WESTFÄLISCHE
WILHELMS-UNIVERSITÄT
MÜNSTER

FACHBEREICH 10
MATHEMATIK UND
INFORMATIK

Skript Einführung in die Algebra

Mitschrift der Vorlesung „Einführung in die Algebra“ von Prof. Dr. Arthur Bartels

Jannes Bantje

4. September 2014

Aktuelle Version verfügbar bei:

GitHub (inklusive Sourcecode)
`https://github.com/JaMeZ-B/latex-wwu`

Bittorrent Sync
`B6WH2DISQ5QVYIRYIEZSF4ZR2IDVKPN3I`

Vorwort — Mitarbeit am Skript

Dieses Dokument ist eine Mitschrift aus der Vorlesung „Einführung in die Algebra, WiSe 2013“, gelesen von Prof. Dr. Arthur Bartels. Der Inhalt entspricht weitestgehend dem Tafelanschrieb. Für die Korrektheit des Inhalts übernehme ich keinerlei Garantie! Für Bemerkungen und Korrekturen – und seien es nur Rechtschreibfehler – bin ich sehr dankbar. Korrekturen lassen sich prinzipiell auf drei Wegen einreichen:

- Persönliches Ansprechen in der Uni, Mails an `j.bantje@wwu.de` (gerne auch mit annotieren PDFs)
- *Direktes* Mitarbeiten am Skript: Den Quellcode poste ich auf GitHub (siehe oben), also stehen vielfältige Möglichkeiten der Zusammenarbeit zur Verfügung: Zum Beispiel durch Kommentare am Code über die Website und die Kombination Fork + Pull Request. Wer sich verdient macht oder ein Skript zu einer Vorlesung, die ich nicht besuche, beisteuern will, dem gewähre ich gerne auch Schreibzugriff.

  Beachten sollte man dabei, dass dazu ein Account bei `github.com` notwendig ist, der allerdings ohne Angabe von persönlichen Daten angelegt werden kann. Wer bei GitHub (bzw. dem zugrunde liegenden Open-Source-Programm „`git`“) – verständlicherweise – Hilfe beim Einstieg braucht, dem helfe ich gerne weiter. Es gibt aber auch zahlreiche empfehlenswerte Tutorials im Internet.[1]
- *Indirektes* Mitarbeiten: TeX-Dateien per Mail verschicken.

  Dies ist nur dann sinnvoll, wenn man einen ganzen Abschnitt ändern möchte (zB. einen alternativen Beweis geben), da ich die Änderungen dann per Hand einbauen muss!

Vorlesungshomepage

`http://wwwmath.uni-muenster.de/reine/u/topos/lehre/WS2013-2014/Algebra/algebra.html`

[1] zB. `https://try.github.io/levels/1/challenges/1`, ist auf Englisch, aber dafür interaktives LearningByDoing

Inhaltsverzeichnis

1 Gruppen

1.1 Definition

Ein **Monoid** ist eine Menge M mit einer Verknüpfung $M \times M \to M, (a,b) \mapsto a \cdot b$ so dass folgende Axiome erfüllt sind:

(i) $\forall a, b, c \in M : (a \cdot b) \cdot c = a \cdot (b \cdot c)$

(ii) $\exists e \in M : \forall a \in M : a \cdot e = a = e \cdot a$

Gilt $\forall a, b \in M \; a \cdot b = b \cdot a$ so heißt M **kommutativ** oder **abelsch**. Beispiel:

(i) $(\mathbb{N}, +)$

(ii) $(\mathbb{Z}, +)$

(iii) $(\mathbb{N}, \cdot)$

(iv) $(N \cup \{\infty\}, +)$ mit $a + \infty = \infty = \infty + a$ $\forall a \in \mathbb{N} \cup \{\infty\}$

Bemerkung: Das neutrale Element e ist eindeutig.

1.2 Definition

Eine **Gruppe** ist ein Monoid G in dem jedes Element ein Inverses besitzt:

$$\forall a \in G : \quad \exists b \in G \text{ mit } a \cdot b = e = b \cdot a$$

1.3 Bemerkung

Das Inverse zu a ist eindeutig und wird mit a^{-1} bezeichnet.

1.4 Bemerkung

Sei G eine Gruppe. $a, b \in G$. Dann besitzt die Gleichung $a \cdot x = b$ eine eindeutige Lösung, nämlich $x = a^{-1} \cdot b$

1.5 Beispiele

i) $(\mathbb{Z}, +)$

ii) $(\mathbb{Q}, +)$

iii) $(\mathbb{Q}^{\times}, \cdot)$ (Menge der Einheiten)

iv) $Gl(V)$ (Menge aller invertierbaren Endomorphismen über V)

v) $Gl(n, K)$ (Menge aller invertierbaren $n \times n$-Matrizen über den Körper K)

vi) Sei X eine Menge. Dann heißt $S_X := \{\sigma : X \to X \,|\, \sigma \text{ ist bijektiv}\}$ die **symmetrische Gruppe** von X. ($S_n := S_{\{1,\dots,n\}}$)

vii) Die Symmetriegruppe $S_{\square}$ des Quadrats

viii) Die Symmetriegruppe $S_{\bigcirc}$ des Kreises

ix) Sei K ein Körper, dann ist die Menge $\mathrm{Aut}(K)$ der **Körperautomorphismen** von K eine Gruppe

x) Sei $p = X^n + a_{n-1}X^{n-1} + \ldots + a_0 \in K[X]$ ein Polynom. Wir werden später die Nullstellen von p untersuchen, in dem wir p eine Gruppe zuordnen

xi) Sei φ eine Kategorie und M ein Objekt von φ. Dann ist die Menge $\mathrm{Aut}_\varphi(M)$ aller invertierbaren Morphismen $f : M \to M$ in φ eine Gruppe.

1.6 Verknüpfungstafeln

Verknüpfungstafeln für die Gruppen $(\mathbb{Z}/4\mathbb{Z}, +)$ und $(S_\triangle, \circ)$

$+$	$[0]$	$[1]$	$[2]$	$[3]$
$[0]$	$[0]$	$[1]$	$[2]$	$[3]$
$[1]$	$[1]$	$[2]$	$[3]$	$[0]$
$[2]$	$[2]$	$[3]$	$[0]$	$[1]$
$[3]$	$[3]$	$[0]$	$[1]$	$[2]$

$\circ$	id	R_1	R_2	S_A	S_B	S_C
id	id	R_1	R_2	S_A	S_B	S_C
R_1	R_1	R_2	id	S_C	S_A	S_B
R_2	R_2	id	R_1	S_B	S_C	S_A
S_A	S_A	S_B	S_C	id	R_1	R_2
S_B	S_B	S_C	S_A	R_2	id	R_1
S_C	S_C	S_A	S_B	R_1	R_2	id

Tabelle 1: Verknüpfungstafeln für $(\mathbb{Z}/4\mathbb{Z}, +)$ und $(S_\triangle, \circ)$

1.7 Definition

Die **Ordnung** einer Gruppe G ist ihre Mächtigkeit $|G|$.

1.8 Definition

Sei G eine Gruppe. Eine Teilmenge $U \subseteq G$ heißt eine **Untergruppe** falls gilt:

(i) $e \in U$

(ii) $\forall a, b \in U$ ist $a \cdot b \in U$

(iii) $\forall a \in U : a^{-1} \in U$

1.9 Definition

Seien G und H Gruppen. Eine Abbildung $\varphi : G \to H$ heißt ein **Gruppenhomomorphismus**, falls gilt:

$$\forall a, b \in G : \varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$$

1.10 Bemerkung

Ist φ ein Gruppenhomomorphismus, so gilt:

(i) $\varphi(e) = e$

(ii) $\forall a \in G : \varphi(a^{-1}) = \varphi(a)^{-1}$

1.11 Beispiel

gemeint: $(\mathbb{Z}, +)$

(i) Sei $n \in \mathbb{N}$. Dann ist $\varphi_n : \mathbb{Z} \to \mathbb{Z}$ mit $\varphi_n(k) = n \cdot k$ ein Gruppenhomomorphismus.

L_a ist kein Gruppenhomomorphismus!

(ii) Sei G eine Gruppe. Zu $a \in G$ sei $L_a : G \to G$ mit $L_a(g) = a \cdot g$ Dann ist $G \xrightarrow{\varphi} S_G$, $a \mapsto L_a$ ein injektiver Gruppenhomomorphismus. Behauptung:

$$\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$$

Beweis:

$$a \cdot b \cdot g = L_{ab}(g) = L_a \circ L_b(g) = L_a\big(L_b(g)\big) = a \cdot b \cdot g$$

Injektivität: Seien $a, b \in G$ mit $L_a = \varphi(a) = \varphi(b) = L_b$. Es gilt $a \cdot g = L_a(g) = L_b(g) = bg \Rightarrow a = b$

(iii) Sei G eine Gruppe und $g \in G$. Dann ist $\operatorname{conj}_g : G \to G$ mit $\operatorname{conj}_g(a) := g \cdot a \cdot g^{-1}$ ein Automorphismus (bijektiver Gruppenhomomorphismus $G \to G$) von G.

Automorphismen dieser Form heißen **innere Automorphismen** .

1.12 Definition

Sei $\varphi : G \to H$ ein Gruppenhomomorphismus. Dann heißt $\operatorname{Bild}(\varphi) = \{\varphi(g) \,|\, g \in G\}$ das **Bild** von φ und $\operatorname{Kern}(\varphi) = \{g \,|\, \varphi(g) = e_H\}$ der **Kern** von φ.

Bemerkung:

- $\operatorname{Kern}(\varphi)$ und $\operatorname{Bild}(\varphi)$ sind Untergruppen von G bzw. H.
- φ surjektiv $\Leftrightarrow \operatorname{Bild}(\varphi) = H$. φ injektiv $\Leftrightarrow \operatorname{Kern}\varphi = \{e_G\}$

1.13 Beispiel

Seien G und H Gruppen. Dann ist auch das kartesische Produkt $G \times H$ eine Gruppe

$$(g,h) \cdot (g',h') = (gg',hh'), e_{G\times H} = (e_G, e_H), (g,h)^{-1} = (g^{-1}, h^{-1})$$

1.14 Lemma

Sei M ein endlicher Monoid. Es gelte

$$\begin{aligned} \forall a, b, b' \in G : a \cdot b = a \cdot b' &\Rightarrow b = b' \\ b \cdot a = b' \cdot a &\Rightarrow b = b' \end{aligned}$$

Dann ist M eine Gruppe. Beweis: Übung

1.15 Definition

Sei G eine Gruppe, $U \subseteq G$ eine Untergruppe. Eine **Linksnebenklasse** von U ist eine Teilmenge von G der Gestalt $a\,U := \{a \cdot u \,|\, u \in U\}$ wobei $a \in G$. Die Menge aller Linksnebenklassen bezeichnen wir mit ${}^{G}\!/_{U} := \{a\,U \,|\, a \in G\}$. Die Anzahl der Linksnebenklassen heißt der **Index** $[G:U]$ von U in G.

Beispiel: $G = \mathbb{Z}, U = 2\mathbb{Z} = \{n \in \mathbb{Z} \,|\, n \text{ ist gerade}\}$. Dann benutzen wir additive Schreibweise $n + U$ für die Linksnebenklasse von U. Dann:

i) $2\mathbb{Z} = 0 + 2\mathbb{Z} = 2 + 2\mathbb{Z} = 4 + 2\mathbb{Z} = -2 + 2\mathbb{Z} = \ldots$

ii) $1 + 2\mathbb{Z} = 3 + 2\mathbb{Z} = 5 + 2\mathbb{Z} = -1 + 2\mathbb{Z} = \ldots$

iii) $\mathbb{Z} = 2\mathbb{Z} \,\dot\cup\, (1 + 2\mathbb{Z})$

1.16 Lemma

Seien $a\,U$ und $b\,U$ Linksnebenklassen von U in G. Dann sind äquivalent:

i) $aU = bU$

ii) $aU \cap bU \neq \emptyset$

iii) $b^{-1}a \in U$

iv) $a \in bU$

Beweis
i)⇒ii) Ist $aU = bU$ dann ist $aU \cap bU = aU$. Da $e \in U$ ist $a = a \cdot e \in aU$, also $bU \cap aU \neq \emptyset$

ii)⇒iii) Sei $g \in aU \cap bU$. Dann $g = a \cdot u = b \cdot v$ mit $u, v \in U$. $\Rightarrow b^{-1} \cdot a = v \cdot u^{-1} \in U$.

iii)⇒iv) Ist $b^{-1} \cdot a \in U$, so folgt $a = b \cdot (b^{-1}a) \in bU$

iv)⇒i) Sei $a \in bU$. Dann $a = b \cdot v$ mit $v \in U$. Es folgt

$$aU = \{a \cdot u \mid u \in U\} = \{b \cdot v \cdot u \mid u \in U\} = \{b \cdot u' \mid u' \in U\} = bU \qquad \square$$

1.17 Lemma

Je zwei Linksnebenklassen von U in G sind gleichmächtig, $|aU| = |bU|$.

Beweis
Für $a \in G$ ist $U \to aU, u \mapsto a \cdot u$ eine bijektive Abbildung ($x \mapsto a^{-1}x$ ist die inverse Abbildung). $\square$

1.18 Satz von Lagrange

Sei G eine endliche Gruppe und U eine Untergruppe von G. Dann gilt:

$$|G| = [G : U] \cdot |U|$$

Beweis
G ist die disjunkte Vereinigung der Linksnebenklassen (Da $g \in gU$, ist G die Vereinigung der Linksnebenklassen, nach dem 1. Lemma ist diese disjunkt). Also

$$|G| = |\dot{\bigcup}_{aU \in G/U} aU| = \sum_{aU \in G/U} |aU| = \sum_{aU \in G/U} |U| = |G/H| \cdot |U| = [G : U] \cdot |U| \qquad \square$$

1.19 Bemerkung

Analog zu Linksnebenklassen kann man die **Rechtsnebenklassen** $Ua = \{u \cdot a \mid u \in U\}$ betrachten. Die Menge der Rechtsnebenklassen bezeichnen wir mit $G\backslash U$.
Übung:

(i) $|G/U| = |G\backslash U|$

(ii) $|U| = |U a|$

(iii) $Ua = Ub \Leftrightarrow Ua \cap Ub \neq \emptyset \Leftrightarrow a \in Ub \Leftrightarrow ab^{-1} \in U$

1.20 Definition

Eine Untergruppe $N \leq G$ heißt ein **Normalteiler**, wenn $aN = Na$ ist für alle $a \in G$.
Bemerkung: Ist G abelsch, so ist jede Untergruppe ein Normalteiler.

1.21 Lemma

Eine Untergruppe $N \leq G$ ist genau dann ein Normalteiler, wenn gilt:

$$\forall a \in G : aNa^{-1} = N$$

(Hier ist $aNa^{-1} = \left\{ana^{-1} \,\middle|\, n \in N\right\}$)
Beispiel: Ist φ ein Gruppenhomomorphismus, so ist $\operatorname{Kern}\varphi \subseteq G$ ein Normalteiler.

1.22 Lemma

Sei $N \leq G$ ein Normalteiler. dann wird auf G/N durch $aN \cdot bN := abN$ eine wohldefinierte Gruppenstruktur erklärt. Ihr neutrales Element ist $eN = N$. Es gilt $(aN)^{-1} = a^{-1}N$. Durch $\pi : G \to G/N, a \mapsto aN$ ist ein Gruppenhomomorphismus mit $\operatorname{Kern}\pi = N$ definiert.

1.23 Definition

G/N heißt **Faktorgruppe** oder **Restklassengruppe** von G nach N.
Beispiel: $G = \mathbb{Z}, N = n\mathbb{Z}, G/\mathbb{N} = \mathbb{Z}/n\mathbb{Z}$.

Beweis der Lemmas
Zur Wohldefiniertheit von $aN \cdot bN := abN$ ist zu zeigen: Ist $a_1N = a_2N$ und $b_1N = b_2N$ so ist $a_1b_1N = a_2b_2N$. Sei also $a_1N = a_2N$ und $b_1N = b_2N$. Es folgt $a := a_2^{-1}a_1 \in N$ und $b := b_2^{-1}b_1 \in N$. Dann ist

$$a_1\, b_1\, N = a_2\, a_2^{-1}\, a_1\, b_2\, b_2^{-1}\, b_1\, N = a_2\, a\, b_2\, b\, N = a_2\, b_2\, \underbrace{(b_2^{-1}\, a\, b_2)}_{\in N}\, \underbrace{b}_{\in N}\, N = a_2\, b_2\, N \qquad \square$$

1.24 Homomorphiesatz

Sei $\varphi : G \to H$ ein Gruppenhomomorphismus und $N \trianglelefteq G$ ein Normalteiler. Gilt $N \subseteq \operatorname{Kern}\varphi$, so gibt es einen eindeutigen Gruppenhomomorphismus $\overline{\varphi} : G/N \to H$ mit $\varphi = \overline{\varphi} \circ \pi$.
Es gilt $\operatorname{Kern}\overline{\varphi} = \pi(\operatorname{Kern}\varphi)$ und $\operatorname{Bild}\overline{\varphi} = \operatorname{Bild}\varphi$. Insbesondere ist $\overline{\varphi}$ ein Isomorphismus, falls φ surjektiv ist und $\operatorname{Kern}\varphi = N$ ist.

$$\begin{tikzcd} G \arrow[r, "\varphi"] \arrow[d, "\pi"'] & H \\ G/N \arrow[ur, dashed, "\overline{\varphi}"'] & \end{tikzcd}$$

Beweis
Wenn $\overline{\varphi}$ existiert, dann ist $\overline{\varphi}(aN) = \overline{\varphi}(\pi(a)) = \varphi(a)$, also ist $\overline{\varphi}$ eindeutig.
Zu Existenz definieren wir $\overline{\varphi}(aN) := \varphi(a)$. zZ: $a_1\, N = a_2\, N \Rightarrow \varphi(a_1) = \varphi(a_2)$. Ist $a_1N = a_2N$, dann $a_2^{-1}a_1 \in N \subseteq \operatorname{Kern}\varphi$, also $\varphi(a_1) = \varphi(a_2a_2^{-1}a_1)$. $\square$

1.25 Korollar

Sei $\varphi : G \to H$ ein Gruppenhomomorphismus. Dann gilt $\operatorname{Bild}\varphi \cong G/\operatorname{Kern}\varphi$.

Beweis
Mit $N = \operatorname{Kern}\varphi$ und $H = \operatorname{Bild}\varphi$ folgt dies aus dem Homomorphiesatz.

1.26 Bemerkung

Seien N, G und Q Gruppen mit Gruppenhomomorphismen

$$N \xhookrightarrow{\;i\;} G \xrightarrow{\;q\;}\!\!\!\!\rightarrow Q$$

Gilt i injektiv, q surjektiv, $\operatorname{Kern} q = \operatorname{Bild} i$ so heißt $(\star)$ eine **kurze exakte Folge** (oder Sequenz). Es gilt dann $Q \cong G/\operatorname{Kern} q \cong G/\operatorname{Bild} i$.

1.27 Definition

Eine Gruppe G, die keinen Normalteiler außer $\{e\}$ und G besitzt, heißt **einfach**.

1.28 Bemerkung

Die einfachen endlichen Gruppen sind vollständig klassifiziert. Es gibt mehrere unendliche Serien solcher Gruppen (zyklische Gruppen von Primzahlordnung, alternierende Gruppen A_n für $n \geq 5$, Gruppen vom Lie-Typ) und 26 sporadische einfache Gruppen. Die größte der sporadischen Gruppen hat etwa die Ordnung $8 \cdot 10^{53}$ und hat den schönen Namen das ”Monster”.

2 Zyklische Gruppen

2.1 Definition

Sei G eine Gruppe und $x \in G$. Dann heißt $\langle x \rangle := \{x^n \mid n \in \mathbb{Z}\}$ die von x **erzeugte Untergruppe**.

2.2 Bemerkung

(i) $\langle x \rangle$ ist eine Untergruppe $e = x^0, \quad x^n \cdot x^m = x^{n+m}, \quad (x^n)^{-1} = x^{-n}$

(ii) $\langle x \rangle$ ist die kleinste Untergruppe von G, die x enthält

(iii) $\langle x \rangle$ ist kommutativ: $x^n \cdot x^m = x^m \cdot x^n$

(iv) $\varphi : \mathbb{Z} \to G$, $\varphi(n) := x^n$ ist ein Gruppenhomomorphismus mit $\operatorname{Bild} \varphi = \langle x \rangle$

2.3 Definition

Eine Gruppe G heißt **zyklisch**, falls sie von einem Element erzeugt wird, d.h. falls es $x \in G$ gibt mit $\langle x \rangle = G$.

2.4 Beispiel

$\mathbb{Z}$ wird erzeugt von $1 \in \mathbb{Z}$ oder auch $-1 \in \mathbb{Z}$, aber nicht von $2 \in \mathbb{Z}$.

