n einfach.

Wobei $A_n = \{\sigma \in S_n \mid \operatorname{sign}(\sigma) = 1\}$.

Beweis. Zwei Zutaten: Sei $\{e\} \neq N \subset A_n$ eine normale Untergruppe.

1) Wenn N ein 3-Zykel enthält, dann ist $N = A_n$

2) N enthält einen 3-Zykel

<u>1)</u> Sei $(abc) \in N$. Wir zeigen $(abd) \in N$.

Wir nehmen $\tau = (ab)(cd) \in A_n$. Dann ist $\tau\sigma\tau^{-1} = (bad)$.

Also ist $(abd) = (\tau\sigma\tau^{-1})^{-1} \in A_n$.

Weil N normal ist gilt $(abd) \in N$.

<u>2)</u> Sei $e \neq \sigma \in N$ ein Element, dass so viele Elemente von $\{1, 2, 3, \dots, n\}$ festhält wie möglich.

Angenommen σ fixiert $n - 3$ Elemente, dann ist σ ein 3-Zykel.

Angenommen σ fixiert $n - 4$ Elemente

$$\sigma = \begin{cases} (abcd) & \notin A_n \\ (ab)(cd) & \end{cases}$$

Sei $e \in \{1, \dots, n\}$ verschieden von a, b, c und d. Setze $\tau = (cde) \in A_n$

Dann ist $\tilde{\sigma} = \tau\sigma\tau^{-1} = (ab)(de) \in N$ und $\tilde{\sigma}\sigma = (dce) \in N$ ↯.

Angenommen σ ändert ≥ 5 Elemente. Schreibe σ also Produkt von disjunkten Zykeln absteigend geordnet nach Länge. Also

$$\sigma = \begin{cases} (abcde\dots)(\dots)(\dots)\dots \\ (abcd)(ef\dots)\dots \\ (abc)(de\dots \\ (ab)(cd)\dots \end{cases}$$

Konjugiere jetzt σ durch $\tau = (bcd) \in A_n$, dann fixiert $\tau\sigma\tau^{-1} \in N$ mehr Elemente als σ.

Also enthält N einen 3-Zykel.

$\Rightarrow N = A_n$ also ist A_n einfach.

<u>Für $n = 5$ und $\#A_5 = 60$</u>

- Berechne eine Tabelle von Konjugationsklassen von A_5.
- Wenn N normal ist, dann ist es eine Vereinigung von Konjugationsklassen.
- Auf der anderen Seite teilt $\#N$ $\#A_5 = 60$.

□

5 Anwendungen

5.1 Satz vom primitiven Element

<u>Erinnerung:</u> Sei L/k eine Körpererweiterung. Die Erweiterung heißt einfach, falls $a \in L$ existiert, mit $L = k(a)$. Solche $a \in L$ heißen primitiv.

<u>Ziel:</u> Sehr viele Erweiterungen sind einfach.

Satz 5.1 (Kriterium für Einfachheit)
Sei L/k eine Körpererweiterung dann sind äquivalent:

1) L/k ist einfach und algebraisch

2) Es gibt nur endlich viele Zwischenkörper

Beweis. $\underline{1) \Rightarrow 2)}$ Angenommen L sei einfach und algebraisch. Wähle primitives Element $a \in L$. Das Minimalpolynom von a sei $f_k(x) \in k[x] \subseteq L[x]$.

Beobachtung: Wenn Z ein Zwischenkörper ist, dann ist a algebraisch über Z und hat Minimalpolynom $f_Z(x) \in Z[x] \subseteq L[x]$.

Es gilt: im Ring $L[x]$ ist f_Z ein normierter Teiler von f_k.

Habe also Abbildung

$$\{\text{Zwischenkörper}\} \xrightarrow{\phi} \underbrace{\{\text{norm. Polynome in } L[x], \text{ die Teiler von } f_k \text{ sind}\}}_{\text{endl. weil } L[x] \text{ faktoriell ist}}$$

Wir möchten zeigen: diese Abbildung ist injektiv. Dazu hätten wir gerne eine Abbildung η sodass $\eta \circ \phi = Id$.

Das geht so: Gegeben Polynom $f(x) = \sum_{i=0}^{n-1} b_i x^i + x^n$. Dann betrachte den Körper $\eta(f) = k(b_0, \ldots, b_{n-1})$.

Um zu prüfen, ob $\eta \circ \phi = Id$, sei Z ein Zwischenkörper. Dann sei $f_Z(x) = \phi(Z) \in Z[x] \subseteq L[x]$.