2.5 Lemma 1

Sei G eine Gruppe. Dann ist G genau dann zyklisch, wenn es einen surjektiven Gruppenhomomorphismus $\varphi : \mathbb{Z} \twoheadrightarrow G$ gibt.

Beweis
Ist $G = \langle x \rangle$ zyklisch, so ist $\varphi : \mathbb{Z} \to G$ mit $\varphi(n) := x^n$ ein surjektiver Gruppenhomomorphismus. Ist $\varphi : \mathbb{Z} \to G$ ein surjektiver Gruppenhomomorphismus so gilt $G = \langle x \rangle$ mit $x := \varphi(1)$

2.6 Satz: Klassifikationssatz für zyklische Gruppen

Sei G eine zyklische Gruppe. Dann ist

$$G \cong \begin{cases} \mathbb{Z}, & \text{falls } |G| = \infty \\ \mathbb{Z}/m\mathbb{Z}, & \text{falls } |G| = m < \infty \end{cases}$$

Beweis
Sei G eine zyklische Gruppe. Aus Lemma 1 (2.5) folgt: $\exists$ surjektiver Gruppenhomomorphismus $\varphi : \mathbb{Z} \twoheadrightarrow G$. Also $G \cong \mathbb{Z}/\operatorname{Kern}\varphi$ nach dem Homomorphiesatz (1.24). Aus Lemma 2 (2.8) folgt $\exists m \in \mathbb{N}$ mit $\operatorname{Kern}\varphi = m\mathbb{Z}$. Ist $m = 0$, so folgt $\operatorname{Kern}\varphi = \{0\}$, also $G \cong \mathbb{Z}/\{0\} \cong \mathbb{Z}$. Andernfalls $G \cong \mathbb{Z}/m\mathbb{Z}$. Ist $m \neq 0$, also $G \cong \mathbb{Z}/m\mathbb{Z}$ so folgt $m = |\mathbb{Z}/m\mathbb{Z}| = |G|$. $\square$

2.7 Bemerkung

Zyklische Gruppen werden durch ihre Ordnung klassifiziert: Für zyklische Gruppen H und G gilt:

$$G \cong H \Leftrightarrow |G| = |H|$$

2.8 Lemma 2

Sei $U \subseteq \mathbb{Z}$ eine Untergruppe. Dann gibt es $m \in \mathbb{N}$ mit $U = m\mathbb{Z} = \langle m \rangle$. Insbesondere ist U zyklisch.

Beweis
Ist $U = \{0\}$, so setze $m := 0$. Sei also $U \neq \{0\}$. Dann gibt es $n \in U, n \neq 0$. Nun ist $n > 0$ oder $-n > 0$. U enthält also mindestens ein n mit $n > 0$. Sei m das minimale positive Element in U.

Behauptung: $U = m\mathbb{Z}$. Wegen $m \in U$ ist $m\mathbb{Z} = \langle m \rangle \subseteq U$. Sei $a \in U$. Division mit Rest ergibt $a = q \cdot m + r$ mit $q \in \mathbb{Z}, r \in \{0, \ldots, m-1\}$. Es folgt

$$r = \underbrace{a}_{\in U} - \underbrace{q \cdot m}_{\in U} \in U$$

Da $r < m$ und $m \in U$ das minimale positive Element war, folgt $r = 0$. Also $a = q \cdot m \in U$. □

2.9 Proposition

Jede Untergruppe einer zyklischen Gruppe ist zyklisch.

Beweis
Sei G zyklisch und $U \subseteq G$. Mit Lemma 1 (2.5) folgt: $\exists \varphi : \mathbb{Z} \twoheadrightarrow G$. Dann ist $U' := \varphi^{-1}(U)$ eine Untergruppe von $\mathbb{Z}$. Lemma 2 besagt $U' = m\mathbb{Z}$. Insbesondere ist U' zyklisch. Damit ist auch $U = \varphi(U')$ zyklisch. □

2.10 Definition

Sei G eine Gruppe und $a \in G$. Dann heißt $\operatorname{ord}(a) := |\langle a \rangle|$ die **Ordnung** von a.

2.11 Bemerkung

$\operatorname{ord}(a)$ ist genau dann endlich, wenn es ein positives $n \in \mathbb{N}$ gibt mit $a^n = e$. In diesem Fall ist $\operatorname{ord}(a)$ die kleinste positive Zahl n mit $a^n = e$.

2.12 Satz

Sei G eine endliche Gruppe und $a \in G$. Dann teilt $\operatorname{ord}(a)$ die Ordnung von G.

Beweis
Satz von Lagrange mit $U := \langle a \rangle$. □

2.13 Satz

Sei G eine Gruppe von Primzahlordnung. Dann gilt

i) G ist zyklisch. Insbesondere $G \cong \mathbb{Z}/p\mathbb{Z}$ mit $p = |G|$

ii) $\{e\}$ und G sind die einzigen Untergruppen von G. Insbesondere ist G einfach.

Beweis
Sei $a \in G \setminus \{e\}$. Da die Ordnung von a die Ordnung von G teilt, ist $\operatorname{ord}(a) \in \{1, |G|\}$. Da $a \neq e$ ist, ist $\operatorname{ord}(a) \neq 1$. Also $\operatorname{ord}(a) = |G|$. Also $\langle a \rangle = G$.
ii) folgt mit Lagrange □

3 Gruppenwirkungen

3.1 Definition

Sei G eine Gruppe und X eine Menge. Eine **Wirkung** von G auf X ist eine Abbildung $G \times X \to X$, $(g, x) \mapsto g \cdot x$ die folgende Axiome erfüllt:

(i) $\forall x \in X : e \cdot x = x$

(ii) $\forall g, h \in G, \forall x \in X : g \cdot (h \cdot x) = (g \cdot h) \cdot x$

3.2 Bemerkung

Oft spricht man auch von einer **Operation** oder **Aktion**.

3.3 Bemerkung

Sei $G \times X \to X$, $(g, x) \mapsto gx$ eine Wirkung. Für $g \in G$ sei $\psi_g : X \to X, \psi_g(x) := gx$. Dann definiert $g \mapsto \psi_g$ einen Gruppenhomomorphismus $G \to S_X$. ($\psi_g \in S_X$ da $\psi_{g^{-1}} = (\psi_g)^{-1}$). Sei umgekehrt $\alpha : G \to S_X$ ein Gruppenhomomorphismus. Dann erhalten wir eine Wirkung $G \times X \to X$ durch $g \cdot x := \underbrace{\alpha(g)}_{\in S_X}(x)$. *siehe 1.5 vi)*

3.4 Beispiele

i) S_X wirkt auf X durch $\sigma \cdot x = \sigma(x)$ für $\sigma \in S_X, x \in X$

ii) Die Symmetriegruppe $S_\square$ des Quadrats wirkt kanonisch auf
- der Menge der Punkte des Quadrats
- der Menge der Ecken des Quadrats
- der Menge der Kanten des Quadrats
- der Menge der Paare von Kanten

iii) Sei G eine Gruppe. Dann ist $G \times G \to G$, $(g, x) \mapsto g \cdot_G x$ eine Wirkung von G auf $X := G$. Dies ist die **Linkstranslationswirkung**.

$g \cdot_R x := xg$, dann $g \cdot_R (h \cdot_R x) = g \cdot_R (xh) = (xh)g = x \cdot (h \cdot g) = (h \cdot g) \cdot_R x$
lässt sich durch Inverse kurieren.

Die **Rechtstranslationswirkung** ist definiert durch $G \times G \to G$, $(g, x) \mapsto x \cdot g^{-1}$

iv) Die **Konjugationswirkung** von G auf $X := G$ ist gegeben durch $G \times G \to G$, $(g, x) \mapsto g \cdot x \cdot g^{-1}$.

v) Sei $U \subseteq G$ eine Untergruppe. Dann wirkt G durch Linkstranslation auf den Linksnebenklassen ${}^G/_U$.

$$G \times {}^G/_U \to {}^G/_U \quad , \quad (g, aU) \mapsto gaU$$

3.5 Definition

Sei $G \times X \to X$ eine Wirkung. Sei $x \in X$.

i) $Gx := \{g \cdot x \mid g \in G\} \subseteq X$ heißt die **Bahn** oder der **Orbit** von x unter G.

ii) $G_x := \{g \mid g \cdot x = x\} \subseteq G$ heißt die **Standgruppe** oder **Isotopiegruppe** von x unter G.

3.6 Bemerkung

G_x ist eine Untergruppe von G, wie man sich leicht überlegt.

3.7 Lemma

Sei $G \times X \to X$ eine Wirkung. Seien $x, y \in X$. Dann gilt $Gx = Gy \iff Gx \cap Gy \neq \emptyset$

Beweis
"$\Rightarrow$" Ist klar, da $x \in Gx$, also $Gx \neq \emptyset$

"$\Leftarrow$" Sei $z \in Gx \cap Gy$. Dann $z = gx = hy$ mit $g, h \in G$. Also $(h^{-1}g) \cdot x = y$. Dann gilt

$$G \cdot y = G(h^{-1}g) \cdot x \subseteq G \cdot x$$

Genauso $Gx \subseteq Gy$. □

3.8 Korollar

X ist die disjunkte Vereinigung der Bahnen.

3.9 Lemma

Sei $G \times X \to X$ eine Wirkung. Sei $x \in X$. Dann definiert

$$G/G_x \xrightarrow{\varphi} Gx \quad , \quad gG_x \mapsto g \cdot x$$

eine Bijektion.

Beweis
φ **ist wohldefiniert:** Sei $gG_x = hG_x$. Dann $h^{-1}g \in G_x$. Also $g \cdot x = h(h^{-1}g) \cdot x = h \cdot x$

φ **surjektiv:** nach Definition der Bahn Gx.

φ **injektiv:** Sei $\varphi(gG_x) = \varphi(hG_x)$. Also $g \cdot x = h \cdot x$. Dann $h^{-1} \cdot g \cdot x = x$, also $h^{-1}g \in G_x$. Daher $hG_x = gG_x$. □

3.10 Satz (Bahnengleichung)

Sei $G \times X \to X$ eine Wirkung auf einer endlichen Menge X. Sei $x_1, \ldots, x_n$ ein **Vertretersystem** der Bahnen, d.h. jede Bahn enthält genau ein x_i. Dann gilt

$$|X| = \sum_{i=1}^{n} |Gx_i| = \sum_{i=1}^{n} [G : G_{x_i}]$$

Beweis
Da X die disjunkte Vereinigung der Bahnen $Gx_1, \ldots, Gx_n$ ist, gilt $|X| = \sum_{i=1}^{n} |Gx_i|$. Da es eine Bijektion $G/G_{x_i} \to Gx_i$ gibt, ist $|Gx_i| = |G/G_{x_i}| = [G : G_{x_i}]$. □

3.11 Definition

Sei $S \subseteq G$ eine Teilmenge. Dann heißt

Z_S	$:= \{g \in G \mid g \cdot s = s \cdot g \ \ \forall s \in S\}$	der **Zentralisator** von S
Z_G	$:= \{g \in G \mid g \cdot h = h \cdot g \ \ \forall h \in G\}$	das **Zentrum** der Gruppe G
N_S	$:= \{g \in G \mid gS = Sg\}$	der **Normalisator** von S in G

3.12 Bemerkung

(i) Z_S und N_S sind Untergruppen von G

(ii) Z_G ist ein Normalteiler.

(iii) Z_G ist abelsch.

(iv) Ist U eine Untergruppe, so ist $U \subseteq N_U$ ein Normalteiler. Genauso ist N_U die größte Untergruppe von G, die U als Normalteiler enthält.

3.13 Bemerkung

$g \cdot s = s \cdot g \iff s = g \cdot s \cdot g^{-1}$

Wer hätte das gedacht…

3.14 Satz (Klassengleichung)

Sei G eine endliche Gruppe und $g_1, \dots, g_n$ ein Vertretersystem für die Konjugationswirkung auf $G \setminus Z_G$. Dann gilt

siehe 3.4 iv)

$$|G| = |Z_G| + \sum_{i=1}^{n} [G : Z_{\{g_i\}}]$$

Beweis
Die Bahnengleichung (3.10) für die Konjugationswirkung von G auf $G \setminus Z_G$ liefert

$$|G| - |Z_G| = |G \setminus Z_G| = \sum_{i=1}^{n} [G : Z_{\{g_i\}}] \qquad \square$$

3.15 Definition

Sei p eine Primzahl. Eine p-**Gruppe** ist eine endliche Gruppe, deren Ordnung eine Potenz von p ist.

3.16 Beispiel

(i) $\mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$

$$H_{\mathbb{Z}/2\mathbb{Z}} = \left\{ \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \middle| \, a, b, c \in \mathbb{Z}/2\mathbb{Z} \right\}$$

$|H_{\mathbb{Z}/2\mathbb{Z}}| = 2^3 = 8$

3.17 Korollar

Sei P eine p-Gruppe, dann folgt aus der Klassengleichung, dass das Zentrum von P nichttrivial ist.

Beweis
Sei $p^m = |P|$. Mit der Klassengleichung (3.14) folgt für ein Vertretersystem x_i, $i = 1, \dots, n$:

$$p^m = |P| = |Z_P| + \sum_{i=1}^{n} [P : Z_{x_i}]$$

Da die x_i nicht im Zentrum von P liegen, ist $Z_{x_i} \neq P \ \forall x_i$. Daher teilt p den Index $[P : Z_{x_i}] = \frac{|P|}{|Z_{x_i}|}$. Also gilt: p teilt auch $|Z_P|$, also $|Z_P| > 1 \Rightarrow Z_P$ ist nicht $\{e\}$. $\square$

4 Sylow-Gruppen

4.1 Definition

Sei G eine endliche Gruppe. Eine Untergruppe P von G heißt p-**Sylow-Gruppe**, wenn P eine p-Gruppe ist und $[G : P]$ teilerfremd zu p ist.

4.2 Bemerkung

Ist $|G| = p^n \cdot l$ mit $p \nmid l$, so hat jede p-Sylow-Gruppe die Ordnung p^n.

4.3 Beispiele

(i) $\mathbb{Z}/12\mathbb{Z}$ enthält eine 2-Sylowgruppe.

(ii) S_3 enthält drei 2-Sylowgruppen

$$\{e, (12)\}, \{e, (13)\}, \{e, (23)\}$$

und eine 3-Sylowgruppe

$$\{e, (123), (132)\}$$

4.4 Satz (Sylow)

Sei G eine endliche Gruppe und p eine Primzahl. Dann gelten folgende 3 Aussagen

(1) Zu jeder p-Untergruppe U von G gibt es mindestens eine p-Sylow-Gruppe P mit $U \subseteq P$. Insbesondere gibt es mindestens eine p-Sylow-Gruppe.

(2) Sind P und Q zwei p-Sylow-Gruppen, dann gibt es ein $g \in G$ mit $gPg^{-1} = Q$. Je zwei p-Sylow-Gruppen sind also konjugiert zueinander.

(3) Für die Anzahl n_p der p-Sylow-Gruppen gilt: $n_p \mid |G|$ und $n_p \equiv 1 \mod p$

Beweis im Internet unter:
`http://wwwmath.uni-muenster.de/reine/u/topos/lehre/WS2013-2014/Algebra/algebra.html`

4.5 Bemerkung

Aussage (k) heißt auch k-ter Sylowsatz.

4.6 Korollar aus (2)

Eine p-Sylow-Gruppe in G ist ein Normalteiler genau dann, wenn sie die einzige p-Sylow-Gruppe von G ist.

Beweis
Sei P eine p-Sylow-Gruppe und $g \in G$. Dann ist gPg^{-1} eine weitere p-Sylow-Gruppe in G. Wenn P die einzige p-Sylowgruppe ist, gilt also $gPg^{-1} = P$. Für die andere Richtung seien P_1 und P_2 p-Sylowgruppen in G. Sei P_1 ein Normalteiler von G. Nach (2) gibt es ein $g \in G$ mit $P_2 = gP_1g^{-1} = P_1$, da P_1 Normalteiler. $\square$

4.7 Satz

Seien p und q Primzahlen mit $p < q$ und $p \nmid (q-1)$. Dann ist jede Gruppe der Ordnung $p \cdot q$ isomorph zu

$$\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$$

Beweis
Sei G die Gruppe mit Ordnung $p \cdot q$. Sei n_p die Anzahl der p-Sylow-Gruppen. Wir wissen:

(a) $n_p \mid p \cdot q$ (b) $n_p \equiv 1 \mod p$

Da p und q prim sind, folgt $n_p \mid p$ oder $n_p \mid q$. Wegen (b) ist $n_p \mid p$ ausgeschlossen, also gilt $n_p \in \{1, q\}$. Aber $n_p = q$ ist unmöglich, denn $q \equiv 1 \mod p \Leftrightarrow p \mid q - 1$ ↯ zur Annahme.
Es gibt also eine normale p-Sylow-Gruppe S_p. Sei n_q die Anzahl der q-Sylow-Gruppen

(a') $n_q \mid p \cdot q$ (b') $n_q \equiv 1 \mod q$

Wie oben folgt $n_q \in \{1, p\}$.
Wegen $q > p$ ist $p \not\equiv 1 \mod q$. Daher bleibt nur $n_q = 1$. Folglich gibt es eine q-Sylow-Gruppe S_q als Normalteiler in G. Außerdem ist $S_q \cap S_p = \{e\}$. Betrachte nun

$$\varphi : S_p \times S_q \to G \quad , \quad (a, b) \mapsto a \cdot b$$

Für $a \in S_p$ und $b \in S_q$ gilt:

$$a \cdot \underbrace{(b \cdot a^{-1} \cdot b^{-1})}_{\in S_p} \in S_p \quad \text{und auch} \quad (a \cdot b \cdot a^{-1}) \cdot b^{-1} \in S_q$$

$$\begin{aligned} &\Rightarrow a \cdot b \cdot a^{-1} \cdot b^{-1} \in S_p \cap S_q \\ &\Rightarrow a \cdot b \cdot a^{-1} \cdot b^{-1} = e \\ &\Rightarrow ab = ba \end{aligned}$$

$\Rightarrow \varphi$ ist ein Gruppenhomomorphismus.
Wegen Primzahlordnung gilt $S_p \cong \mathbb{Z}/p\mathbb{Z}$, $S_q \cong \mathbb{Z}/q\mathbb{Z}$. Sei $a \in S_p$ und $b \in S_q$ mit $\varphi(a, b) = ab = e$

$$ab = e \Leftrightarrow \underbrace{a}_{\in S_q} = \underbrace{b^{-1}}_{\in S_p} \Rightarrow a, b \in S_q \cap S_q$$

folglich gilt $a = b = e$. $\Rightarrow \varphi$ ist injektiv. Da $|S_p \times S_q| = |G| = p \cdot q$, ist φ auch surjektiv. $\square$

5 Polynome

5.1 Definition

Sei R ein kommutativer Ring mit 1. Ein formaler Ausdruck

$$p = a_n X^n + a_{n-1} X^{n-1} + \ldots + a_1 X + a_0$$

mit $a_n, \ldots, a_0 \in R$ heißt **Polynom** mit Koeffizienten in R. Die Menge aller Polynome wird mit $R[X]$ bezeichnet. Der **Grad** $d(p)$ von p ist gegeben durch $d(p) = \max\{i \,|\, a_i \neq 0\}$. Das Element $a_{d(p)} \in R$ heißt **Leitkoeffizient** von p. Für das Nullpolynom 0 setzen wir $d(0) := -\infty$ und $l(0) = 0$.
Ein Polynom mit $a_i = 0$ für $i \geq 1$ heißt **konstant**. Ist $l(p) = 1$, dann heißt p **normiert**.

5.2 Bemerkung

X ist eine formale Variable. Es gilt $0 \cdot X = 0$, aber X ist kein Element von R. Jedes $p \in R[X]$ definiert eine Abbildung $f_p : R \to R$, $\lambda \mapsto p(\lambda)$.

5.3 Beispiele

(i) $p = X^2 + X$ als Element von $\mathbb{F}_2[X]$. In diesem Fall ist $f_p = 0$, aber $p \neq 0$.

(ii) $p = 2X$ als Element von $\mathbb{F}_2[X]$ ist das Nullpolynom.

(iii) $p = 2X$ als Element von $\mathbb{Z}[X]$ ist nicht das Nullpolynom.

5.4 Bemerkung

Auf $R[X]$ lassen sich eine Addition und eine Multiplikation erklären:

$$(\sum_{k=0}^{n} a_k \cdot X^k) + (\sum_{k=0}^{n} b_k \cdot X^k) := \sum_{k=0}^{n} (a_k + b_k) \cdot X^k$$
$$(\sum_{k=0}^{m} a_k \cdot X^k) \cdot (\sum_{l=0}^{n} b_l \cdot X^l) := \sum_{j=0}^{m+n} (\sum_{k+l=j} a_k \cdot b_l) \cdot X^j$$

Das Konstante Polynom 1 ist ein Einselement für $\cdot$. Das konstante Polynom 0 ist ein Nullelement für $+$.