Da die Koeffizienten von f_Z alle aus Z sind, ist $\eta(f_Z) \subseteq Z$.

Sehe: $f_Z \in n(f_Z)[x]$ ist irreduzibel, hat also Nullstelle $\Rightarrow f_Z$ ist Minimalpolynom von a über $\eta(f_Z)$.

$\Rightarrow [L : Z] = [Z(a) : Z] = \deg f_Z = [L : \eta(f_Z)] = [\eta(f_Z)(a) : \eta(f_z)]$

$\Rightarrow [Z : \eta(f_Z)] = 1 \Rightarrow Z = \eta(f_Z)$

$\underline{2) \Rightarrow 1)}$ Angenommen es gibt nur endlich viele Zwischenkörper.

L ist algebraisch: Widerspruch! Angenommen es gäbe ein transzendentes Element a. Dann $L \supseteq k(a) \supseteq k$ ein Zwischenkörper, und $k(a) \simeq k(x)$ den rationalen Funktionen in einer Variablen.

Dann haben wir aber Unterkörper $k(a) \supsetneq k(a^2) \supsetneq k(a^4) \ldots$
Wir haben also ∞ viele Zwischenkörper. $\lightning$

L ist einfach: Die Körpererweiterung L/k ist sogar endlich, also $L = k(a_1, \dots, a_n)$ für geeignete $a_i \in L$. Denn durch Adjunktion

$$k \subseteq k(a_1) \subseteq k(a_1, a_2) \subseteq \dots$$

konstruieren wir Ketten von Zwischenkörpern, es gibt aber nur endlich viele!

Falls k endlich ist, dann ist L auch endlich (weil endliche Erweiterungen von endlichem Körper) und L^* ist zyklisch. Finde also $a \in L^*$ sodass $L^* = \{a, a^2, a^3, \dots, a^n\}$

$\Rightarrow k(a) = L$, also ist a primitiv!

Sei also ab sofort k unendlich.

Wir wissen schon: es gibt endlich viele $a_1, \dots, a_n \in L$ sodass $L = k(a_1, \dots, a_n)$. Betrachte Abbildung

$$\begin{aligned} k &\longrightarrow \text{Zwischenkörper} \\ \lambda &\longmapsto k(a_1 + \lambda a_2) \end{aligned}$$

Finde also $\lambda_1 \neq \lambda_2 \in k$ sodass $k(a_1 + \lambda_1 a_2) = k(a_1 + \lambda_2 a_2) = Z$.

Wir wissen: $Z \subseteq k(a_1, a_2)$ und wissen auch: $\lambda_2(a_1 + \lambda_1 a_2) - \lambda_1(a_1 + \lambda_2 a_2) = (\lambda_2 - \lambda_1)a_1 \in Z$. $\Rightarrow a_1 \in Z$.

Analog folgt auch $a_2 \in Z$.

Insgesamt: $k(a_1 ü \lambda_1 a_2) = k(a_1, a_2)$

also $k(a_1, a_2, \dots, a_n) = k(a_1 ü \lambda_1 a_2, a_3, \dots, a_n)$.

Wiederhole das Argument, erhalte primitives Element $a \in L$. $\square$

Satz 5.2 (Satz vom primitiven Element)
Sei L/k eine separable, endliche Körpererweiterung. Dann ist $L(k)$ einfach.

Beweis. Sei $N \subset \overline{k}$ die normale Hülle von L. Dann ist N/k endlich und galois'sch. Dann gibt es maximal endlich viele Zwischenkörper $N \supseteq \dots \supseteq k$. (genau so viele wie $\mathrm{Gal}(N/k)$ Untergruppen hat) $\Rightarrow L/k$ hat endlich viele Zwischenkörper und ist damit einfach. $\square$

5.2 Kreisteilungskörper

<u>Ziel:</u> Antwort auf die Frage, ob das regelmäßige n-Eck konstruierbar ist.

Dazu betrachte Zerfällungskörper L_n von $x^n - 1 \in \mathbb{Q}[x]$, genannt n-te Kreisteilungskörper.

Wir wissen: $L_n \subseteq \mathbb{C}$, die Nullstellen von $x^n - 1$ heißen n-te Einheitswurzeln. Die Menge der n-ten Einheitswurzeln bilden zyklische Untergruppe von $\mathbb{C}^*$, eine Einheitswurzel heißt primitiv, wenn sie die Gruppe erzeugt.