5.5 Definition

Eine Element $a \in R$ heißt **Nullteiler**, falls $b \in R \setminus \{0\}$ existiert mit $a \cdot b = 0$ (oder $b \cdot a = 0$). Falls R nur 0 als Nullteiler besitzt, heißt R **nullteilerfrei** oder **Integritätsring**.

5.6 Beispiele

(i) Jeder Körper ist nullteilerfrei.

(ii) 2 in $\mathbb{Z}/4\mathbb{Z}$ ist ein Nullteiler, denn $2 \cdot 2 = 4$ und $4 \equiv 0 \mod 4$.

5.7 Satz

Sei R ein kommutativer Ring mit 1. Seien $p, q \in R[X]$. Dann gilt:

(a) $d(p+q) \leq \max\{d(p), d(q)\}$

(b) $d(p \cdot q) \leq d(p) + d(q)$

Ist R nullteilerfrei, dann ist $d(p \cdot q) = d(p) + d(q)$. Außerdem ist $l(p \cdot q) = l(p) \cdot l(q)$.

Beweis
Für $p = 0$ oder $q = 0$ ist die Aussage klar.
$p = \sum_i a_i X^i$, $q = \sum_j b_j X^j$. Dann ist $a_i + b_i = 0$ für $i > \max\{d(p), d(q)\}$. Hieraus folgt (a). Außerdem ist $\sum_{k+l=j} a_k \cdot b_l = 0$ für $j \geq d(p) + d(q)$. Für $j = d(p) + d(q)$ erhalten wir

$$\sum_{k+l=j} a_k \cdot b_l = l(p) \cdot l(q)$$

5.8 Division mit Rest

Sei K ein Körper und seien $p, q \in K[X]$ mit $q \neq 0$. Dann gibt es genau eine Zerlegung der Form $p = s \cdot q + r$ mit $d(r) < d(q)$.

Beweis
Eindeutigkeit: Sei $p = s_0 q + r_0 = s_1 q + r_1$ mit $d(r_i) < d(q)$ für $i \in \{0, 1\}$.

$$(s_o - s_1)q = r_1 - r_0 \quad \Rightarrow \underbrace{d\big((s_0 - s_1)q\big)}_{d(s_0 - s_1) + d(q)} = d(r_1 - r_0) \leq \max\{d(r_0), d(r_1)\} < d(q)$$

$\Rightarrow d(s_1 - s_1) < 0 \Rightarrow d(s_1 - s_1) = -\infty \Rightarrow s_0 - s_1 = 0$, also auch $r_0 = r_1$.

Existenz Für $d(p) < d(q)$ setzen wir $s = 0$ und $r = p$.

Sei jetzt also $d(p) \geq d(q)$: Sei $n := d(q)$, sei $p = aX^{n+k} + \ldots$ und $q = b \cdot X^n + \ldots$. Das Polynom $p - ab^{-1}X^k q$ hat einen kleineren Grad als p. Nach Induktionsvorraussetzung gibt es $s, r \in K[X]$ mit $d(r) < d(q)$ und

$$p - ab^{-1}X^k q = s \cdot q + r \iff p = (s + ab^{-1}X^k)q + r \qquad \square$$

5.9 Bemerkung

Der Satz ist auch richtig für einen Polynomring $R[X]$, falls der Leitkoeffizient $l(p) \in R$ eine Einheit ist, d.h. $\exists x \in R$ mit $x \cdot l(q) = 1$.

R kommutativer Ring mit 1

Beispiel:

die Rechnung spare ich mir hier mal …

$$(X^5 + 3X^4 + X^3 - 6X^2 + 2X + 2) : (X^3 + 2X^2 + X - 1) = X^2 + X - 2$$

5.10 Korollar

Ist $\alpha \in K$ eine Nullstelle von $p \in K[X]$ $(p(\alpha) = f_p(\alpha) = 0)$. Dann gilt $p = q \cdot (X - \alpha)$ mit $q \in K[X]$.

Beweis
Übung

5.11 Definition

Ein Körper heißt **algebraisch abgeschlossen**, falls jedes nichtkonstante Polynom $p \in K[X]$ eine Nullstelle in K hat. Dann folgt, dass jedes Polynom $p \in K[X]$ in ein Produkt von Linearfaktoren zerfällt:

$$p = l(p)(X - \alpha_1)(X - \alpha_2) \dots (X - \alpha_n)$$

Beispiele:

- $\mathbb{C}$ ist algebraisch abgeschlossen.
- $\mathbb{R}$ ist nicht algebraisch abgeschlossen: Betrachte $X^2 + 1$

6 Ideale und Hauptidealringe

In Abschnitt 6 seien alle Ringe kommutativ mit Eins

6.1 Definition

Sei R ein Ring. Eine Teilmenge $I \subseteq R$ heißt **Ideal**, falls gilt:

(i) $I \subseteq R$ ist eine Untergruppe bezüglich $+$

(ii) $\forall a \in I : \forall r \in R : r \cdot a \in I$

6.2 Beispiel

(i) Für $N \in \mathbb{N}$ ist $N \cdot \mathbb{Z}$ ein Ideal in $\mathbb{Z}$.

(ii) $\left\{a_n X^n + a_{n-1}X^{n-1} + \ldots + a_1 X \,\middle|\, a_n, \ldots, a_1 \in R\right\} \subseteq R[X]$ ist ein Ideal.

(iii) Sei $a \in R$. Dann ist $(a) := \{r \cdot a \,|\, r \in R\}$ ein Ideal. Ideale dieser Form heißen **Hauptideale**.

(iv) Seien $a_1, \ldots, a_n \in R$. Dann ist $(a_1, \ldots, a_n) := \{r_1 a_1 + \ldots + r_n a_n \,|\, r_1, \ldots, r_n \in R\}$ ein Ideal.

(v) Sei $\psi : R \to S$ ein Ringhomomorphismus. Dann ist $\operatorname{Kern} \psi$ ein Ideal.

6.3 Bemerkung

Sei $I \subseteq R$ ein Ideal. Dann wird die Faktorgruppe R/I (bezüglich $+$) zu einem Ring durch $(r+I)(s+I) := r \cdot s + I$. Dies ist wohldefiniert: Seien $r + I = r' + I$ und $s + I = s' + I$. Dann $r - r', s - s' \in I$.

$$r's' + I = (r + (r' - r))(s + (s' - s)) + I = rs + \underbrace{r(s' - s)}_{\in I} + \underbrace{(r' - r)s}_{\in I} + \underbrace{(r' - r)(s' - s)}_{\in I} + I = r \cdot s + I$$

R/I heißt der **Faktorring** oder der **Quotientenring**.

6.4 Bemerkung

Sei $I \subseteq R$ ein Ideal. Dann ist $\pi : R \to R/I$ mit $\pi(r) := r + I$ ein Ringhomomorphismus mit $\operatorname{Kern} \pi = I$.

6.5 Homomorphiesatz

Sei $\psi : R \to S$ ein Ringhomomorphismus und $I \subseteq R$ ein Ideal. Gilt $I \subseteq \operatorname{Kern} \psi$ so gibt es einen eindeutigen Ringhomomorphismus $\overline{\psi} : R/I \to S$ mit $\psi = \overline{\psi} \circ \pi$.

Es gilt $\operatorname{Kern} \overline{\psi} = \pi(\operatorname{Kern} \psi)$ und $\operatorname{Bild} \overline{\psi} = \operatorname{Bild} \psi$. Insbesondere ist $\overline{\psi}$ ein Isomorphismus, falls ψ surjektiv und $\operatorname{Kern} \psi = I$ ist. Es ist $\overline{\psi}(r + I) = \psi(r)$.

$$\begin{tikzcd} R \arrow[r, "\psi"] \arrow[d, "\pi"'] & S \\ R/I \arrow[ur, dashed, "\overline{\psi}"'] & \end{tikzcd}$$

Beweis
Übung!

6.6 Korollar

Ist $\psi : R \to S$ ein Ringhomomorphismus, so gilt $\operatorname{Bild} \psi \cong R/\operatorname{Kern} \psi$. Ist ψ surjektiv, so gilt $S \cong R/\operatorname{Kern} \psi$.

6.7 Definition

Ein **Hauptidealring** ist ein nullteilerfreier Ring, in dem jedes Ideal ein Hauptideal ist.

6.8 Beispiel

$\mathbb{Z}$ ist ein Hauptidealring. Die Ideale sind die $n\mathbb{Z}$.

6.9 Satz

Sei K ein Körper. Dann ist $K[X]$ ein Hauptidealring.

Beweis
Sei $I \subseteq K[X]$ ein Ideal. Ist $I = \{0\}$, so ist nichts zu zeigen. Sei also $I \neq \{0\}$. Wähle $f \in I \setminus \{0\}$ von minimalem Grad. Behauptung: $I = (f)$. Sei $g \in I$. Division mit Rest liefert $g = q \cdot f + r$ wobei r kleineren Grad als f hat. Es ist aber $r = g - q \cdot f \in I$. Also folgt $r = 0$, da f minimal war. Also $g = q \cdot f \in (f)$. $\square$

6.10 Beispiel

$\mathbb{Z}[X]$ ist kein Hauptidealring: $(2X)$ ist kein Hauptideal in $\mathbb{Z}[X]$.

6.11 Definition

Sei R ein Ring und $I \subseteq R$ ein Ideal.

(i) I heißt **prim** oder ein **Primideal**, wenn $I \subsetneq R$ und für $r, s \in R$ gilt:

$$r \cdot s \in I \Longrightarrow r \in I \text{ oder } s \in I$$

(ii) I heißt **maximal**, wenn $I \subsetneq R$ und es kein Ideal J gibt mit $I \subsetneq J \subsetneq R$.

6.12 Bemerkung

$(0) = \{0\}$ ist genau dann ein Primideal, wenn R nullteilerfrei ist.

6.13 Lemma

$(0) = \{0\}$ ist genau dann maximal, wenn R ein Körper ist.

Beweis
Ist R ein Körper, so sind $\{0\}$ und R die einzigen Ideale in R (Ist $r \in I$ mit $r \neq 0$, also $s = (s \cdot r^{-1})r \in I$ für alle $s \in R$. Also $I = R$). Sei umgekehrt (0) ein maximales Ideal. Sei $r \in R \setminus \{0\}$. Zu zeigen: r ist invertierbar in R. Betrachte das Ideal (r). Es ist $(0) \subsetneq (r)$, da $r \in (r)$. (0) maximal $\Rightarrow (r) = R$. Also $1 \in (r)$. Also $\exists s \in R$ mit $1 = s \cdot r$. Also $r^{-1} = s \in R$. $\square$

6.14 Beispiel

Sei $(0) \neq \underset{\neq \mathbb{Z}}{I} = n\mathbb{Z} \subseteq \mathbb{Z}$ ein Ideal. Dann gilt $n\mathbb{Z}$ ist maximal $\iff$ n ist Primzahl $\iff$ ist ein Primideal.

Beweis
Für n, m gilt

$$n \text{ teilt } m \iff mZ \subseteq n\mathbb{Z}$$

Ist n eine Primzahl und $n\mathbb{Z} \subseteq k\mathbb{Z}$. Dann folgt k teilt n. Ist n eine Primzahl so folgt $k \in \{\pm n, \pm 1\}$. Also $k\mathbb{Z} \in \{\mathbb{Z}, n\mathbb{Z}\}$. Sei weiter n eine Primzahl und $r \cdot s \in n\mathbb{Z}$. Dann teilt n das Produkt $r \cdot s$. Da n eine Primzahl ist, muss n r oder s teilen. Also $r \in n\mathbb{Z}$ oder $s \in n\mathbb{Z}$. $\square$

6.15 Satz

Sei R ein Ring und $I \subsetneq R$ ein Ideal. Dann gilt:

(i) I ist prim $\iff$ R/I ist nullteilerfrei

(ii) I ist maximal $\iff$ R/I ist ein Körper.

Beweis

(i) Sei I prim. Sei $(r+I)(s+I) = 0 \in R/I$. Dann $r \cdot s + I = 0 \in R/I$, also $r \cdot s \in I$. Mit I prim folgt $r \in I$ oder $s \in I$. $\Rightarrow r + I = 0$ oder $s + I = 0$.

Sei R/I nullteilerfrei. Sei $r \cdot s \in I$. Dann $(r+I)(s+I) = r \cdot s + I = 0 \in R/I$. Da R/I nullteilerfrei ist, folgt: $r + I = 0$ oder $s + I = 0 \Rightarrow r \in I$ oder $s \in I$. □

(ii) Sei I maximal. Sei $a + I \in R/I$, $a + I \neq 0 \in R/I$, also $a \notin I$. Gesucht ist ein multiplikatives Inverses zu $a+I$, also ein $b \in R$ mit $ab + I = 1 + I$. Nun ist $(I, a) := \{s + r \cdot a \,|\, s \in I, r \in R\}$ ein Ideal mit $I \subsetneq (I, a) \subseteq R$. Da I maximal ist, folgt $(I, a) = R$. Da dann $1 \in (I, a)$ folgt $1 = s + b \cdot a$ mit $s \in I$ und $b \in R$. Also $a \cdot b + I = 1 + I$.

Sei R/I ein Körper. Sei $J \subsetneq R$ ein Ideal mit $I \subsetneq J$. Dann ist $\overline{J} = \{j + I \,|\, j \in J\}$ ein Ideal in R/I. Da $J \neq I$ ist $\overline{J} \neq \{0 + I\}$. Es folgt $\overline{J} = R/I$ und damit $J = R$. □

6.16 Bemerkung

Seien $I, J \subseteq R$ Ideale

(i) $I \cap J$ ist ein Ideal.

(ii) $I \cup J$ ist nicht immer ein Ideal.

(iii) $I + J := \{a + b \,|\, a \in I, b \in J\}$ ist ein Ideal. Es ist das kleinste Ideal, das I und J enthält.

Gilt $I + J = R$, so heißen I und J **koprim**.

6.17 Beispiel

Betrachte $\mathbb{Z}$, dann gilt: $I := n\mathbb{Z}$, $J := m\mathbb{Z}$ sind genau dann koprim, wenn n und m teilerfremd sind. Allgemeiner gilt:

$$n\mathbb{Z} + m\mathbb{Z} = \mathrm{ggT}(n, m)\mathbb{Z} \quad \text{und} \quad n\mathbb{Z} \cap m\mathbb{Z} = \mathrm{kgV}(n, m)\mathbb{Z}$$

6.18 Chinesischer Restsatz

Seien $I_1, \ldots, I_n \subseteq R$ Ideale, die paarweise koprim sind, also $I_i + I_j = R$ für $i \neq j$. Dann ist $\psi : R \to R/I_1 \times \ldots \times R/I_n$ mit $\psi(x) := (x + I_1, \ldots, x + I_n)$ surjektiv und induziert einen Isomorphismus

$$R/I_1 \cap \ldots \cap I_n = R/\mathrm{Kern}\,\psi \cong R/I_1 \times \ldots \times R/I_n$$

Beweis für $n = 2$

Da $I_1 + I_2 = R$ gibt es $a_1 \in I_1$ und $a_2 \in I_2$ mit $a_1 + a_2 = 1$. Seien $r_1 + I_1 \in R/I_1$ und $r_2 + I_2 \in R/I_2$ gegeben. Gesucht ist $r \in R$ mit $r + I_1 = r_1 + I_1$, $r + I_2 = r_2 + I_2$. Betrachte $r := r_1 a_2 + r_2 a_1$. Dann gilt

$$r + I_1 = r_1 \cdot a_2 + r_2 \cdot a_1 + I_1 = r_1 \cdot a_2 + I_1 = r_1 \cdot a_2 + r_1 \cdot a_1 + I_1 = r_1(a_2 + a_1) + I_1 = r_1 + I_1$$
$$r + I_2 = r_1 \cdot a_2 + r_2 \cdot a_1 + I_2 = r_2 \cdot a_1 + I_2 = r_2 \cdot a_1 + r_2 \cdot a_2 + I_2 = r_2(a_1 + a_2) + I_2 = r_2 + I_2$$

Also ist ψ surjektiv. Da $\mathrm{Kern}\,\psi = I_1 \cap \ldots \cap I_n$ folgt der Rest aus dem Homomorphiesatz. □

Beweis für allgemeines $n \in \mathbb{N}$
Nach Lemma 6.19 gibt es $d_j \in I_j$, $e_j \in J_j$ mit $d_j + e_j = 1$. Es folgt

$$e_j + I_i = \begin{cases} 0 + I_i = 0 \in R/I_i, & \text{falls } i \neq j \\ e_j + d_j + I_j = 1 + I_j = 1 \in R/I_j, & \text{falls } i = j \end{cases}$$

Sei $a_1, \ldots, a_n \in R$. Setze $x := a_1 \cdot e_1 + a_2 \cdot e_2 + \ldots + a_n \cdot e_n$. Dann gilt

$$x + I_j = (a_1e_1 + I_j) + (a_2e_2 + I_j) + \ldots + (a_ne_n + I_j) = a_je_j + I_j = a_j + I_j.$$

Also $\psi(x) = (a_1 + I_1, a_2 + I_2, \ldots, a_n + I_n)$. Damit ist ψ surjektiv. □

6.19 Lemma

Seien $I_1, \ldots, I_n \subseteq R$ paarweise koprime Ideale. Für $j \in \{1, \ldots, n\}$ sei $J_j := \bigcap_{i \neq j} I_i$. Dann sind I_j und J_j koprim.

Beweis
Da I_j koprim zu I_i für $i \neq j$, gibt es $a_i \in I_i$, $a_i' \in I_j$ mit $1 = a_i + a_i'$. Dann gilt $1 = \prod_{i \neq j}(a_1 + a_i') \in I_j + J_j$. Also $R = I_j + J_j$ und I_j und J_j sind koprim.

6.20 Korollar

Seien $a_1, \ldots, a_n \in \mathbb{Z}$ paarweise teilerfremd. Seien $x_1, \ldots, x_n \in \mathbb{Z}$ beliebig. Dann gibt es eine Lösung $x \in \mathbb{Z}$ für die gemeinsamen Kongruenzen

$$x \equiv x_i \mod a_i \qquad :\Leftrightarrow x + a_i\mathbb{Z} = x_i + a_i\mathbb{Z}$$

Die Menge aller Lösungen von ($\star$) ist $x + a_1 \cdot \ldots \cdot a_n\mathbb{Z}$

Beweis
Betrachte $\psi : \mathbb{Z} \to \mathbb{Z}/a_1\mathbb{Z} \times \ldots \times \mathbb{Z}/a_n\mathbb{Z}$, $x \mapsto (x + a_1\mathbb{Z}, \ldots, x + a_n\mathbb{Z})$. Dann erfüllt x die Kongruenzen ($\star$) genau dann wenn

$$\psi(x) = (x_1 + a_1\mathbb{Z}, \ldots, x_n + a_n\mathbb{Z})$$

gilt. Da ψ surjektiv ist, gibt es ein solches x. Alle weiteren Lösungen sind von der Form $x + y$ mit $y \in \operatorname{Kern} \psi$. □

6.21 Beispiel

Suche $x \in \mathbb{Z}$ mit $x \equiv 1 \mod 3$, $x \equiv 2 \mod 4$, $x \equiv 1 \mod 5$.

$$1 = \underset{\in 3\mathbb{Z}}{(21)} + \underset{\in 4\mathbb{Z},5\mathbb{Z}}{(-20)} = \underset{\in 4\mathbb{Z}}{(16)} + \underset{\in 3\mathbb{Z},5\mathbb{Z}}{(-15)} = \underset{\in 5\mathbb{Z}}{(25)} + \underset{\in 3\mathbb{Z},4\mathbb{Z}}{(-24)}$$
$$x := 1 \cdot (-20) + 2 \cdot (-15) + 1 \cdot (-24) = -20 - 30 - 24 = -74$$

7 Primfaktorzerlegung

In Kapitel 7 sei R immer ein kommutativer nullteilerfreier Ring.

7.1 Definition

$$R^\times := \{\varepsilon \in R \,|\, \exists \delta \in R \text{ mit } \varepsilon \cdot \delta = 1\}$$

heißt die Gruppe der **Einheiten**.

7.2 Definition

Seien $a, b \in R$. Wir sagen a teilt b, falls es ein $x \in R$ gibt mit $b = a \cdot x$. Wir schreiben dafür auch $a \mid b$.

7.3 Bemerkung

Für $a, b \in R$, $\delta, \varepsilon \in R^\times$ gilt: $a \mid b \iff \varepsilon \cdot a \mid \delta \cdot b$.

7.4 Definition

Sei $p \in R \setminus (R^\times \cup \{0\})$

i) p heißt **irreduzibel**, falls gilt $p = a \cdot b$ mit $a, b \in R \Longrightarrow a \in R^\times$ oder $b \in R^\times$

ii) p heißt **prim** oder ein **Primelement**, falls gilt:

$$p \mid a \cdot b \text{ mit } a, b \in R \Longrightarrow p \mid a \text{ oder } p \mid b$$

7.5 Bemerkung

Für $n \in \mathbb{Z} \setminus \{-1, 0, 1\}$. n ist prim $\Leftrightarrow n$ ist eine Primzahl $\iff$ n ist irreduzibel.

7.6 Lemma

Sei $p \in R \setminus (R^\times \cup \{0\})$.

i) p ist prim $\iff$ (p) ist Primideal.

ii) p ist prim $\Longrightarrow p$ ist irreduzibel.

Beweis

i) Ist klar, da $a \in (p) \iff p \mid a$.

ii) Sei p prim und $p = a \cdot b$. Insbesondere $p \mid a \cdot b$ und es folgt $p \mid a$ oder $p \mid b$. O.B.d.A: $p \mid a$. Also $p \cdot r = a$ für ein $r \in R$. Es folgt $p = a \cdot b = p \cdot r \cdot b$, also $1 = r \cdot b$, also $b \in R^\times$. $\square$

7.7 Bemerkung

Ist R ein Hauptidealring, so gilt auch "irreduzibel $\Rightarrow$ prim". Im Allgemeinen ist das aber nicht richtig.

7.8 Definition

R heißt **faktoriell**, falls sich jedes $r \in R \setminus (R^\times \cup \{0\})$ als Produkt von Primelementen schreiben lässt.

7.9 Bemerkung

Hauptidealringe sind faktoriell (LA2). Insbesondere ist $K[X]$ faktoriell, falls K ein Körper ist.

7.10 Lemma

Sei R ein faktorieller Ring und $p \in R \setminus (R^\times \cup \{0\})$. Dann gilt: p prim $\iff$ p irreduzibel.

Beweis
"$\Rightarrow$": ist sowieso richtig

"$\Leftarrow$": Sei p irreduzibel. Aus R faktoriell folgt $p = q_1 \cdot \ldots \cdot q_n$ mit $q_1, \ldots, q_n$ Primelementen. Insbesondere $q_i \notin R^\times$. Da p irreduzibel ist, folgt $n = 1$ und $p = q_1$ ist prim. □

7.11 Lemma (Eindeutigkeit der Primfaktorzerlegung)

Sei R faktoriell. Sind $p_1, \ldots, p_n$ und $q_1, \ldots, q_m$ Primelemente mit $p_1 \cdot \ldots \cdot p_n = q_1 \cdot \ldots \cdot q_m$ so gilt $n = m$. Weiter gibt es Einheiten $\varepsilon_1, \ldots, \varepsilon_n$ sodass nach Umordnung $p_i = \varepsilon_i \cdot q_i$ für $i = 1, \ldots, n$.

Beweis
Aus $p_1 \mid q_1 \cdots q_m$ folgt, möglicherweise nach Umnummerierung, $p_1 \mid q_1$. Da q_1 irreduzibel ist, folgt $q_1 = \varepsilon_1 \cdot p_1$. Weiter folgt $p_2 \cdot \ldots \cdot p_n = (\varepsilon_1 \cdot q_2) \cdot \ldots \cdot q_m$. Per Induktion über die Anzahl der Faktoren folgt $n = m$ und $q_i = \varepsilon_i p_i$ mit Einheiten ε_i. □

etwas –Zitat– "sloppy" …:D

7.12 Beispiele

(i) $\mathbb{Z}^\times = \{-1, 1\}$, K Körper $K^\times = K \setminus \{0\}$. $K[X]^\times = K^\times$. R Ring $R[X]^\times = R^\times$.

(ii) In $K[X]$, K Körper ist $(X - \alpha)$ für alle $\alpha \in K$ irreduzibel, also prim.
(Beweis: $X - \alpha \mid f \in K[X] \iff f(\alpha) = 0$)

(iii) In $\mathbb{R}[X]$ ist $X^2 + 1$ irreduzibel (also prim)

Was ist $\mathbb{R}[X]/(X^2+1)$?

7.13 Definition

Sei R ein Ring und $a_1, \ldots, a_n \in R$

i) $d \in R$ heißt ein **größter gemeinsamer Teiler (**ggT**)** von $a_1, \ldots, a_n$ falls gilt:
   (a) $d \mid a_i$ für $i = 1, \ldots, n$
   (b) Ist $d' \in R$ mit $d' \mid a_i$ für $i = 1, \ldots, n$, so gilt $d' \mid d$.

ii) $v \in R$ heißt ein **kleinstes gemeinsames Vielfaches (**kgV**)** von $a_1, \ldots, a_n$ falls gilt:
   (a) $a_i \mid v$ für $i = 1, \ldots, n$
   (b) Ist $v' \in R$ mit $a_i \mid v'$ für $i = 1, \ldots, n$, so gilt $v \mid v'$.

7.14 Bemerkung

In beliebigen Ringen müssen weder kgV noch ggT existieren. Falls $\mathrm{kgV}(a_1, \ldots, a_n)$ existiert, so ist es auch eindeutig bis auf Multiplikation mit einer Einheit. Ebenso für ggT.

In faktoriellen Ringen existieren kgV und ggT immer und können über die Primfaktorzerlegung bestimmt werden.

7.15 Satz

Sei R ein Hauptidealring und $a_1, \dots, a_n \in R$

i) Wenn $(d) = (a_1, \dots, a_n)$, so ist d ein ggT von $a_1, \dots, a_n$

ii) Wenn $(v) = (a_1) \cap (a_2) \cap \ldots \cap (a_n)$, so ist v ein kgV von $a_1, \dots, a_n$

Beweis

i) Da $a_i \in (a_1, \dots, a_n) = (d) = \{x \cdot d \,|\, x \in R\}$ gilt $d \mid a_i$ für alle i. Sei d' ein weiterer gemeinsamer Teiler. Dann $a_i \in (d')$ für $i = 1, \dots, n$. Es folgt $(d) = (a_1, \dots, a_n) \subseteq (d')$. Es folgt $d \in (d')$, also $d' \mid d$.

ii) Übung

7.16 Bemerkung

$a \mid b \iff b \in (a)$.

7.17 Euklidischer Algorithmus

Seien $f_1, f_2 \in K[X]$, $f_2 \neq 0$. Durch wiederholte Division mit Rest erhalten wir:

$$\begin{aligned} f_1 &= q_1 \cdot f_2 + f_3 \qquad && d(f_3) < d(f_2) \\ f_2 &= q_2 \cdot f_3 + f_4 && d(f_4) < d(f_3) \\ &\vdots \\ f_n &= q_n \cdot f_{n+1} \end{aligned}$$

7.18 Lemma

$f_{n+1} = \mathrm{ggT}(f_1, f_2)$

Beweis

Den Algorithmus aufsteigend sehen wir, dass f_{n+1} alle f_i teilt. Insbesondere ist f_{n+1} ein gemeinsamer Teiler von f_1 und f_2. Ist d' ein weiterer gemeinsamer Teiler von f_1 und f_2, so sehen wir, indem wir dem Algorithmus absteigend folgen, dass d' alle f_i teilt. Insbesondere gilt $d' \mid f_{n+1}$. Damit ist $f_{n+1} = \mathrm{ggT}(f_1, f_2)$. □

8 Satz von Gauß

Sei R in 8 immer nullteilerfrei, mit 1 und kommutativ.

8.1 Satz von Gauß

Sei R faktoriell. Dann ist auch $R[X]$ faktoriell.

8.2 Bemerkung

Im Beweis benutzen wir, dass $K[X]$ faktoriell ist, falls K ein Körper ist.

8.3 Bemerkung

Sei $f \in \mathbb{Q}[X]$. Dann gibt es $c \in \mathbb{Z}$ mit $\tilde{f} := c \cdot f \in \mathbb{Z}[X]$. Für jede Primzahl p induziert $\mathbb{Z} \to {}^{\mathbb{Z}}\!/\!_{p\mathbb{Z}}$ einen Ringhomomorphismus $\Phi : Z[X] \to {}^{\mathbb{Z}}\!/\!_{p\mathbb{Z}}[X]$ mit $\sum_{n=1}^{N} a_n X^n \mapsto \sum_{n=1}^{N} (a_n + p\mathbb{Z}) X^n$.

8.4 Konstruktion (Körper aus einem Ring)

Sei $B = R \times R \setminus \{0\}$. Auf B betrachten wir die Äquivalenzrelation

$$(z, n) \sim (z', n') :\Leftrightarrow n' \cdot z = n \cdot z'.$$

Transitivität: $(z, n) \sim (z', n') \sim (z'', n'')$. Dann gilt

$$n'' \cdot z \cdot n' = n'' \cdot z' \cdot n = n' \cdot z'' \cdot n.$$

Da R nullteilerfrei ist, folgt $n'' \cdot z = z'' \cdot n \Rightarrow (z, n) \sim (z'', n'')$. Wir schreiben nun $\frac{z}{n}$ für die Äquivalenzklasse von (z, n) bezüglich dieser Äquivalenzrelation und $Q(R)$ für die Menge der Äquivalenzklassen.

8.5 Lemma

Durch $\frac{z}{n} + \frac{z'}{n'} := \frac{n' \cdot z + n \cdot z'}{n \cdot n'}$ und $\frac{z}{n} \cdot \frac{z'}{n'} := \frac{z \cdot z'}{n \cdot n'}$ wird $Q(R)$ zu einem Körper.

Beweis
Nachrechnen.

8.6 Definition

$Q(R)$ heißt der **Quotientenkörper** von R.
Beispiel: $Q(\mathbb{Z}) = \mathbb{Q}$

8.7 Bemerkung

Die Abbildung $i : R \to Q(R)$ mit $i(r) := \frac{r}{1}$ ist ein injektiver Ringhomomorphismus. Wir unterscheiden oft nicht zwischen r und $i(r) = \frac{r}{1}$ und fassen R als Unterring von $Q(R)$ auf.

8.8 Definition

Eine Menge $P \subseteq R$ von Primelementen heißt ein **Repräsentantensystem** der Primelemente, falls es zu jedem Primelement $q \in R$ ein eindeutiges $p \in P$ gibt und $\varepsilon \in R^{\times}$ mit $q = \varepsilon \cdot p$.

8.9 Beispiel

i) Die (positiven) Primzahlen $P = \{2, 3, 5, 7, 11, \dots\}$ sind ein Repräsentantensystem für die Primzahlen in $\mathbb{Z}$.

ii) Die Polynome $\{(X - \alpha) \mid \alpha \in \mathbb{C}\}$ sind ein Repräsentantensystem für die Primelemente in $\mathbb{C}[X]$.

8.10 Bemerkung

Sei $P \subseteq R$ ein Repräsentantensystem der Primelemente. Sei R faktoriell.

i) Jedes $a \in R \setminus \{0\}$ lässt sich eindeutig schreiben als

$$a = \varepsilon \cdot \prod_{p \in P} p^{v_p(a)}$$

wobei $\varepsilon \in R^\times$ und $v_p(a) \in \mathbb{N}_{\geq 0}$, $v_p(a) = 0$ für fast alle $p \in P$.

ii) Jedes $x \in Q(R) \setminus \{0\}$ lässt sich eindeutig schreiben als

$$x = \varepsilon \cdot \prod_{p \in P} p^{v_p(x)}$$

wobei $\varepsilon \in R^\times$, $v_p(x) \in \mathbb{Z}$ und $v_p(x) = 0$ für fast alle $p \in P$. Wir setzen $v_p(0) := \infty$.

8.11 Definition

Sei $f = a_n X^n + a_{n-1} X^{n-1} + \dots + a_1 X + a_0 \in Q(R)[X]$. $f \neq 0$, wobei R faktoriell ist. Dann setzen wir für $p \in P$

$$v_p(f) := \min_{i=0,\dots,n} v_p(a_i) \quad , \quad v_p(0) := \infty$$

8.12 Bemerkung

$f \in R[X] \iff v_p(f) \geq 0 \; \forall p \in P$.

8.13 Lemma von Gauß

Sei R faktoriell und $p \in R$ prim. Für $f, g \in Q(R)[X]$ gilt dann:

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

Beweis
Wir betrachten zunächst mehrere Spezialfälle:

(1) $f = a, g = b \in Q(R)$. Dann ist $(\star)$ klar.

(2) $f = a \in Q(R), g = b_n X^n + \dots + b_0 \in Q(R)[X]$. Dann gilt

$$v_p(a \cdot g) = v_p(ab_n X^n + \dots + ab_0) = \min_i v_p(a \cdot b_i) = \min_i (v_p(a) + v_p(b_i)) = v_p(a) + v_p(g).$$

(3) $f = 0$ oder $g = 0$ ist auch klar.

(4) $f, g \in R[X]$ mit $v_p(f) = v_p(g) = 0$.
Wir schreiben R_p für das von p erzeugte Hauptideal in R und $R[X]_p$ für das von p erzeugte Hauptideal in $R[X]$. Betrachte den durch $R \to {}^{R}/_{R_p}$ induzierten Ringhomomorphismus $\Phi : R[X] \to {}^{R}/_{R_p}[X]$. Es gilt

$$\operatorname{Kern}\Phi = \{h \in R[X] \mid p \text{ teilt alle Koeffizienten von } h\} \cup \{0\} = \{h \in R[X] \mid v_p(h) > 0\} \cup \{0\}.$$

Wegen $v_p(f) = v_p(g) = 0$ folgt $\Phi(f) \neq 0 \neq \Phi(g)$. Es ist $\Phi(f \cdot g) = \Phi(f) \cdot \Phi(g)$ $(\#)$
p ist prim in $R \Rightarrow R_p \subseteq R$ ist Primideal $\Rightarrow {}^{R}/_{R_p}$ nullteilerfrei $\Rightarrow {}^{R}/_{R_p}[X]$ ist nullteilerfrei. Also $(\#) \Rightarrow \Phi(f \cdot g) \neq 0$ da $\Phi(f) \neq 0 \neq \Phi(g)$. Es folgt also $f, g \notin \operatorname{Kern}\Phi \Rightarrow v_p(f \cdot g) = 0$.

Seien nun $f = a_n X^n + \ldots + a_0, g = b_m X^m + \ldots + b_0 \in Q(R)[X]$, $f, g \neq 0$ aber sonst beliebig. Sei $A \in R$ das Produkt der Nenner der a_i und $B \in R$ das Produkt der Nenner der b_i. Dann $A \cdot f, B \cdot g \in R[X]$. Setze $N := -v_p(A \cdot f), M := -v_p(B \cdot g)$. Mit (2) folgt:

$$v_p(p^N \cdot A \cdot f) = v_p(p^N) + v_p(A \cdot f) = N + v_p(A \cdot f) = 0 \qquad v_p(p^M \cdot B \cdot g) = 0$$

(4) liefert

$$v_p\big((p^N \cdot A \cdot f)(p^M \cdot B \cdot g)\big) = v_p(p^N \cdot A \cdot f) + v_p(p^M \cdot B \cdot g)$$

mit (2) folgt

$$\begin{aligned} v_p(p^N \cdot A \cdot f \cdot p^M \cdot B \cdot g) &= v_p(p^N) + v_p(A) + v_p(B) + v_p(p^M) + v_p(f \cdot g) \\ v_p(p^N \cdot A \cdot f) &= v_p(p^N) + v_p(A) + v_p(f) \\ v_p(p^M \cdot B \cdot g) &= v_p(B) + v_p(p^M) + v_p(g) \end{aligned}$$

$(\star\star)$ liefert $v_p(f \cdot g) = v_p(f) + v_p(g)$ □

8.14 Korollar

Sei R faktoriell und $h = X^n + a_{n-1}X^{n-1} + \ldots + a_0 \in R[X]$ ein normiertes Polynom. Ist $h = f \cdot g$ mit $f, g \in Q(R)[X]$ beide normiert so gilt $f, g \in R[X]$.

Beweis
Zu zeigen: $v_p(f), v_p(g) \geq 0$ für alle Primelemente $p \in R$. Da f, g und h normiert sind, gilt $v_p(f), v_p(g), v_p(h) \leq 0$. Wegen $h \in R[X]$ folgt $v_p(h) = 0$. Mit dem Gauß-Lemma folgt:

$$0 = v_p(h) = v_p(f \cdot g) = v_p(f) + v_p(g)$$

Also $v_p(f) = v_p(g) = 0$. □

8.15 Definition

Sei R faktoriell. $f = a_n X^n + a_{n-1}X^{n-1} + \ldots + a_0 \in R[X]$ heißt **primitiv**, wenn $\operatorname{ggT}(a_n, \ldots, a_0) = 1$ ist.

8.16 Bemerkung

(1) Normierte Polynome sind primitiv.

(2) $f \in R[X]$ ist primitiv $\iff$ $\forall p \in R$ prim gilt $v_p(f) = 0$

(3) Jedes $f \in Q(R)[X]$, $f \neq 0$ lässt sich faktorisieren als $f = a \cdot \tilde{f}$ mit $a \in Q(R)$ und $\tilde{f} \in R[X]$ primitiv:

$$a := \prod_{p \in P} p^{v_p(f)} \quad , \quad \tilde{f} = a^{-1} \cdot f.$$

Bsp: $\frac{3}{2}X^2 + \frac{3}{7}X + \frac{9}{2} = \frac{1}{14}(21X^2 + 6X + 63) = \frac{3}{14}(7X^2 + 2X + 21)$

8.17 Proposition

Sei R faktoriell

i) Jedes Primelement $p \in R$ ist auch ein Primelement in $R[X]$.

ii) Sei $q \in R[X]$ primitiv und ein Primelement in $Q(R)[X]$. Dann ist q auch prim in $R[X]$.

iii) Jedes $f \in R[X] \setminus (R^\times \cup \{0\})$ lässt sich faktorisieren als $f = p_1 \cdot \ldots \cdot p_n \cdot q_1 \cdot \ldots \cdot q_m$ mit $p_1, \ldots, p_n \in R$ prim und $q_1, \ldots, q_m \in R[X]$ primitiv und prim in $Q(R)[X]$.

Beweis

i) Sei $\Phi : R[X] \to {}^{R}/_{Rp}[X]$ der von $R \to {}^{R}/_{Rp}$ induzierte Ringhomomorphismus. Dann liegt $f \in R[X]$ genau dann im $\mathrm{Kern}\,\Phi$ wenn alle Koeffizienten von f durch p geteilt werden. Also $\mathrm{Kern}\,\Phi = R[X]p$. Mit dem Homomorphiesatz folgt:

$$^{R[X]}/_{R[X]p} \cong {}^{R}/_{Rp}[X]$$

p prim $\Rightarrow Rp \subseteq P$ Primideal $\Rightarrow {}^{R}/_{Rp}$ nullteilerfrei $\Rightarrow {}^{R}/_{Rp}[X]$ nullteilerfrei. Daraus folgt $^{R[X]}/_{R[X]p}$ nullteilerfrei, also ist $R[X]p \subseteq R[X]$ ein Primideal. Damit folgt $p \in R[X]$ ist Primelement.

ii) Seien $f, g \in R[X]$ mit $q \mid f \cdot g$ in $R[X]$. Damit teilt q auch $f \cdot g$ in $Q(R)[X]$. Da q prim ist in $Q(R)[X]$ folgt $q \mid f$ oder $q \mid g$ in $Q(R)[X]$. O.B.d.A. $q \mid f$. Also $f = q \cdot h$ mit $h \in Q(R)[X]$. Sei $p \in R$ prim. Mit dem Lemma von Gauß folgt

$$0 \leq v_p(f) = v_p(q) + v_p(h) = v_p(h)$$

da q primitiv

Also ist $v_p(h) \geq 0$ für alle p. Damit $h \in R[X]$. Es folgt $q \mid f$ schon in $R[X]$.

iii) Sei $f = a \cdot \tilde{f}$ mit $a = \mathrm{ggT}$ der Koeffizienten von f. Dann ist $\tilde{f} \in R[X]$ primitiv. Da R faktoriell ist, gibt es Primelemente $p_1, \ldots, p_n \in R$ mit $a = p_1, \ldots, p_n$. Da $Q(R)[X]$ faktoriell ist, gibt es $\tilde{f}_1, \ldots, \tilde{f}_m \in Q(R)[X]$ prim mit

$Q(R)$ Körper $\Rightarrow$ $Q(R)[X]$ HIR

$$\tilde{f} = \tilde{f}_1 \cdot \ldots \cdot \tilde{f}_m.$$

Jedes $\tilde{f}_i$ lässt sich schreiben als $\tilde{f}_i = c_i \cdot q_i$ mit $c_i \in Q(R)$ und $q_i \in R[X]$ primitiv. Setze $c := c_1 \cdot \ldots \cdot c_m$. Es folgt $\tilde{f} = c \cdot q_1 \cdot \ldots \cdot q_m$. Mit $\tilde{f}_i$ ist auch q_i prim $\in Q(R)[X]$. Es bleibt zu zeigen: $c \in R^\times$.