Ganz allgemein: Identifiziere die Gruppe der n-ten Einheitswurzeln $\{e^{\frac{2\pi i}{n}\cdot j} \mid 1 \leq j \leq n\}$ und $\mathbb{Z}/(n)$.

Wissen schon: Die j-te Einheitswurzel ist primitiv $\Leftrightarrow \text{ggT}(j, n) = 1 \Leftrightarrow$ Restklasse von j ist Einheit in $\mathbb{Z}/(n)$.

Muss primitive Einheitswurzeln verstehen, um die irredzuiblen Faktoren von $x^n - 1$ (und damit L_n) zu verstehen. Wie viele primitive Einheitswurzeln gibt es?

Definition 5.3
Die Abbildung

$$\begin{aligned} \mathbb{N} &\xrightarrow{\varphi} \mathbb{N} \\ n &\mapsto \#\{\textit{prim } n\textit{-te Einheitswurzeln}\} \end{aligned}$$

heißt Eulersche φ-Funktion.

Satz 5.4
Es gilt:

1) *Wenn $n, m \in \mathbb{N}$ teilerfremd sind $\Rightarrow \varphi(n \cdot m) = \varphi(n) \cdot \varphi(m)$*

2) *Wenn $p \in \mathbb{N}$ prim ist $\alpha \in \mathbb{N} \Rightarrow \varphi(p^\alpha) = p^{\alpha-1}(p-1)$*

3) *Dann*
$$\varphi(p_1^{\alpha_1} \cdot \dots \cdot p_n^{\alpha_n}) = p_1^{\alpha_1 - 1} \dots p_n^{\alpha_n - 1}(p_1 - 1) \dots (p_n - 1)$$
falls $p_1, \dots, p_n$ paarweise verschiedene Primzahlen sind.

Beweis. 1) Chinesischer Restsatz: $\mathbb{Z}/(n \cdot m) = \mathbb{Z}/(n) \times \mathbb{Z}/(m)$ also

$$(\mathbb{Z}/(n \cdot m))^* = (\mathbb{Z}/(n))^* \times (\mathbb{Z}/(m))^*$$

also $\varphi(n \cdot m) = \varphi(n) \cdot \varphi(m)$

2) Die Nullteiler (= nicht Einheiten) im Ring $\mathbb{Z}/(p^\alpha)$ sind genau die Restklassen der j mit $\text{ggT}(j, p^\alpha) \neq 1$. Das sind exakt:

$$p, 2 \cdot p, 2 \cdot p, 4 \cdot p, \dots, p^{\alpha-1}p$$

also $p^{\alpha-1}$ viele. Also #Einheiten $= p^\alpha - p^{\alpha-1} = p^{\alpha-1} \cdot (p-1)$ □

Definition 5.5
Das n-te Kreisteilungspolynom ist

$$\phi_n(x) = \prod_{\substack{\xi \text{ eine prim} \\ n\text{-te EHW}}} (x - \xi) \qquad \in \mathbb{C}[x]$$

Dann $\deg \phi_n = \varphi(n)$.

Bemerkung: ϕ_n kann man ganz gut ausrechnen! Denn

$$\phi_n(x) = \prod_{\substack{\xi \text{ eine} \\ n\text{-te EHW}}} (x - \xi)$$

Wenn ξ jetzt irgendeine n-te Einheitswurzel ist, mit $\operatorname{ord}(\xi) = d$, dann ist $d \mid n$ und ξ ist primitive d-te Einheitswurzel.

$$\Rightarrow x^n - 1 = \prod_{\substack{\xi \text{ eine} \\ n\text{-te EHW}}} (x - \xi) = \prod_{d|n} \prod_{\substack{\xi \text{ eine prim} \\ n\text{-te EHW}}} (x - \xi) = \prod_{d|n} \phi_d(x)$$

Wissen noch: $\phi_1(x) = x - 1$

Falls p prim:

$$x^p - 1 = \phi_1(x) \cdot \phi_p(x) \Rightarrow \phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + 1$$

Analog:

$$x^{15} - 1 = \phi_1(x) \cdot \phi_3(x) \cdot \phi_5(x)\phi_{15}(x)$$

$$\phi_{15}(x) = \frac{x^{15} - 1}{(x-1)(x^2+x+1)(x^4+x^3+x^2+x+1)} = x^8 - x^7 + x^5 - x^4 + x^3 - x + 1$$

Bemerkung: Für alle n gilt sogar $\phi_n \in \mathbb{Z}[x]$

Bemerkung: Für alle n ist ϕ_n irreduzibel.