Sei $p \in R$ prim. Dann

$$0 = v_p(\tilde{f}) = v_p(c) + v_p(q_1) + \ldots + v_p(q_m) = v_p(c)$$

Also $v_p(c) = 0$ für alle $p \in R$ prim. Damit ist $c \in R^\times$. $\square$

8.18 Beweis des Satz von Gauß

Um zu zeigen, dass $R[X]$ faktoriell ist, müssen wir zeigen, dass sich jedes $f \in R[X] \setminus (R^\times \cup \{0\})$ als Produkt von Primelementen schreiben lässt. Dies folgt sofort aus der Proposition 8.17. $\square$

8.19 Korollar

Sei R faktoriell. Dann ist $q \in R[X]$ genau dann prim wenn

i) $q \in R$ prim in R, <u>oder</u>

ii) $q \in R[X]$ primitiv und prim in $Q(R)[X]$.

Beweis

Nach i) und ii) in Proposition 8.17 sind die Elemente aus i) und ii) im Korollar prim in $R[X]$. Ist $q \in R[X]$ prim, so lässt sich wie in iii) der Proposition faktorisieren. Da q prim ist, besteht diese Faktorisierung nur aus einem Element. $\square$

9 Irreduzible Polynome

Sei in Kapitel 9 R immer faktoriell und $K := Q(R)$

9.1 Beispiel

i) Sei K ein Körper. Dann sind alle Polynome vom Grad 1 irreduzibel.

ii) Ist K algebraisch abgeschlossen, so sind die Polynome vom Grad 1 genau die irreduziblen Polynome.

iii) Die irreduziblen Polynome über $\mathbb{R}$ sind genau
   a) alle Polynome vom Grad 1 und
   b) alle Polynome vom Grad 2, die keine Nullstelle in $\mathbb{R}$ haben.

iv) Sei K ein Körper und $p \in K[X]$ mit $2 \leq d(p) \leq 3$. Dann ist p genau dann irreduzibel, wenn p keine Nullstelle in K hat.

v) $(X^2+1)^2 \in \mathbb{R}[X]$ ist nicht irreduzibel, aber besitzt keine Nullstelle in $\mathbb{R}$.

9.2 Bemerkung

Sei $f \in K[X] \setminus \{0\}$. Dann gibt es $c \in K^\times$ und $\tilde{f} \in R[X]$ primitiv mit $f = c \cdot \tilde{f}$. Es gilt Kapitel 8. f ist irreduzibel in $K[X] \iff \tilde{f}$ ist irreduzibel in $K[X] \iff \tilde{f}$ ist irreduzibel in $R[X]$.

9.3 Satz (Reduktionskriterium)

Sei $p \in R$ prim. Sei $f = a_nX^n + \ldots + a_0 \in R[X]$, $\operatorname{grad} f = n \geq 1$. Sei $\Phi : R[X] \to {}^{R}/_{Rp}[X]$ der von $R \to {}^{R}/_{Rp}$ induzierte Ringhomomorphismus. Weiter sei

(i) $p \nmid a_n$

(ii) $\Phi(f)$ irreduzibel in ${}^{R}/_{Rp}[X]$

Dann ist f irreduzibel in $K[X]$.

Beweis
Wir nehmen zunächst an, dass f primitiv ist. Dann genügt es zu zeigen, dass f irreduzibel in $R[X]$ ist. Sei also $f = g \cdot h$ mit $g, h \in R[X]$. Dann ist a_n das Produkt der höchsten Koeffizienten von g und h. Insbesondere teilt p keinen dieser Koeffizienten und es folgt $\operatorname{grad} g = \operatorname{grad} \Phi(g)$ und $\operatorname{grad} h = \operatorname{grad} \Phi(h)$. Da $\Phi(f) = \Phi(g) \cdot \Phi(h)$ irreduzibel ist, ist $\Phi(g) \in ({}^{R}/_{Rp})^\times$ oder $\Phi(h) \in ({}^{R}/_{Rp})^\times$. O.B.d.A $\Phi(g) \in ({}^{R}/_{Rp})^\times$. Insbesondere $\operatorname{grad}(\Phi(g)) = 0$. Also auch $\operatorname{grad}(g) = 0$. Also $g \in R$. Wegen $f = g \cdot h$ gilt $g \mid a_i \in R$ für $i = n, \ldots, 0$. Da f primitiv ist, folgt $g \in R^\times$.

Ist f nicht primitiv, so gilt $f = \operatorname{ggT}(a_i) \cdot \tilde{f}$ mit $\tilde{f} \in R[X]$ primitiv. Es genügt zu zeigen, dass $\tilde{f}$ irreduzibel ist. Mit $\Phi(f)$ ist auch $\Phi(\tilde{f})$ irreduzibel in ${}^{R}/_{Rp}[X]$. Sei $\tilde{a}_n$ der höchste Koeffizient von $\tilde{f}$. Dann ist $a_n = \operatorname{ggT}(a_i) \cdot \tilde{a}_n$. Da $p \nmid a_n$ folgt $p \nmid \tilde{a}_n$. Also können wir den ersten Teil des Beweises auf $\tilde{f}$ anwenden. Daher ist $\tilde{f}$ und damit auch f irreduzibel. $\square$

9.4 Beispiel

$f = 19X^3 + 17X + 15$ ist irreduzibel in $\mathbb{Q}[X]$ (und in $\mathbb{Z}[X]$): Das Bild von f unter $\Phi : \mathbb{Z}[X] \to {}^{\mathbb{Z}}/_{2\mathbb{Z}}[X]$ ist $\Phi(f) = X^3 + X + 1$ irreduzibel, da $\Phi(f)$ keine Nullstelle in ${}^{\mathbb{Z}}/_{2\mathbb{Z}}$ hat: $\Phi(f)(1) = 1 + 1 + 1 = 1 \neq 0$ und $\Phi(f)(0) = 0 + 0 + 1 = 1 \neq 0$.

9.5 Satz (Eisenstein)

Sei $f = a_n X^n + \ldots + a_0 \in R[X]$ ein primitives Polynom von $\operatorname{grad} f = n \geq 1$. Weiter sei $p \in R$ prim mit

(i) $p \nmid a_n$

(ii) $p \mid a_i$ für $i < n$

(iii) $p^2 \nmid a_0$

Dann ist f irreduzibel in $R[X]$ und damit auch in $K[X]$.

Beweis
Sei $f = g \cdot h$ mit $g, h \in R[X]$. Sei dabei $g = c_k X^k + \ldots + c_0$, $h = d_l X^l + \ldots + d_0$ mit $\operatorname{grad}(g) = k$, $\operatorname{grad}(h) = l$. Sei $\Phi : R[X] \to {}^{R}/_{R_p}[X]$ der von $R \to {}^{R}/_{Rp}$ induzierte Ringhomomorphismus. Für $\alpha \in R$ setze $\overline{\alpha} := \alpha + R_p \in {}^{R}/_{Rp}$. Es ist $\Phi(f) = \overline{a_n} X^n$ wegen ii). Da $\Phi(f) = \Phi(g) \cdot \Phi(h)$ folgt[2] $\Phi(g) = \overline{c_k} X^k$ und $\Phi(h) = \overline{d_l} X^l$.

Angenommen: $k \geq 1$ und $l \geq 1$. Dann folgt $\overline{c_o} = 0$ und $\overline{d_0} = 0$. Dann teilt p sowohl c_0 als auch d_0. Aber $p^2 \nmid a_0 = c_0 \cdot d_0$. $\lightning$

Es folgt $k = 0$ oder $l = 0$. O.B.d.A. $k = 0$. Also $g \in R$. Wegen $f = g \cdot h$ und f primitiv folgt $g \in R^\times$. Damit ist f irreduzibel. $\square$

9.6 Beispiel

$X^n + p \in \mathbb{Q}[X]$ für p eine Primzahl ist irreduzibel. Insbesondere gibt es in $\mathbb{Q}[X]$ irreduzible Polynome von beliebigem Grad ≥ 1.

9.7 Beispiel

Sei k ein Körper und $k(t) := Q(k[t])$ der **Körper der rationalen Funktionen** in einer Variablen t über k. Dann ist $f := X^n - t \in k(t)[X]$ irreduzibel. Es ist nämlich $k[t]$ faktoriell und $t \in k[t]$ prim. Also können wir das Kriterium von Eisenstein anwenden.

9.8 Beispiel

Sei p eine Primzahl. Behauptung: $f = X^{p-1} + X^{p-2} + \ldots + X + 1 = \frac{X^p - 1}{X - 1} \in \mathbb{Q}[X]$ ist irreduzibel. Wir zeigen $f(X+1) = \frac{(X+1)^p - 1}{(X+1) - 1} = X^{p-1} + \binom{p}{1} X^{p-2} + \ldots + \binom{p}{p-1}$ ist irreduzibel. Nun gilt $p \mid \binom{p}{r}$ für $r < p$ und $\binom{p}{1} = p$. Nach Eisenstein ist das irreduzibel.

9.9 Lemma

Sei $f = a_n X^n + a_{n-1} X^{n-1} + \ldots + a_0 \in K[X]$. Dann ist f genau dann irreduzibel, wenn

$$f(X+1) = a_n (X+1)^n + a_{n-1} (X+1)^{n-1} + \ldots + a_1 (X+1) + a_0$$

in $K[X]$ irreduzibel ist.

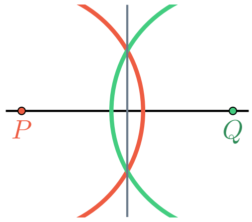
Beweis
Es ist $f \mapsto f(X+1)$ ein Ringisomorphismus von $K[X]$ (Das Inverse ist $f \mapsto f(X-1)$). Also ist f genau dann irreduzibel, wenn $f(X+1)$ irreduzibel ist. $\square$

[2] ist nur richtig, wenn ${}^{R}/_{Rp}[X]$ faktoriell, also wenn ${}^{R}/_{Rp}$ faktoriell ist. Wenn nicht betrachte $K := Q({}^{R}/_{Rp})$ (nullteilerfrei, da Rp Primideal) und ${}^{R}/_{Rp}[X] \subset K[X]$ und benutze die eindeutige Primfaktorzerlegung in $K[X]$.

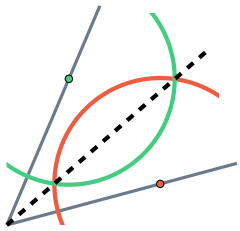
10 Konstruktion mit Zirkel und Lineal

10.1 Beispiel

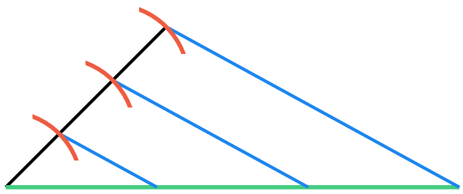
1) Sei en $P, Q \in \mathbb{R}^2$. Dann lässt sich der Mittelpunkt $M := \frac{P+Q}{2}$ zwischen P und Q mit Zirkel und Lineal konstruieren:



2) Winkelhalbierung



3) Drittelung einer Strecke:



10.2 Konstruktionsprobleme

(1) Winkeldrittellung

(2) Delische Problem: Würfelverdoppellung

(3) Quadratur des Kreises: $\mathrm{Vol}(\bigcirc) = \mathrm{Vol}(\square)$

(4) Konstruktion des regelmäßigen n-Ecks: $\triangle, \square$,Pentagon

10.3 Definition

Sei M eine Menge von Punkten in $\mathbb{R}^2$.

$$\curlywedge(M) := \left\{ P \in \mathbb{R}^2 \,\middle|\, P \text{ ist mit Zirkel und Lineal aus } M \text{ konstruierbar} \right\}$$

Genauer: Für $M \subseteq \mathbb{R}^2$ sei

$$\begin{aligned} \mathrm{Gr}(M) &:= \left\{ g \subseteq \mathbb{R}^2 \text{ Gerade} \,\middle|\, |g \cap M| \geq 2 \right\} \\ \mathrm{Kr}(M) &:= \left\{ k \subseteq \mathbb{R}^2 \text{ ein Kreis} \,\middle|\, \text{Mittelpunkt } (k) \in M,\ \text{Radius } (k) = \text{ Abstand } (P, Q) \text{ mit } P, Q \in M \right\} \end{aligned}$$

Setze nun

$$\curlywedge(M) := \left\{ P \in \mathbb{R}^2 \;\middle|\; \begin{array}{l} \quad\exists g \neq g \in \mathrm{Gr}(M) : P \in g \cap g' \\ \text{oder } \exists k \neq k' \in \mathrm{Kr}(M) \text{ mit } P \in k \cap k' \\ \text{oder } \exists k \in \mathrm{Kr}(M), g \in \mathrm{Gr}(M) \text{ mit } P \in k \cap g \end{array} \right\}$$

und $\curlywedge^{(0)}(M) = M$. $\curlywedge^{(n)}(M) := \curlywedge^{(1)}(\curlywedge^{(n-1)}(M))$ für $n \geq 1$. Dann ist $(M) = \bigcup_{n=0}^{\infty} \curlywedge^{(n)}(M)$.
Warnung: $g \in \mathrm{Gr}(M), P \in g \not\Longrightarrow P \in \curlywedge(M)$, $k \in \mathrm{Kr}(M), P \in k \not\Longrightarrow P \in \curlywedge(M)$

10.4 Bemerkung

Wir ersetzen $\mathbb{R}^2$ durch den Körper $\mathbb{C}$. Damit ergibt sich

(3) Quadratur des Einheitskreises: $\sqrt{\pi} \in \curlywedge(\{0,1\})$

(2) Delisches Problem: Verdoppelung des Einheitswürfels: $\sqrt[3]{2} \in \curlywedge(\{0,1\})$

(4) Konstruktion des regelmäßigen Einheits-n-Ecks: $e^{\frac{2\pi}{n}i} \in \curlywedge(\{0,1\})$ *Zentriwinkel*

(1) Drittellung des Winkels $\varphi \in [0, 2\pi]$:. $e^{\frac{i\varphi}{3}} \in \curlywedge(\{0, 1, e^{i\varphi}\})$

10.5 Proposition 1

Sei $M \subseteq \mathbb{C}$ mit $\{0,1\} \subseteq M$. Dann gilt

i) $i \in \curlywedge(M)$

ii) $z \in \curlywedge(M) \Longrightarrow -z, \overline{z}, \mathrm{Re}(z), \mathrm{Im}(z), |z| \in \curlywedge(M)$

iii) $z \in \curlywedge(M), z \neq 0 \Longrightarrow \frac{1}{z} \in \curlywedge(M)$

iv) $z_1, z_2 \in \curlywedge(M) \Longrightarrow z_1 + z_2, z_1 \cdot z_2 \in \curlywedge(M)$

v) $z \in \mathbb{C}, z^2 \in \curlywedge(M) \Longrightarrow z \in \curlywedge(M)$

Beweis
Übung und Lorenz

10.6 Korollar

i) $\curlywedge(\{0,1\}) \subseteq \mathbb{C}$ ist ein Unterkörper.

ii) $\mathbb{Q} \subseteq \curlywedge(\{0,1\})$, sogar $\mathbb{Q}[i] \subseteq \curlywedge(\{0,1\})$

iii) $\mathbb{Q}[i] \subsetneq \curlywedge(\{0,1\})$

Beweis
Proposition 1 (auch iii) mit $\sqrt{z} \in \curlywedge(\{0,1\}), \sqrt{z} \notin \mathbb{Q}[i]$

10.7 Frage

Was sind Beispiele von Unterkörpern von $\mathbb{C}$?

(i) $\mathbb{Q} \subseteq \mathbb{C}$ (ii) $\mathbb{R} \subseteq \mathbb{C}$ (iii) $\mathbb{C}$

10.8 Beispiel

$\mathbb{Q}[i] := \{a + bi \,|\, a, b \in \mathbb{Q}\}$ ist ein Unterkörper von $\mathbb{C}$

$$(a+bi)^{-1} = \frac{a-bi}{a^2+b^2} = \frac{a}{a^2+b^2} + \frac{b}{a^2+b^2} i \in \mathbb{Q}[i]$$

10.9 Lemma

Sei $K \subseteq \mathbb{C}$ ein Unterkörper. Sei $\alpha \in \mathbb{C} \setminus K$ mit $\alpha^2 \in K$. Dann ist $K[\alpha] := \{a + b\alpha \,|\, a, b \in K\}$ ein Unterkörper von $\mathbb{C}$.

Beweis
Zu zeigen: $\forall 0 \neq a + b\alpha \in K[\alpha]$ ist $(a+b\alpha)^{-1} \in K[\alpha]$. Für $x, y \in K$ gilt $(x + y\alpha) = (a+b\alpha)^{-1}$ genau dann, wenn gilt

$$\begin{aligned} ax + b\alpha^2 y &= 1 \\ bx + ay &= 0 \end{aligned}$$

Es ist $\det \begin{pmatrix} a & b\alpha^2 \\ b & a \end{pmatrix} = a^2 - b^2\alpha^2$. Ist $b = 0$, so ist $a \neq 0$ und $\alpha^2 - b^2\alpha^2 \neq 0$. ist $b \neq 0$, so ist auch $a^2 - b^2\alpha^2 \neq 0$, denn sonst $\frac{a^2}{b^2} = \alpha^2$ und damit $\alpha = \pm \frac{a}{b} \in K$, aber $\alpha \notin K$.

Damit ist das Gleichungssystem lösbar und $(a + b\alpha)$ in $K[\alpha]$ invertierbar. □

10.10 Definition

Wir sagen dann:

$$K[\alpha]/K$$

ist eine **quadratische Körpererweiterung**.

10.11 Satz

Für $z \in \mathbb{C}$ sind äquivalent:

i) $z \in \mathcal{A}(\{0,1\})$

ii) Es gibt eine Kette $\mathbb{Q} = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_n$ von Unterkörpern von $\mathbb{C}$ mit $z \in K_n$ und K_i/K_{i-1} ist eine quadratische Körpererweiterung, also gilt für jedes $i = 1, \ldots, n : \exists \omega_i \in K_i \backslash_{i-1}$ mit $\omega_i^2 \in K_{i-1}$ und $K_i = K_{i-1}[\omega_i]$.

Beweis
ii) ⇒ i) Proposition 1 (10.5)+ Induktion nach n

i) ⇒ ii) Sei $z \in \mathcal{A}(\{0,1\})$. Dann gibt es $P_1, \ldots, P_n \in \mathbb{C}$ mit $P_n = z$, so dass P_{i+1} aus $M_i = \{0, 1, P_1, \ldots, P_i\}$ durch einen Konstruktionsschritt konstruiert werden kann. Also: Es gilt

(i) $P_{i+1} \in g \cap g', g \neq g' \in \mathrm{Gr}(M_i)$ oder
(ii) $P_{i+1} \in k \cap k', k \neq k' \in \mathrm{Kr}(M_i)$ oder
(iii) $P_{i+1} \in k \cap g, k \in \mathrm{Kr}(M_i), g \in \mathrm{Gr}(M_1)$

Sei K_i der kleinste Unterkörper von $\mathbb{C}$, der M_i enthält.
Behauptung (*): Ist $K_{i+1} \supsetneq K_i$, so gibt es $\omega_{i+1} \in K_{i+1} \setminus K_i$ mit $\omega_{i+1}^2 \in K_i$ und $K_{i+1} = K_i[\omega_{i+1}]$

Klar: (*) ⇒ ii) Beweis modulo (*) □

10.12 Beispiel

$$\omega := e^{\frac{2\pi i}{5}}$$

(Also $\omega \in \mathcal{A}(\{0,1\}) \iff$ regelmäßige 5-Eck ist konstruierbar)
Es ist $\omega^5 = 1$. Also ist ω Nullstelle von $X^5 - 1$. Es ist

$$X^5 - 1 = (X-1)(X^4 + X^3 + X^2 + X + 1)$$

Insbesondere $(\omega - 1)(\omega^4 + \omega^3 + \omega^2 + \omega + 1) = 0$. Da $\omega \neq 1$, ist also $\omega^4 + \omega^3 + \omega^2 + \omega + 1 = 0$. Sei $z := \omega + \omega^{-1}$. Dann folgt $\quad | \cdot \omega^{-2}$

$$\omega^2 + \omega + 1 + \omega^{-1} + \omega^{-2} = 0$$

Es ist $z^2 = \omega^2 + 2 + \omega^{-2}$. Mit $(\#)$ folgt $z^2 + z - 1 = 0$. Also $z \in \left\{-\frac{1}{2} \pm \frac{1}{2}\sqrt{5}\right\}$. Daher $z \in \mathbb{Q}[\sqrt{5}]$. Weiter ist $\omega^2 - z\omega = \omega^2 - \omega^2 - 1 = -1$. Also

$$\left(\omega - \frac{z}{2}\right)^2 = \omega^2 - z\omega + \frac{z^2}{4} = -1 + \frac{z^2}{4} \in \mathbb{Q}[\sqrt{5}]$$

Es ist also $\mathbb{Q} \subseteq \mathbb{Q}[\sqrt{5}] \subseteq \mathbb{Q}[\sqrt{5}][\omega - \frac{z}{2}]$ und $\omega \in \mathbb{Q}[\sqrt{5}][\omega - \frac{z}{2}]$.
$\Longrightarrow$ Das regelmäßige 5-Eck ist mit Zirkel und Lineal konstruierbar. $\square$

11 Algebraische Körpererweiterungen

11.1 Definition

Die Notation gleicht leider der von Quotientenringen!

Sei K ein Unterkörper des Körpers L. Dann sagen wir L ist eine **Körpererweiterung** (KE) von K oder kurz L/K ist eine Körpererweiterung.

11.2 Beispiele

$\mathbb{Q}[i]/\mathbb{Q}$, $\mathbb{Q}[\sqrt{2}]/\mathbb{Q}$, $\mathbb{C}/\mathbb{Q}$, $\mathbb{R}/\mathbb{Q}$, $\mathbb{C}/\mathbb{R}$, $\mathbb{R}/\mathbb{Q}[\sqrt{2}]$, $\ldots$

11.3 Definition

Ein **Zwischenkörper** einer Körpererweiterung L/K ist ein Unterkörper E von L der K enthält:

$$K \subseteq E \subseteq L$$

11.4 Bemerkung

Sind E und E' Zwischenkörper von L/K, dann ist auch $E \cap E'$ ein Zwischenkörper von L/K.

11.5 Definition

Sei L/K eine Körpererweiterung und $M \subseteq L$ eine Teilmenge. Dann gibt es einen kleinsten Zwischenkörper von L/K, der M enthält, nämlich der Durchschnitt aller Zwischenkörper von L/K, die M enthalten. Wir bezeichnen diesen Zwischenkörper mit $K(M)$. $K(M)$ heißt von M erzeugt. Wenn $M = \{\alpha_1, \ldots, \alpha_n\}$, dann setzen wir $K(\alpha_1, \ldots, \alpha_2) := K(\{\alpha_1, \ldots, \alpha_n\})$

11.6 Beispiel

Ist $\alpha \in \mathbb{C}$ mit $\alpha^2 \in K$, so ist

$$K(\alpha) = K[\alpha] = \{a + \alpha b \,|\, a, b \in K\}$$

11.7 Bemerkung

Ist L/K eine Körpererweiterung, so ist L insbesondere ein K-Vektorraum.

11.8 Definition

Sei L/K eine Körpererweiterung. $[L : K] := \dim_K L$ heißt der **Grad von** L/K. Ist $[L : K] < \infty$, so heißt L/K endlich, sonst unendlich.

11.9 Beispiel

$\{1, i\}$ ist eine $\mathbb{Q}$-Basis von $\mathbb{Q}[i]$. Also $\big[\mathbb{Q}[i] : Q\big] = 2$. Jede quadratische Körpererweiterung hat Grad 2. Die Umkehrung ist auch richtig (Übung).

11.10 Gradsatz

Sei E ein Zwischenkörper von L/K, dann gilt:

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

Beweis
Sei B eine K-Basis von E und A eine E-Basis von L. Es genügt zu zeigen, dass $A{\cdot}B := \{a \cdot b \,|\, a \in A, b \in B\}$ eine K-Basis von L ist.

$A \cdot B$ **ist** K**-EZS:** Sei $l \in L$. Da A ein E-EZS von L ist, gilt $l = \sum_{a\in A} \alpha_a \cdot a$ mit $\alpha_a \in E$, fast alle $\alpha_a = 0$. Da B ein K-EZS von E ist, gilt

$$\alpha_a = \sum_{b\in B} \beta_{b,a} \cdot b$$

mit $\beta_{b,a} \in K$ (und fast alle gleich 0). Es folgt

$$l = \sum_{a\in A} \alpha_a \cdot a = \sum_{a\in A} (\sum_{b\in B} \beta_{b,a} \cdot b) \cdot a = \sum_{a\in A, b\in B} \beta_{b,a} \cdot b \cdot a$$

$A \cdot B$ **ist linear unabhängig über** K**:** Sei also $\sum_{a\in A, b\in B} \alpha_{a,b} \cdot a \cdot b = 0$ mit $\alpha_{a,b} \in K$, fast alle $= 0$. Dann ist auch

$$\sum_{a\in A} \underbrace{(\sum_{b\in B} \alpha_{a,b} \cdot b)}_{\in E} \cdot a = 0$$

Da A linear unabhängig über E folgt für alle $a \in A: \sum \alpha_{a,b} \cdot b = 0$. Da B linear unabhängig über K folgt $\alpha_{a,b} = 0$ für alle $a \in A, b \in B$. (Dies zeigt auch $a \cdot b = a' \cdot b' \iff a = a' \wedge b = b'$) $\square$

11.11 Beispiel

Sei $\omega = e^{\frac{2\pi i}{5}}$. Am Donnerstag haben wir gezeigt: $(\omega - \frac{z}{2})^2 \in \mathbb{Q}[\sqrt{5}]$ mit $z \in \mathbb{Q}[\sqrt{5}]$. Es ist $\mathbb{Q} \subsetneq \mathbb{Q}[\sqrt{5}]$, da $\sqrt{5} \notin \mathbb{Q}$. Außerdem $\mathbb{Q}[\sqrt{5}] \subsetneq \mathbb{Q}[\sqrt{5}, \omega - \frac{z}{2}]$, da $\mathbb{Q}[\sqrt{5}] \subseteq \mathbb{R}$ aber $\mathbb{R} \not\ni \omega \in \mathbb{Q}[\sqrt{5}, \omega - \frac{z}{2}]$. Es folgt

$$\left[\mathbb{Q}[\sqrt{5}, \omega - \frac{z}{2}] : \mathbb{Q}\right] = 4$$

(Es ist auch $[\mathbb{Q}[\omega] : \mathbb{Q}] = 4$)

11.12 Korollar

Sei L/K eine Körpererweiterung mit $[L:K]$ eine Primzahl. Dann sind L und K die einzigen Zwischenkörper von L/K.

Beweis
Ist E ein Zwischenkörper von L/K, so gilt $p = [L:K] = [L:E] \cdot [E:K]$. Es gilt also $[L:E] = 1$ oder $[E:K] = 1$. Also gilt entweder $L = E$ oder $E = K$. $\square$

11.13 Definition

Sei L/K eine Körpererweiterung.

(i) $\alpha \in L$ heißt **algebraisch** über K, wenn es $f \in K[X]$, $f \neq 0$ gibt mit $f(\alpha) = 0$.

(ii) L/K heißt **algebraisch**, wenn alle $\alpha \in L$ algebraisch über K sind.

11.14 Beispiel

- $\omega \in \mathbb{C}$ ist algebraisch über $\mathbb{Q}$: $(X^5 - 1)(\omega) = 0$
- Für alle $n, k \in \mathbb{Z}$ ist $\sqrt[n]{k} \in \mathbb{R}$ algebraisch über $\mathbb{Q}$: $(X^n - k)(\sqrt[n]{k}) = 0$

11.15 Fragen

1) Ist $\sqrt[n]{k} + \sqrt[n']{k'}$ algebraisch über $\mathbb{Q}$?
2) Ist die Summe und das Produkt von algebraischen Elementen wieder algebraisch?

11.16 Proposition

Sei L/K eine Körpererweiterung und $\alpha \in L$ algebraisch über K.

i) Es gibt ein eindeutiges normiertes Polynom $p_\alpha \in K[X]$ mit $(p_\alpha) = \{f \in K[X] \mid f(\alpha) = 0\}$
ii) p_α ist irreduzibel und (p_α) ein Primideal in $K[X]$

Beweis
$I := \{f \in K[X] \mid f(\alpha) = 0\} \subseteq K[X]$ ist ein Ideal ($f, g \in I : (f + g)(\alpha) = f(\alpha) + g(\alpha) = 0$ und $\varphi \in K[X], f \in I : (\varphi \cdot f)(\alpha) = \varphi(\alpha) \cdot f(\alpha) = 0$). Da $K[X]$ ein Hauptidealring ist, gibt es $p_\alpha \in K[X]$ mit $I = (p_\alpha)$. p_α wird eindeutig durch Normierung. I ist sogar ein Primideal. Seien $f, g \in K[X]$ mit $f \cdot g \in I$. Dann $0 = (f \cdot g)(\alpha) = f(\alpha) \cdot g(\alpha)$. Also $f(\alpha) = 0$ oder $g(\alpha) = 0$. Daraus folgt, dass $f \in I$ oder $g \in I$. Daher ist p_α prim und damit auch irreduzibel. □

11.17 Definition

p_α heißt das **Minimalpolynom** von α über K.

11.18 Bemerkung

p_α ist das normierte Polynom von kleinstem Grad mit $p_\alpha(\alpha) = 0$.

11.19 Bemerkung

Sei L/K eine Körpererweiterung und $\alpha \in L$. Ist $p \in K[X]$ irreduzibel und normiert mit $p(\alpha) = 0$, so ist α algebraisch über K und $p_\alpha = p$. (Denn: $p_\alpha \mid p$, da p_α und p irreduzibel und normiert sind, folgt $p_\alpha = p$).

11.20 Definition

Sei L/K eine Körpererweiterung und $\alpha \in L$. Dann heißt der Ringhomomorphismus $\phi_\alpha : K[X] \to L$ mit $\phi_\alpha(f) := f(\alpha)$ **Einsetzungshomomorphismus**. Es ist $\operatorname{Kern} \phi_\alpha = \{f \in K[X] \mid f(\alpha) = 0\}$. Wir setzen

$$K[\alpha] := \operatorname{Bild} \phi_\alpha.$$

11.21 Bemerkung

(i) $K[\alpha]$ ist Unterring von L, der K enthält. Es gilt nach dem Homomorphiesatz (6.5)

$$K[\alpha] \cong K[X]/\operatorname{Kern} \phi_\alpha$$

(ii) α ist genau dann algebraisch, wenn $\operatorname{Kern} \phi_\alpha \neq \{0\}$. In diesem Fall ist $\operatorname{Kern} \phi_\alpha = (p_\alpha)$.

11.22 Lemma

Sei $\alpha \in L$ algebraisch über K. Dann gilt $\dim_K K[\alpha] = d(p_\alpha)$

Beweis
Sei $p_\alpha = X^n + a_{n-1}X^{n-1} + \ldots + a_1 X + a_0 \in K[X]$. Wir zeigen: $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ ist eine Basis von $K[\alpha]$.

Lineare Unabhängigkeit: Sei $b_{n-1} \cdot \alpha^{n-1} + b_{n-2} \cdot \alpha^{n-2} + \ldots + b_1 \cdot \alpha + b_1 \cdot 1 = 0$ mit $b_i \in K$. Setze $f := b_{n-1}X^{n-1} + b_{n-2}X^{n-2} + \ldots + b_1 X + b_0 \in K[X]$. Es folgt $f(\alpha) = 0$. Da $d(f) < d(p_\alpha) = n$ folgt $f = 0$. Damit sind $b_{n-1} = b_{n-2} = \ldots = b_1 = b_0 = 0$

Erzeugendensystem Es ist $K[\alpha] = \langle \alpha^k \mid k = 0, 1, 2, \ldots \rangle_K$. Zu zeigen: Für $N \geq n$ ist $\alpha^N \in \langle \alpha^0, \alpha^1, \ldots, \alpha^{N-1} \rangle$. Mit $p_\alpha(\alpha) = 0$ folgt

$$\alpha^n = -a_{n-1} \cdot \alpha^{n-1} - a_{n-2} \cdot \alpha^{n-2} - \ldots - a_1 \cdot \alpha - a_0 \cdot \alpha^0$$

Daher $\alpha^N = -a_{n-1} \cdot \alpha^{N-1} - \ldots - a_1 \cdot \alpha^{N-n+1} - a_0 \cdot \alpha^{N-n} \in \langle \alpha^0, \ldots, \alpha^{N-1} \rangle$ □

11.23 Zusammenfassung

$$\begin{aligned}
K(\alpha) &= \text{der von } \alpha \text{ erzeugte Körper} \\
K[\alpha] &= \text{der von } \alpha \text{ erzeugte Ring} \\
K[\alpha] &\cong \begin{cases} K[X]/(p_\alpha), & \text{falls } \alpha \text{ algebraisch} \\ K[X] & \text{sonst} \end{cases} \\
\dim_K K[\alpha] &= \begin{cases} d(p_\alpha), & \text{falls } \alpha \text{ algebraisch} \\ \infty, & \text{sonst} \end{cases}
\end{aligned}$$

11.24 Satz

Sei L/K eine Körpererweiterung und $\alpha \in L$. Dann sind äquivalent:

(i) α ist algebraisch über K

(ii) $\dim_K K[\alpha] < \infty$

(iii) $K[\alpha] = K(\alpha)$

(iv) $K(\alpha)/K$ ist endlich.

Beweis
Wegen $K[\alpha] \subseteq K(\alpha)$ gilt "iv) $\Rightarrow$ ii)". Weiter gilt "ii)& iii) $\Rightarrow$iv)". Es genügt daher i) $\Rightarrow$ ii) $\Rightarrow$ iii) $\Rightarrow$ i) zu zeigen.

i) $\Rightarrow$ ii) folgt aus $\dim_K K[\alpha] = d(p_\alpha) < \infty$

ii) $\Rightarrow$ iii) Es gilt immer $K[\alpha] \subseteq K(\alpha)$. Es genügt daher zu zeigen, dass $K[\alpha]$ ein Körper ist. Zu zeigen:

$$\forall \beta \in K[\alpha] \setminus \{0\} \text{ gilt } \beta^{-1} \in K[\alpha]$$

Betrachte $M_\beta : K[\alpha] \to K[\alpha]$ mit $M_\beta(x) = \beta \cdot x$. Zu zeigen: $1 \in \operatorname{Bild} M_\beta$. Behauptung: M_β ist surjektiv. Da $\dim_K K[\alpha] < \infty$ und $M_\beta : K[\alpha] \to K[\alpha]$ K-linear ist, genügt es zu zeigen $\operatorname{Kern} M_\beta = \{0\}$. Sei $x \in \operatorname{Kern} M_\beta$, also $M_\beta(x) = \beta \cdot x = 0$. Da $\beta \neq 0$ und $K[\alpha]$ nullteilerfrei ist (da $K[\alpha] \subseteq L$), folgt $x = 0$.

iii) $\Rightarrow$i) Angenommen α ist nicht algebraisch. Dann gilt $K[\alpha] \cong K[X]$. Nun ist aber $K[X]$ kein Körper. ↯ □

11.25 Korollar 1

Sei $^L/_K$ eine Körpererweiterung, $\alpha \in L$ algebraisch über K. Dann gilt $[K(\alpha) : K] = \deg(p_\alpha)$

Beweis

$$[K(\alpha) : K] = \dim_K K(\alpha) \overset{11.24}{=} \dim_K K[\alpha] \overset{11.22}{=} \deg p_\alpha \qquad \square$$

11.26 Korollar 2

Endliche Körpererweiterungen sind algebraisch.

Beweis
Sei $^L/_K$ endlich und $\alpha \in L$. Dann ist $K(\alpha) \subseteq L$. Daher ist $[K(\alpha) : K] \leq [L : K] < \infty$. Mit Satz 11.24 folgt: α ist algebraisch über K. □

11.27 Korollar 3

Sei $^L/_K$ eine Körpererweiterung und $\alpha \in L$. Dann gilt:

$$\alpha \text{ algebraisch über } K \iff {}^{K(\alpha)}/_K \text{ ist algebraisch}$$

Beweis
"$\Leftarrow$": ist klar, da $\alpha \in K(\alpha)$

"$\Rightarrow$": Sei $\alpha \in L$ algebraisch über K. Mit Satz 11.24 folgt $^{K(\alpha)}/_K$ ist endlich. Mit Korollar 2 (11.26) folgt $^{K(\alpha)}/_K$ ist algebraisch. □

11.28 Korollar 4

Sei $^L/_K$ eine Körpererweiterung. Seien $\alpha, \beta \in L$ algebraisch über K. Dann ist $^{K(\alpha,\beta)}/_K$ endlich und damit algebraisch. Insbesondere sind $-\alpha, \alpha+\beta, \alpha\cdot\beta$ algebraisch über K. Ist $\alpha \neq 0$, so ist auch α^{-1} algebraisch über K.

Beweis
Mit der Gradformel folgt:

$$[K(\alpha,\beta) : K] = [K(\alpha,\beta) : K(\alpha)] \cdot [K(\alpha) : K]$$

Da α algebraisch über K ist, ist $[K(\alpha) : K] < \infty$. Es ist $K(\alpha,\beta) = K(\alpha)(\beta)$. Da β algebraisch über K ist, ist β auch algebraisch über $K(\alpha)$. Daher ist $^{K(\alpha)(\beta)}/_{K(\alpha)}$ endlich. □

11.29 Bemerkung

Sei $^L/_K$ eine Körpererweiterung und $A, B \subseteq L$. Dann gilt $K(A \cup B) = K(A)(B) = K(B)(A)$

Beweis
"$\supseteq$": $K(A \cup B)$ ist ein Zwischenkörper von $^L/_{K(A)}$ da $K(A) \subseteq K(A \cup B)$. Er enthält auch B. Also $K(A)(B) \subseteq K(A \cup B)$, da $K(A)(B)$ der kleinster Zwischenkörper von $^L/_{K(A)}$ ist, der B enthält.

"$\subseteq$": Es ist $K(A \cup B)$ der kleinster Zwischenkörper von $^L/_K$, der $A \cup B$ enthält. Da $A \cup B \subseteq K(A)(B)$ und $K(A)(B)$. Zu K von $^L/_K$ folgt "$\subseteq$".

11.30 Korollar 5

Sei L/K eine Körpererweiterung. Dann ist

$$\overline{K}^L := \{\alpha \in L \,|\, \alpha \text{ ist algebraisch über } K\}$$

ein Zwischenkörper von L/K.

Beweis
Korollar 4 (11.28).

11.31 Definition

$\overline{K}^L$ heißt der **algebraische Abschluss** von K in L.

11.32 Bemerkung

Sei $\overline{Q} := \overline{Q}^{\mathbb{C}}$. Dann ist $\overline{\mathbb{Q}}/\mathbb{Q}$ algebraisch, aber nicht endlich.

11.33 Beispiel

$[\mathbb{Q}(\sqrt[n]{2}) : \mathbb{Q}] = \deg p_{\sqrt[n]{2}} = n$ da $p_{\sqrt[n]{2}} = X^n - 2$, was irreduzibel nach Eisenstein ist.

11.34 Korollar

Das Delische Problem (10.4) ist nicht mit Zirkel und Lineal lösbar.

Beweis
Zu zeigen: $\sqrt[3]{2} \notin \mathcal{A}(\{0, 1\})$. Angenommen doch. Dann gibt es eine Folge von Körpern $\mathbb{Q} = K_0 \subseteq K_1 \subseteq K_2 \subseteq \ldots \subseteq K_n$ mit: $\sqrt[3]{2} \in K_n$ und K_i/K_{i-1} ist eine quadratische Erweiterung.
Es ist $[K_i : K_{i-1}] = 2$. Mit der Gradformel folgt: $[K_n : \mathbb{Q}] = 2^n$. Andererseits ist $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$. Es folgt

$$2^n = [K_n : \mathbb{Q}] = \left[K_n : \mathbb{Q}(\sqrt[3]{2})\right] \cdot \left[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}\right] = \left[K_n : \mathbb{Q}(\sqrt[3]{2})\right] \cdot 3$$

$\Rightarrow [K_n : \mathbb{Q}(\sqrt[3]{2})] = \frac{2^n}{3}$ ↯ □

12 Auflösung von algebraischen Gleichungen über $\mathbb{Q}$

12.1 Beispiel

Sei $f = X^2 + pX + q \in \mathbb{Q}[X]$. Für $\alpha \in \mathbb{C}$ gilt dann

$$f(\alpha) = 0 \iff \alpha^2 + p\alpha = -q \iff (\alpha + \frac{p}{2})^2 - \frac{p^2}{4} = -q \iff \alpha + \frac{p}{2} = \pm\sqrt{\frac{p^2}{4} - q}$$
$$\iff \alpha = -\frac{p}{2} \pm \sqrt{\frac{p^2}{4} - q}$$

12.2 Frage

Was passiert mit Polynomen von Grad $= 3, 4, 5, \ldots$?

12.3 Bemerkung

Sei $f = X^3 + aX^2 + bX + c \in \mathbb{Q}[X]$. Dann ist $f(X - \frac{a}{3}) = X^3 + pX + q$ mit $p, q \in \mathbb{Q}$.