<u>Zusammenfassung:</u>

- L_n ist Zerfällungskörper von $x^n - 1$, also $L_n/\mathbb{Q}$ ist Galois

- Wenn ξ eine primitive n-te Einheitswurzel ist, dann ist $L_n = \mathbb{Q}(\xi)$. Minimalpolynom von ξ ist ϕ_n.
$$\Rightarrow [L_n : \mathbb{Q}] = \phi(n) = \#(\mathbb{Z}/(n))^*$$

Satz 5.6

$$\mathrm{Gal}(L_n/\mathbb{Q}) \cong (\mathbb{Z}/(n))^*$$

Beweis. Müssen injektiven Gruppenmorphismus finden! Wähle primitive Einheitswurzel ξ. Gegeben $\sigma \in \mathrm{Gal}(L_n/\mathbb{Q})$ betrachte $\sigma(\xi)$. Dies ist primitive n-te Einheitswurzel, weil σ die Nullstellen von ϕ_n permutiert.

Also: $\sigma(\xi) = \xi^{r_\sigma}$ wobei $r_\sigma \in (\mathbb{Z}/(n))^*$.

Nachrechnen: Die Abbildung

$$\begin{aligned} \mathrm{Gal}(L_n/\mathbb{Q}) &\longrightarrow (\mathbb{Z}/(n))^* \\ \sigma &\longmapsto r_\sigma \end{aligned}$$

ist Gruppenmorphismus. Die Abbildung ist injektiv, denn σ ist durch $\mathrm{Bild}(\sigma(\xi))$ festgelegt, denn $L_n = \mathbb{Q}(\xi)$. □

Satz 5.7 (nach ein Satz von Gauß)
Das reguläre n-Eck ist genau dann konstruierbar, wenn n von der Form

$$n = 2^\alpha \cdot p_1 \cdot \dots \cdot p_r$$

ist, wobei $\alpha \in \mathbb{N}$, und p_i sind unterschiedliche Primzahlen der Form $2^{n_i} + 1$.

Bemerkung: Angenommen $r = m \cdot l$ mit l ungerade

$$\Rightarrow 2^\nu + 1 = (2^{m+1} + 1) \cdot (2^{m(l-1)} - 2^{m(l-2)} + \dots - 2^l + 1)$$

keine Primzahl.

Inhalt... Konsequenz: Bei den Zahlen $2^{n_i} + 1$ aus dem Satz von Gauß darf n_i keine ungeraden Primteiler haben. d.h. n_i ist 2-er Potenz.

Sprache: Primzahlen der Form
$$2^{(2^{m_i})} + 1$$
heißen Fermatsche Primzahlen.

Beweis der Notwendigkeit von Gauß Bedingung. Sei n gegeben, sodass das reguläre n-Eck konstruierbar ist. $e^{\frac{2\pi i}{n}} \in \mathrm{Kons}(\{0, 1\})$.

Wir wissen schon: dann ist $\underbrace{[\mathbb{Q}(\xi):\mathbb{Q}]}_{\varphi(n)} = 2^m$ für geeignete $m \in \mathbb{N}$.

Zerlegen n in Primfaktoren:
$$n = \prod p_i^{\alpha_i}$$
wobei p_i Primzahlen $\alpha_i \in \mathbb{N}$.

Dann
$$\varphi(n) = \prod p_i^{\alpha_i - 1} \prod (p_i - 1) \leftarrow \text{soll 2-er Potenz sein}$$
Also in Primfaktorzerlegung von n dürfen alle ungeraden Primfaktoren maximal mit Multiplizität 1 auftreten und müssen Fermatsch sein! □

Die Hinreichendheit der Gaußschen Bedingung folgt aus diesem Satz:

Satz 5.8
Sei $\{0,1\} \subseteq M \subseteq \mathbb{C}$, sei $k = \mathbb{Q}(M \cup \overline{M})$, sei $z \in \mathbb{C}$. Dann ist die Zahl z mit Zirkel und Lineal aus M konstruierbar, wenn der Zerfällungskörper L/k des Minimalpolynoms von z über k Grad $[L:k] = 2^m$ hat.

Beweis. L/k ist separabel, normal und endlich, also galois'sch, $\mathrm{Gal}(L/k) = 2^m$ ist also eine 2er-Gruppe.

Sylow $\Rightarrow$ finde Kette von Untergruppen
$$\{1\} = N_0 \subsetneq N_1 \subsetneq N_2 \subseteq \cdots \subseteq N_l = \mathrm{Gal}(L/K)$$
Wobei für alle i gilt:

- N_i ist normal in N_{i+1}
- $N_{i+1}/N_i \simeq \mathbb{Z}/(2)$

Hauptsatz der Galoistheorie: dazu gehört Kette von Zwischenkörpern
$$L = Z_l \supsetneq Z_{l-1} \supsetneq \cdots \supsetneq Z_0 = k$$
sodass für alle i: Z_i/Z_{i-1} ist galois'sch mit Gruppe $\mathbb{Z}/(2)$, also insbesondere $[Z_i : Z_{i-1}] = 2$.

$\Rightarrow \forall i : Z_i$ entsteht aus Z_{i-1} durch Adjunktion einer Quadratwurzel. Aber: Quadratwurzeln können wir mit Zirkel und Lineal konstruieren. □

5.3 Das Quadratische Reziprozitätsgesetz

Sei p eine Primzahl. Sei $a \in \mathbb{Z}$ kein Vielfaches von p. Nenne a einen quadratischen Rest modulo p wenn die Gleichung $x^2 \equiv q(\mod p)$ in $\mathbb{Z}$ eine Lösung hat. Ansonsten nenne a quadratischen Nichtrest $\mod p$.

Frage: Wie viele quadratische Reste gibt es? Wie können wir entscheiden, ob gegebener $a \in \mathbb{Z}$ ein Quadratischer Rest ist.

Erste Beobachtung

- Die Eigenschaft: $e \notin (p) \Leftrightarrow$ Restklasse $\underline{a} \neq 0$ in $\mathbb{Z}/(p) = \mathbb{F}_p$. Also: $\underline{a} \in \mathbb{F}_p^*$.
- a ist quadratischer Rest $\mod p \Leftrightarrow \underline{a}$ ist Quadrat in $\mathbb{F}_p^* \Leftrightarrow \underline{a}$ liegt im Bild des Gruppenmorphismus

$$\begin{aligned} q : \mathbf{F}_p^* &\longrightarrow \mathbb{F}_p^* \\ n &\longmapsto n^2 \end{aligned}$$

Frage: Wie viele Elemente von $\mathbb{F}_p^*$ sind Quadrate?

Antwort: Falls $p = 2$: Alle! $\mathbb{F}_p^* = \{1\}$

Antwort: Sei $p \neq 2$. Dann $\ker(q) = \{\pm 1\}$

Also ist $\#\operatorname{Im}(q) = \#\mathbb{F}_p^* / \#\ker = \frac{p-1}{2}$

Das heißt: genau die Hälfte der Elemente in $\mathbb{F}_p^*$ sind Quadrate.

Frage: Ist unser gegebenes $a \in \mathbb{F}_p^*$ jetzt ein Quadrat?

Antwort 1: Ausprobieren, indem man alle Elemente quadriert. Das macht aber sehr viel Mühe!

Antwort 2 (Euler): Man betrachte folgenden Gruppenmorphismus:

$$\begin{aligned} e : \mathbb{F}_p^* &\longrightarrow \mathbb{F}_p^* \\ n &\longmapsto n^{\frac{p-1}{2}} \end{aligned}$$

Man erinnere sich: $\mathbb{F}_p^*$ ist zyklisch mit $p-1$ Elementen gegeben $n \in \mathbb{F}_p^*$, dann $\operatorname{ord}(n) \mid p-1$

$\Rightarrow \operatorname{ord}(n^{\frac{p-1}{2}}) \in \{1, 2\}$

Wenn n ein Quadrat ist, $n = m^2$ in $\mathbb{F}_p^*$, dann

$$n^{\frac{p-1}{2}} = m^{p-1} = 1$$

Wir sehen insgesamt: Die Abbildung e ist ein Morphismus

$$e : \mathbb{F}_p^* \longrightarrow (\{\pm 1\}, \cdot) \subseteq \mathbb{F}_p^*$$

Also: $\# \ker(e) = \#\mathbb{F}_p^*/2 = \frac{p-1}{2} = \#$Quadrate.

Da alle Quadrate im Kern liegen $\Rightarrow \ker = \{$Quadrate$\}$

<u>Euler Kriterium:</u> a ist Quadrat in $\mathbb{F}_p^*$ genau dann wenn $a^{\frac{p-1}{2}} = 1$ in $\mathbb{F}_p^*$.

Die Abbildung e ist multiplikativ.

Das Euler Kriterium ist viel besser, macht aber immer noch sehr viel Arbeit. Die beste Lösung: quadratische Reziprozität