12.4 Satz (Cardano'sche Formel)

Sei $f = X^3 + pX + q \in \mathbb{Q}[X]$. Sei $\xi := e^{2\pi i/3}$. Sei $\alpha \in \mathbb{C}$ mit $\alpha^2 = (\frac{p}{3})^3 + (\frac{q}{2})^2$. Seien $u, v \in \mathbb{C}$ mit $u^3 = -\frac{q}{2} + \alpha$, $v^3 = -\frac{q}{2} - \alpha$, $u \cdot v = -\frac{1}{3}p$. Dann sind

$$x_1 := u + v \qquad x_2 := \xi^2 u + \xi v \qquad x_3 := \xi u + \xi^2 v$$

die Nullstellen von f.

Beweis
Bosch Seite 274 □

12.5 Bemerkung

Es gibt auch Formeln für Polynome vom Grad 4. (Bosch Seite 278).

12.6 Frage

Sei $\alpha \in \mathbb{C}$ algebraisch über $\mathbb{Q}$. Lässt sich dann α mittels $+, -, \cdot, (\,)^{-1}, \sqrt[n]{(\,)}$ durch Elemente aus $\mathbb{Q}$ ausdrücken?
Beispiel:

$$\frac{\sqrt[3]{7} - \sqrt[5]{\sqrt[2]{11} + \frac{5}{2}}}{\sqrt[p]{101}}$$

12.7 Definition

Eine Körpererweiterung L/K heißt eine **Radikalerweiterung**, falls es $\alpha \in L$ und $n \in \mathbb{N}^*$ gibt mit

a) $\alpha^n \in K$ b) $L = K(\alpha)$

12.8 Bemerkung

Ist $\operatorname{char} K > 0$ (also $p \cdot 1 = 0$ für ein $p \geq 1$) so fast man die obige Definition üblicherweise etwas weiter.

12.9 Definition

Sei $f \in \mathbb{Q}[X]$. Dann heißt f **durch Radikale auflösbar**, falls es eine Kette von Zwischenkörpern $\mathbb{Q} = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_n \subseteq \mathbb{C}$ gibt mit:

(i) f zerfällt über K_n in Linearfaktoren ($\Leftrightarrow K_n$ enthält alle komplexen Nullstellen von f)

(ii) Für $i = 1, \ldots, n$ ist ${}^{K_i}/_{K_{i-1}}$ eine Radikalerweiterung.

Ein Unterkörper $E \subseteq \mathbb{C}$ heißt durch Radikale auflösbar, falls es eine Kette von Zwischenkörpern $\mathbb{Q} = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_n \subseteq \mathbb{C}$ gibt mit

(i) $E \subseteq K_n$

(ii) wie vorher

12.10 Beispiel

(i) Jedes Polynom von Grad 2 ist durch Radikale auflösbar: Ist $f = X^2 + pX + q$ so enthält $\mathbb{Q}(\sqrt{p^2 - 4q})$ alle Nullstellen von f

(ii) Sei $f = X^3 + pX + q \in \mathbb{Q}[X]$, so enthält $\mathbb{Q}(\xi, \alpha, u)$ mit $\xi = e^{2\pi i/3}$, $\alpha^2 = (\frac{p}{3})^3 + (\frac{p}{2})^2$, $u^3 = -\frac{p}{2} + \alpha$ alle Nullstellen von f

$$\mathbb{Q} \subseteq \mathbb{Q}(\xi) \subseteq \mathbb{Q}(\xi, \alpha) \subseteq \mathbb{Q}(\xi, \alpha, u)$$

ist eine Kette von Radikalerweiterungen.

Ausblick: Wir werden sehen, dass es Polynome in $\mathbb{Q}[X]$ gibt, die nicht durch Radikale auflösbar sind.

12.11 Definition

Eine Gruppe G heißt **auflösbar**, wenn es eine Folge von von normalen Untergruppen

Notation: $N \trianglelefteq G$ falls $N \leq G$ eine normale Untergruppe ist

$$\{e\} = N_0 \trianglelefteq N_1 \trianglelefteq N_2 \trianglelefteq \ldots \trianglelefteq N_n = G$$

gibt, so dass für $i = 1, \ldots, n$ ${}^{N_i}/_{N_{i-1}}$ abelsch ist.

12.12 Lemma

Sei G eine endliche Gruppe. Ist G auflösbar, so gibt es eine Folge

$$\{e\} = N_0 \trianglelefteq N_1 \trianglelefteq \ldots \trianglelefteq N_n = G$$

von normalen Untergruppen, so dass für $i = 1, \ldots, n$ ${}^{N_i}/_{N_{i-1}}$ zyklisch von Primzahlordnung ist.

Beweis
Übung.

12.13 Lemma

Sei $N \trianglelefteq G$ eine normale Untergruppe. Dann gilt

$$G \text{ auflösbar} \iff N \text{ und } {}^{G}/_{N} \text{ sind auflösbar}$$

Beweis
Übung.

12.14 Korollar

p-Gruppen sind auflösbar.

Beweis
Durch Induktion nach der Ordnung der Gruppe. Für die triviale Gruppe ist die Aussage sicher richtig. Sei P eine p-Gruppe. Das Zentrum Z von P ist eine abelsche normale Untergruppe (siehe 3.17). Da P eine p-Gruppe ist, ist $Z \neq \{e\}$. Weiter ist $|P/Z| < |P|$. Nach Induktionsannahme ist P/Z auflösbar. Da Z als Zentrum abelsch und damit auflösbar ist, folgt mit dem Lemma 12.13: P ist auflösbar. □

13 Primkörper

13.1 Bezeichnung

Sei K ein Körper. Dann setzen wir

$$n_K := \underbrace{1_K + \ldots + 1_K}_{n\text{-mal}}$$

Für eine Primzahl p setzen wir $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$

13.2 Definition

Sei K ein Körper. Die kleinste positive Zahl $p \in \mathbb{N}$, für die $p_K = 0_K \in K$ ist, heißt die **Charakteristik** $\operatorname{char} K$ von K. Gibt es keine solche Zahl, so setzen wir $\operatorname{char} K = 0$

13.3 Beispiel

- $\operatorname{char}(\mathbb{Q}) = \operatorname{char}(\mathbb{R}) = \operatorname{char}(\mathbb{C}) = 0$
- $\operatorname{char}(\mathbb{F}_p) = \operatorname{char} Q(\mathbb{F}_p[X]) = p$

13.4 Bemerkung

Ist $(n \cdot m)_K = 0$, so folgt $n_K = 0$ oder $m_K = 0$. Insbesondere ist $\operatorname{char} K$ eine Primzahl oder gleich 0.

13.5 Bemerkung

Sei K ein Körper. Dann ist

$$k := \left\{ \frac{n_K}{m_K} \in K \,\middle|\, n, m \in \mathbb{Z}, m_k \neq 0 \right\} \qquad \text{mit } (-n)_K = -n_K \text{ für } n \geq 0$$

der kleinste Unterkörper von K. Es heißt der **Primkörper** von K. Es gilt:

$$k = \begin{cases} \mathbb{Q}, & \text{falls } \operatorname{char} K = 0 \\ \mathbb{F}_p, & \text{falls } \operatorname{char} K = p \end{cases}$$

13.6 Bemerkung

Sei $\sigma : K \to L$ ein Ringhomomorphismus zwischen Körpern. Für $a \in K \setminus \{0\}$ gilt dann

$$1 = \sigma(1) = \sigma(a \cdot a^{-1}) = \sigma(a) \cdot \sigma(a^{-1})$$

1) Es folgt $\sigma(a^{-1}) = \sigma(a)^{-1}$. Insbesondere gibt es keinen Unterschied zwischen "Ringhomomorphismus zwischen Körpern" und einem "Körperhomomorphismus".
2) Es ist $\sigma(a) \neq 0$. Insbesondere ist σ injektiv.

13.7 Lemma

Sei $\sigma : K \to L$ ein Körperhomomorphismus. Dann stimmen die Primkörper von K und L überein und die Einschränkung von σ auf die Primkörper ist die Identität.

Beweis
Es gilt $\sigma(n_K) = n_L$. Insbesondere ist $n_K = 0 \iff n_L = 0$. □

14 Zerfällungskörper

14.1 Definition

Sei K ein Körper und $f \in K[X]$. Ein Zerfällungskörper von f ist ein Körper L mit

(i) $K \subseteq L$

(ii) f zerfällt über L in Linearfaktoren. d.h. $f = \beta(X-\alpha_1)\cdots(X-\alpha_n)$ mit $\alpha_1,\dots,\alpha_n \in L, \beta \in K$

(iii) $L = K(\alpha_1,\dots,\alpha_n)$

14.2 Beispiel

$X^2+1 \in \mathbb{R}[X]$ hat keine Nullstelle in $\mathbb{R}$, zerfällt aber über $\mathbb{C}$. $X^2+1 = (X-i)(X+i)$. Da $\mathbb{C} = \mathbb{R}[i]$ ist $\mathbb{C}$ ein Zerfällungskörper für $X^2+1 \in \mathbb{R}[X]$.

14.3 Satz von Kronecker

Sei K ein Körper und $g \in K[X]$ eine Polynom von Grad ≥ 1. Dann gibt es eine endliche Körpererweiterung E/K in der g eine Nullstelle hat.

Beweis
Sei f ein irreduzibler Teiler von g. Dann ist $(f) \subseteq K[X]$ ein Primideal. Da $K[X]$ ein Hauptidealring ist, ist (f) auch maximal. Daher ist $E := K[X]/(f)$ eine Körpererweiterung von K. Sei $\alpha := X + (f) \in E$. Dann gilt:

$$g(\alpha) \overset{14.4}{=} g + (f) = 0 \in E$$

Es ist $[E:K] = \deg(f) < \infty$. □

14.4 Lemma

Seien $f, g \in K[X]$, $R := K[X]/(f)$. Dann gilt für $\alpha := X + (f) \in R$

$$g(\alpha) = g + (f)$$

Beweis
Es ist $\alpha^i = (X+(f))^i = X^i + (f)$. Ist $g = \sum_{i=0}^n a_i X^i$, so folgt

$$g(\alpha) = \sum_{i=1}^n a_i\alpha^i = \sum_{i=1}^n a_i X^i + (f) = g + (f)$$ □

14.5 Korollar (Existenz von Zerfällungskörpern)

Sei $f \in K[X]$. Dann gibt es einen Zerfällungskörper für f.

Beweis
Per Induktion nach $n := \deg f$. Ist $n = 0$ so ist nichts zu zeigen.
Induktionsschritt: $n-1 \mapsto n$: Sei $n = \deg f$. nach Kronecker gibt es eine Körpererweiterung L/K in der f eine Nullstelle $\alpha \in L$ hat. Also $f = \tilde{f}\cdot(X-\alpha) \in L[X]$ mit $\deg \tilde{f} = n-1$. Nach Induktionsannahme gibt es einen Zerfällungskörper $\tilde{L}/L$ für $\tilde{f}$. Dann zerfällt auch $f = (X-\alpha)\cdot\beta(X-\alpha_1)\cdot\ldots\cdot(X-\alpha_{n-1})$ über $\tilde{L}$. Nun ist $Z := K(\alpha,\alpha_1,\dots,\alpha_n) \subseteq \tilde{L}$ ein Zerfällungskörper von f. □

14.6 Definition

Seien ${}^{L_1}/_{K}$ und ${}^{L_2}/_{K}$ Körpererweiterungen. Ein K-**Homomorphismus** $\sigma : {}^{L_1}/_{K} \to {}^{L_2}/_{K}$ ist ein Ringhomomorphismus $\sigma : L_1 \to L_2$ mit $\sigma|_K = \mathrm{id}_K$. Gibt es einen bijektiven K-Homomorphismus $\sigma : {}^{L_1}/_{K} \to {}^{L_2}/_{K}$ so heißen ${}^{L_1}/_{K}$ und ${}^{L_2}/_{K}$ **isomorph**. Wir schreiben auch ${}^{L_1}/_{K} \cong {}^{L_2}/_{K}$.

14.7 Bemerkung

(i) K-Homomorphismen sind K-linear: $\alpha \in K, x \in L_1$ dann: $\sigma(\alpha \cdot x) = \sigma(\alpha) \cdot \sigma(x) = \alpha \cdot \sigma(x)$

(ii) ${}^{L_1}/_{K} \cong {}^{L_2}/_{K} \Longrightarrow [L_1 : K] = [L_2 : K]$.

14.8 Bemerkung

Sei $\varphi : K \to L$ ein Ringhomomorphismus zwischen Körpern. Sei $\Phi : K[X] \to L[X]$ der durch φ induzierte Ringhomomorphismus.

$$\Phi(\sum_{i=0}^{n} a_i X^i) = \sum_{i=0}^{n} \varphi(a_i) X^i$$

Wir schreiben $\Phi(f) = f^\varphi$. Für $f \in K[X]$ und $\alpha \in K$ gilt dann $\varphi\big(f(\alpha)\big) = f^\varphi\big(\varphi(\alpha)\big)$. Insbesondere

$$f(\alpha) = 0 \iff f^\varphi\big(\varphi(\alpha)\big) = 0$$

14.9 Fortsetzungssatz

Seien

(i) $\sigma : K_1 \to K_2$ ein Isomorphismus von Körpern

(ii) ${}^{L_1}/_{K_1}$ und ${}^{L_2}/_{K_2}$ Körpererweiterungen

(iii) $f \in K_1[X]$ irreduzibel

(iv) $\alpha_1 \in L_1$ eine Nullstelle von f, $\alpha_2 \in L_2$ eine Nullstelle von f^σ

$$\begin{tikzcd}
L_1 & L_2 \\
K_1(\alpha_1) \arrow[u, hook] \arrow[r, dashed, "\hat\sigma"] & K_2(\alpha_2) \arrow[u, hook] \\
K_1 \arrow[u, hook] \arrow[r, "\sigma"] & K_2 \arrow[u, hook]
\end{tikzcd}$$

Behauptung: Es existiert genau eine Fortsetzung $\hat\sigma : K_1(\alpha_1) \xrightarrow{\cong} K_2(\alpha_2)$ von σ mit $\hat\sigma(\alpha_1) = \alpha_2$. Weiter gilt: $\hat\sigma\big(g(\alpha_1)\big) = g^\sigma(\alpha_2)$

Beweis
Sei o.B.d.A f normiert. Dann ist auch f^σ normiert. Da mit σ auch die induzierte Abbildung $\psi : K_1[X] \to K_2[X], g \mapsto g^\sigma$ ein Isomorphismus ist, ist mit f auch $f^\sigma = \psi(f)$ irreduzibel. Es folgt

$$p_{\alpha_1} = f \quad \text{und} \quad p_{\alpha_2} = f^\sigma$$

Damit folgt auch

$$\begin{aligned}
(f) &= \mathrm{Kern}(\Phi_{\alpha_1} : K_1[X] \twoheadrightarrow K_1[\alpha_1] = K_1(\alpha_1)) \\
(f^\sigma) &= \mathrm{Kern}(\Phi_{\alpha_2} : K_2[X] \twoheadrightarrow K_2[\alpha_2] = K_2(\alpha_2))
\end{aligned}$$

Wir erhalten induzierte Isomorphismen nach dem Homomorphiesatz:

$$\begin{aligned}
\overline{\Phi_{\alpha_1}} : {}^{K_1[X]}/_{(f)} \xrightarrow{\cong} K_1(\alpha_1) \quad &, \quad g + (f) \mapsto g(\alpha_1) \\
\overline{\Phi_{\alpha_2}} : {}^{K_2[X]}/_{(f^\sigma)} \xrightarrow{\cong} K_2\alpha_2 \quad &, \quad g + (f^\sigma) \mapsto g(\alpha_2)
\end{aligned}$$

Da $\psi\big((f)\big) = \big(\psi(f)\big) = (f^\sigma)$ induziert ψ einen Isomorphismus

$$\overline{\psi} : {}^{K_1[X]}/_{(f)} \xrightarrow{\cong} {}^{K_2[X]}/_{(f^\sigma)} \quad , \quad g + (f) \mapsto g^\sigma + (f^\sigma)$$

Insgesamt ist

$$\begin{array}{ccccccc} \hat{\sigma} : K_1(\alpha_1) & \xrightarrow{(\overline{\Phi_{\alpha_1}})^{-1}} & {}^{K_1[X]}/_{(f)} & \xrightarrow{\overline{\psi}} & {}^{K_2[X]}/_{(f^\sigma)} & \xrightarrow{\overline{\Phi_{\alpha_2}}} & K_2(\alpha_2) \\ g(\alpha_1) & \longmapsto & g + (f) & \longmapsto & g^\sigma + (f^\sigma) & \longmapsto & g^\sigma(\alpha_2) \end{array}$$

Eindeutigkeit ist klar, da $K_1(\alpha_1) = K_1[\alpha_1]$. □

14.10 Lemma

Sei $\sigma : K_1 \to K_2$ ein Körperisomorphismus und ${}^{L_1}/_{K_1}$, ${}^{L_2}/_{K_2}$ Körpererweiterungen. Sei $\alpha_1 \in L_1$ algebraisch über K_1. Dann gibt es höchstens $[K_1(\alpha_1) : K_1] = \deg p_{\alpha_1}$ Fortsetzungen von σ zu Körperhomomorphismen

$$\tau : K_1(\alpha_1) \to L_2$$

Beweis
Ist $\tau : K_1(\alpha_1) \to L_2$ eine solche Fortsetzung, so ist $\tau(\alpha_1)$ eine Nullstelle von $p_{\alpha_1}^\sigma$. Nun ist nach dem Fortsetzungssatz τ durch $\tau(\alpha_1)$ schon eindeutig festgelegt. Da $p_{\alpha_1}^\sigma$ höchstens $\deg p_{\alpha_1}^\sigma = \deg p_{\alpha_1}$-viele Nullstellen in L_2 hat, gibt es höchstens $\deg p_{\alpha_1}$ viele τ‘s. □

14.11 Proposition

Sei $\sigma : {}^L/_K \to {}^L/_K$ ein K-Endomorphismus. Ist ${}^L/_K$ algebraisch, so ist σ bijektiv, also ein K-Automorphismus.

Beweis
Jeder K-Homomorphismus ist injektiv. Es bleibt die Surjektivität zu zeigen. Sei $\alpha \in L$. Sei

$$N = \{\beta \in L \,|\, p_\alpha(\beta) = 0\} \ni \alpha$$

Da σ ein K-Homomorphismus ist, gilt $\sigma(N) \subseteq N$. Da σ injektiv und N endlich ist, gilt $\sigma(N) = N$. Da $\alpha \in N$ gibt es $\beta \in N$ mit $\sigma(\beta) = \alpha$. □

14.12 Satz (Eindeutigkeit des Zerfällungskörpers)

Sei $\sigma : K_1 \to K_2$ ein Körperisomorphismus und $f \in K_1[X]$. Sei ${}^{L_1}/_{K_1}$ ein Zerfällungskörper von f und ${}^{L_2}/_{K_2}$ ein Zerfällungskörper von f^σ. Dann lässt sich $\sigma : K_1 \to K_2$ zu einem Körperisomorphismus $\tau : L_1 \to L_2$ fortsetzen.

Beweis
Per Induktion nach $\deg f$. Für $\deg f \leq 0$ ist nichts zu zeigen. Sei die Eindeutigkeit für alle Polynome von Grad $< n$ gezeigt.
Sei ${}^{L_1}/_{K_1}$ Zerfällungskörper von f, ${}^{L_2}/_{K_2}$ Zerfällungskörper von f^σ. Sei g ein irreduzibler Teiler von f, der keine Nullstelle in K_1 hat (Gibt es keinen solchen Teiler, so zerfällt f über K_1 und f^σ über K_2, also $L_1 = K_1, L_2 = K_2$). Sei $\alpha_1 \in L_1$ eine Nullstelle von g und $\alpha_2 \in L_2$ eine Nullstelle von g^σ. Nach dem Fortsetzungssatz (14.9) setzt sich $\sigma : K_1 \to K_2$ zu einen Körperisomorphismus $\tau_0 : K_1(\alpha_1) \to K_2(\alpha_2)$ mit $\tau_0(\alpha_1) = \alpha_2$ fort. Sei nun $\tilde{f} \in K_1(\alpha_1)[X]$ mit $f = \tilde{f} \cdot (X - \alpha_1)$. Dann ist ${}^{L_1}/_{K_1(\alpha_1)}$ ein Zerfällungskörper von $\tilde{f}$ und ${}^{L_2}/_{K_2(\alpha_2)}$ ein Zerfällungskörper von $\tilde{f}^{\tau_0}$.

Nach der Induktionsannahme gibt es eine Fortsetzung von $\tau_0 : K_1(\alpha_1) \xrightarrow{\cong} K_2(\alpha_2)$ zu $\tau : L_1 \xrightarrow{\cong} L_2$. Da τ eine Fortsetzung von τ_0 ist und τ_0 eine Fortsetzung von σ ist, ist τ eine Fortsetzung von σ. □

14.13 Korollar (Fortsetzungssatz für Zerfällungskörper)

Sei $f \in K[X]$ und L der Zerfällungskörper von f. Sei E ein Zwischenkörper von L/K und $\sigma : E/K \to L/K$ ein K-Homomorphismus. Dann gibt es eine Fortsetzung von σ zu einen K-Automorphismus von L.

Beweis
Betrachte L/E und $L/\sigma(E)$ als Zerfällungskörper von $f \in E[X]$ und $f^\sigma \in \sigma(E)[X]$. Die Eindeutigkeit liefert eine Fortsetzung von σ zu einem K-Automorphismus. $\square$

14.14 Frage

Gilt immer $\sigma(E) \subseteq E$?

Beispiel: $f = X^4 - 2 \in \mathbb{Q}[X]$. Der Zerfällungskörper ist $\mathbb{Q}(i, \sqrt[4]{2})$. Sei $E := \mathbb{Q}(\sqrt[4]{2})$. Was für $\mathbb{Q}$-Homomorphismen $E/\mathbb{Q} \to \mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q}$ gibt es?
Die Nullstellen von f sind $\sqrt[4]{2}, -\sqrt[4]{2}, i\sqrt[4]{2}, -i\sqrt[4]{2}$. Da f irreduzibel, gibt es nach dem Fortsetzungssatz genau 4 $\mathbb{Q}$-Homomorphismen $\sigma_i : \mathbb{Q}(\sqrt[4]{2}) \to L$. Diese sind bestimmt durch

$$\mathrm{id} = \sigma_1(\sqrt[4]{2}) = \sqrt[4]{2}, \quad \sigma_2(\sqrt[4]{2}) = -\sqrt[4]{2}, \quad \sigma_3(\sqrt[4]{2}) = i\sqrt[4]{2}, \quad \sigma_4(\sqrt[4]{2}) = -i\sqrt[4]{2}$$

Es ist

$$\begin{aligned} \sigma_1\big(\mathbb{Q}(\sqrt[4]{2})\big) &= \mathbb{Q}(\sqrt[4]{2}) & \qquad \sigma_2\big(\mathbb{Q}(\sqrt[4]{2})\big) &= \mathbb{Q}(\sqrt[4]{2}) \\ \sigma_3\big(\mathbb{Q}(\sqrt[4]{2})\big) &\nsubseteq \mathbb{Q}(\sqrt[4]{2}) & \qquad \sigma_4\big(\mathbb{Q}(\sqrt[4]{2})\big) &\nsubseteq \mathbb{Q}(\sqrt[4]{2}) \end{aligned}$$

14.15 Proposition (Invarianz von Zerfällungskörpern unter K-Homomorphismen)

Sei $f \in K[X]$, L eine Zerfällungskörper von f. Sei E/L eine Körpererweiterung und $\sigma : E/K \to E/K$ ein K-Homomorphismus. Dann gilt $\sigma(L) = L$

$$\begin{tikzcd} E \arrow[r, "\sigma"] & E \\ L \arrow[u, hook] \arrow[r, "\sigma|_L"] & L \arrow[u, hook] \\ K \arrow[u, hook] \arrow[r, "\cong"] & K \arrow[u, hook] \end{tikzcd}$$

Beweis
Seien $\alpha_1, \dots, \alpha_n$ die Nullstellen von f in L. Es gilt $L = K(\alpha_1, \dots, \alpha_n)$ da L Zerfällungskörper von f ist. Da σ ein K-Homomorphismus ist, gilt für $\beta \in L$:

$$f(\beta) = 0 \iff f^\sigma\big(\sigma(\beta)\big) = f\big(\sigma(\beta)\big) = 0.$$

Also gilt $\sigma(\alpha_i) \in \{\alpha_1, \dots, \alpha_n\} \subseteq L$ für alle i. Es folgt $\sigma(L) \subseteq L$. Da L/K endlich ist, folgt $\sigma(L) = L$. $\square$

14.16 Proposition

Sei $\sigma : K_1 \to K_2$ ein Körperisomorphismus, L_1/K_1 eine endliche Körpererweiterung, L_2/K_2 eine beliebige Körpererweiterung. Dann gibt es höchstens $n := [L_1 : K_1]$ viele Fortsetzungen $\tau_1, \dots, \tau_n : L_1 \to L_2$ von $\sigma : K_1 \to K_2$.

Erinnerung: Do. $L_1 = K(\alpha_1)$

Beweis
Per Induktion nach n. Für $n = 1$ ist nichts zu zeigen. Sei also $n = [L_1 : K_1] > 1$ und $\alpha \in L_1 \setminus K_1$. Wir wissen schon, dass es höchstens $m = [K_1(\alpha_1) : K_1]$ viele verschiedene Fortsetzungen $\sigma_1, \dots, \sigma_m : K_1(\alpha) \to L_1$ von σ gibt.

Nach Induktionsannahme $([L_1 : K_1(\alpha)] < [L_1 : K_1])$ gibt es zu jedem σ_i höchstens $\frac{n}{m} = [L_1 : K_1(\alpha)]$-viele Fortsetzungen $\tau_{i,j} : L_1 \to L_2$ von $\sigma_i : K_1(\alpha) \to L_2$. Nun sind die $\tau_{i,j}$ aber alle möglichen Fortsetzungen von σ. Da es höchstens $m \cdot \frac{n}{m} = n$ viele $\tau_{i,j}$ gibt, folgt die Behauptung. $\square$

14.17 Beispiel

$K_1 = K_2 = \mathbb{Q}$, $L_1 = \mathbb{Q}\big(\sqrt[4]{2}\big)$, $L_2 = \mathbb{Q}\big(\sqrt[4]{2}, i\big)$. Es gibt 4 Fortsetzungen $\sigma_1, \dots, \sigma_4 : \mathbb{Q}\big(\sqrt[4]{2}\big) \to \mathbb{Q}\big(\sqrt[4]{2}, i\big)$ von $\mathrm{id} : K_1 \xrightarrow{\cong} K_2$. Es ist $[L_1 : K_1] = \big[\mathbb{Q}\big(\sqrt[4]{2}\big) : \mathbb{Q}\big] = 4$.

15 Normale Körpererweiterungen

15.1 Definition

Eine Körpererweiterung L/K heißt **normal**, wenn folgendes gilt: Sei $f \in K[X]$ irreduzibel. Besitzt f eine Nullstelle in L, so zerfällt f über L in Linearfaktoren.
(Kurz: "eine Nullstelle $\Longrightarrow$ alle Nullstellen")

15.2 Bemerkung

L/K ist genau dann normal, wenn für alle algebraischen $\alpha \in L$ das Minimalpolynom $p_\alpha \in K[X]$ über L in Linearfaktoren zerfällt.

15.3 Beispiel

$\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ ist nicht normal. $\mathbb{Q}(\sqrt[4]{2},i)/\mathbb{Q}$ ist normal nach dem nächsten Satz.

15.4 Satz

Sei L/K eine endliche Körpererweiterung. Dann sind äquivalent:

(i) L/K ist normal

(ii) L ist ein Zerfällungskörper eines Polynoms $f \in K[X]$.

(iii) Sei E/L eine Körpererweiterung und $\tau : E/K \to E/K$ ein K-Homomorphismus. Dann gilt $\tau(L) = L$.

Beweis

(i)⇒(ii): Da L/K endlich ist, gibt es $\alpha_1, \dots, \alpha_n \in L$ mit $L = K(\alpha_1, \dots, \alpha_n)$. Da L/K normal ist, ist L der Zerfällungskörper von $p_{\alpha_1} \cdot p_{\alpha_2} \cdot \ldots \cdot p_{\alpha_n}$

(ii)⇒(iii): Heute um 10:30 :D …oder auch 14.15

(iii)⇒(i): Sei $f \in K[X]$ irreduzibel und $\alpha \in L$ eine Nullstelle von f. Sei E ein Zerfällungskörper von f über L. Sei $\beta \in E$ eine Nullstelle von f. Zu zeigen: $\beta \in L$. Nach Fortsetzungssatz gibt es einen K-Homomorphismus $\sigma : K(\alpha)/K \to E/K$ mit $\sigma(\alpha) = \beta$. Nach dem Fortsetzungssatz für Zerfällungskörper besitzt σ eine Fortsetzung zu einen K-Automorphismus $\tau : E/K \to E/K$. Nach Vorraussetzung folgt $\tau(L) = L$ also $\beta = \sigma(\alpha) = \tau(\alpha) \in L$. □

15.5 Definition

Sei L/K eine Körpererweiterung. Mit $\mathrm{Aut}(L/K)$ bezeichnen wir die Gruppe der K-Automorphismen von L/K.

15.6 Bemerkung

Sei E ein Zwischenkörper von L/K. Da jeder E-Automorphismus von L/E auch ein K-Automorphismus von L/K ist, ist $\mathrm{Aut}(L/E)$ eine Untergruppe von $\mathrm{Aut}(L/K)$.

15.7 Proposition

Sei E ein Zwischenkörper von ${}^{L}/_{K}$. Sei weiter ${}^{E}/_{K}$ normal. Dann ist $\mathrm{Aut}({}^{L}/_{E})$ eine normale Untergruppe von $\mathrm{Aut}({}^{L}/_{K})$

Beweis

$\mathrm{Aut}({}^{L}/_{E}) = \mathrm{Kern}(\mathrm{Aut}({}^{L}/_{K}) \xrightarrow{\sigma \mapsto \sigma|_E} \mathrm{Aut}({}^{E}/_{K}))$. Der Kern eines Gruppenhomomorphismus ist immer eine normale Untergruppe. □

16 Separable Körpererweiterungen

16.1 Definition

Sei $f \in K[X]$ ein Polynom von Grad n heißt **separabel**, wenn f im Zerfällungskörper von f n verschiedene Nullstellen hat.

16.2 Beispiel

(i) $X^2 + 1 \in \mathbb{Q}[X]$ ist separabel: $X^2 + 1 = (X - i)(X + i)$

(ii) $X^2 + 1 \in \mathbb{F}_2[X]$ ist nicht separabel: $X^2 + 1 = (X + 1)^2$

16.3 Definition

Die K-lineare Abbildung

$$D : K[X] \to K[X] \quad , \quad D(\sum_{i=0}^{n} a_i X^i) = \sum_{i=0}^{n} a_i \cdot i X^{i-1}$$

heißt die **formale Ableitung**.
Warnung: Für $f = X^2 \in \mathbb{F}_2[X]$ ist $Df = 2 \cdot X = 0$

16.4 Bemerkung

wurde auch in einer Übungsaufgabe im letzten Semester gezeigt

Es gilt die **Leibnizregel**:

$$\mathrm{D}(f \cdot g) = \mathrm{D}(f) \cdot g + f \cdot \mathrm{D}(g)$$

16.5 Lemma

Sei $f \in K[X]$ und $\alpha \in K$. Dann sind äquivalent:

(1) α ist mehrfache Nullstelle von f, also $(X - \alpha)^2 \mid f$

(2) $f(\alpha) = f'(\alpha) = 0$

Beweis
Schreibe $f = g(X - \alpha)^r$ mit $g(\alpha) \neq 0$. Dann ist

$$\mathrm{D}(f) = \mathrm{D}(g) \cdot (X - \alpha)^r + g \cdot \mathrm{D}((X - \alpha)^r) = \mathrm{D}(g) \cdot (X - \alpha)^r + g \cdot r(X - \alpha)^{r-1}$$

Es folgt $f(\alpha) = f'(\alpha) = 0 \iff r \geq 2$. □

16.6 Korollar

Sei $\operatorname{char} K = 0$ und f irreduzibel. Dann hat f keine mehrfachen Nullstellen und ist separabel.

Beweis
Da $\operatorname{grad} f \geq 1$ ist $f' \neq 0$. Wäre α (im Zerfällungskörper von f) eine Nullstelle von f und f', so wäre α auch eine Nullstelle vom ggT von f und f' (in $K[X]$). Da $\operatorname{grad} f' < \operatorname{grad} f$ und f irreduzibel ist, ist dieser ggT aber 1 und hat keine Nullstelle. □
(Ist $h = \mathrm{ggT}(f, f') \in K[X]$, so gibt es $k_1, k_2 \in K[X]$ mit $h = k_1 f + k_2 f'$)

16.7 Definition

Eine algebraische Körpererweiterung ${}^{L}\!/\!{}_{K}$ heißt **separabel**, falls jedes irreduzible Polynom $f \in K[X]$, das eine Nullstelle hat, separabel ist.

Kurz: "eine Nullstelle $\Rightarrow n$ verschiedene Nullstellen"

16.8 Bemerkung

Eine algebraische Körpererweiterung ${}^{L}\!/\!{}_{K}$ ist genau dann separabel, wenn alle p_α, $\alpha \in L$, separabel sind.

16.9 Bemerkung

${}^{L}\!/\!{}_{K}$ algebraisch, $\operatorname{char} K = 0 \Longrightarrow {}^{L}\!/\!{}_{K}$ ist separabel.

16.10 Bemerkung

${}^{L}\!/\!{}_{K}$ separabel, und E ist ein Zwischenkörper von ${}^{L}\!/\!{}_{K}$, dann sind auch ${}^{L}\!/\!{}_{E}$ und ${}^{E}\!/\!{}_{K}$ separabel.

16.11 Bemerkung

Ist ${}^{L}\!/\!{}_{K}$ eine endliche Körpererweiterung, so gibt es eine Körpererweiterung ${}^{N}\!/\!{}_{L}$, so dass ${}^{N}\!/\!{}_{K}$ normal ist. ${}^{L}\!/\!{}_{K}$ endlich $\Rightarrow \alpha_1, \dots, \alpha_n \in L$ mit $L = K(\alpha_1, \dots, \alpha_n)$. Sei nun N der Zerfällungskörper von

$$f := p_{\alpha_1} \cdot \ldots \cdot p_{\alpha_n} \in K[X] \subseteq L[X]$$

über L. Dann ist ${}^{N}\!/\!{}_{K}$ der Zerfällungskörper von f über K.

16.12 Satz

Sei ${}^{L}\!/\!{}_{K}$ eine endliche Körpererweiterung und ${}^{N}\!/\!{}_{L}$ eine Körpererweiterung so dass ${}^{N}\!/\!{}_{K}$ normal ist. Dann sind äquivalent:

(i) ${}^{L}\!/\!{}_{K}$ separabel

(ii) Es gibt $n = [L : K]$-viele verschiedene K-Homomorphismen $\sigma_1, \dots, \sigma_n : {}^{L}\!/\!{}_{K} \to {}^{N}\!/\!{}_{K}$.

Beweis

(i)⇒(ii): folgt aus dem Lemma 16.13

(ii)⇒(i): Sei $\alpha \in L$. Sei $\tau : {}^{L}\!/\!{}_{K} \to {}^{N}\!/\!{}_{K}$ ein K-Homomorphismus. Dann ist auch $\tau|_{K(\alpha)} : {}^{K(\alpha)}\!/\!{}_{K} \to {}^{N}\!/\!{}_{K}$ ein K-Homomorphismus. Wir wissen (Fortsetzungssatz), dass es höchstens $m = [K(\alpha) : K] = \deg p_\alpha$-viele K-Homomorphismen $\sigma_i : {}^{K(\alpha)}\!/\!{}_{K} \to {}^{L}\!/\!{}_{K}$ gibt. Weiter gibt es zu jedem σ_i höchstens $\frac{n}{m} = [L : K(\alpha)]$-viele Fortsetzungen $\tau_{ij} : {}^{L}\!/\!{}_{K} \to {}^{N}\!/\!{}_{K}$ (14.16).

Da es nach (ii) n K-Homomorphismen ${}^{L}\!/\!{}_{K} \to {}^{N}\!/\!{}_{K}$ gibt, muss es also auch m verschiedene K-Homomorphismen $\sigma_1, \dots, \sigma_m : {}^{K(\alpha)}\!/\!{}_{K} \to {}^{L}\!/\!{}_{K}$ geben. Dann sind die $\sigma_i(\alpha)$ paarweise verschieden (denn $\sigma_i(\alpha) = \sigma_j(\alpha) \Rightarrow \sigma_i = \sigma_j$). Andererseits ist jedes $\sigma_i(\alpha)$ eine Nullstelle von $p_\alpha^{\sigma_i} = p_\alpha$. Die $\sigma_i(\alpha)$ sind also die gesuchten m-vielen Nullstellen von p_α. □

16.13 Lemma

Sei $\sigma : K_1 \to K_2$ eine Körperisomorphismus. Seien ${}^{L_1}/_{K_1}$ und ${}^{L_2}/_{K_2}$ Körpererweiterungen. Dabei gelte

1) ${}^{L_1}/_{K_1}$ ist separabel und endlich
2) Für alle $\alpha \in L_1$ zerfällt $p_\alpha^\sigma \in K_2[X]$ über L_2 in Linearfaktoren.

Dann gibt es $n = [L_1 : K_1]$-viele Fortsetzungen von $\sigma : K_1 \to K_2$ zu $\tau : L_1 \to L_2$.

Beweis
Per Induktion nach n. Für $n = 1$ ist nichts zu zeigen. Sei $\alpha \in L_1 \setminus K_1$. Da p_α separabel ist, hat p_α nach Vorraussetzung $m = \operatorname{grad} p_\alpha = [K_1(\alpha) : K_1]$-viele verschiedene Nullstellen $\beta_1, \ldots, \beta_m$ in L_2. Nach dem Fortsetzungssatz (14.9) gibt es zu jeder dieser Nullstellen eine Fortsetzung $\tau_i : K_1(\alpha) \to L_2$ von $\sigma : K_1 \to K_2$ mit $\tau_i(\alpha) = \beta_i$. Für jedes τ_i gibt es nach Induktionsannahme $\frac{n}{m} = [L_1 : K_1(\alpha)]$-viele Fortsetzungen $\tau_{ij} : L_1 \to L_2$ von τ_i. Insgesamt gibt es $m \cdot \frac{n}{m}$ viele Fortsetzungen von σ. □

16.14 Korollar

Sei ${}^{L}/_{K}$ eine Körpererweiterung. Sei $\alpha \in L$ algebraisch über K. Ist $p_\alpha \in K[X]$ separabel, so ist ${}^{K(\alpha)}/_{K}$ separabel.

Beweis
Sei ${}^{N}/_{K(\alpha)}$ eine Körpererweiterung, so dass ${}^{N}/_{K}$ normal ist. Da p_α separabel ist, gibt es nach Fortsetzungssatz (14.9) $n = [K(\alpha) : K] = \operatorname{grad} p_\alpha$-viele K-Homomorphismen ${}^{K(\alpha)}/_{K} \to {}^{N}/_{K}$. nach Satz 16.12 ist ${}^{K(\alpha)}/_{K}$ separabel. □

16.15 Satz vom primitiven Element

Sei ${}^{L}/_{K}$ eine endliche und separable Körpererweiterung. Dann gibt es $\alpha \in L$ mit $L = K(\alpha)$.

Beweis
Da ${}^{L}/_{K}$ endlich ist, gibt es $\alpha_1, \ldots, \alpha_n \in L$ mit $L = K(\alpha_1, \ldots, \alpha_n)$. Die Behauptung folgt per Induktion aus folgendem Lemma 16.16 □

16.16 Lemma

Sei ${}^{L}/_{K}$ eine separable Körpererweiterung. Seien $\alpha, \beta \in L$. Dann gibt es $\gamma \in L$ mit $K(\alpha, \beta) = K(\gamma)$.

Beweis (für den Fall $|K| = \infty$)
Mit ${}^{L}/_{K}$ ist auch ${}^{K(\alpha,\beta)}/_{K}$ separabel. Sei ${}^{N}/_{K(\alpha,\beta)}$ eine Körpererweiterung, so dass ${}^{N}/_{K}$ normal ist. Dann gibt es $n = [K(\alpha, \beta) : K]$-viele K-Homomorphismen $\sigma_1, \ldots, \sigma_n : K(\alpha, \beta) \to {}^{N}/_{K}$. Da die σ_i verschieden sind, gilt für $i \neq j : \sigma_i(\alpha) \neq \sigma_j(\alpha)$ oder $\sigma_i(\beta) \neq \sigma_j(\beta)$. Für $i \neq j$ gilt also

$$0 \neq \big(\sigma_i(\alpha) - \sigma_j(\alpha)\big) + \big(\sigma_i(\beta) - \sigma_j(\beta)\big)X = (\sigma_i(\alpha) + \sigma_i(\beta)X) - (\sigma_j(\alpha) + \sigma_j(\beta)X) \in N[X]$$

Betrachte

$$f = \prod_{i \neq j} \big((\sigma_i(\alpha) + \sigma_i(\beta)X) - (\sigma_j(\alpha) + \sigma_j(\beta)X)\big) \neq 0$$

Da $|K| = \infty$ und $f \neq 0$, gibt es $x \in K$ mit $f(x) \neq 0$. Es folgt, dass die Elemente $\sigma_i(\alpha) + \sigma_i(\beta)x = \sigma_i(\alpha + \beta x)$ paarweise verschieden sind. Sei $\gamma := \alpha + \beta x \in L$. Da die $\sigma_i(\gamma)$ alle Nullstellen von p_γ sind, folgt $[K(\gamma) : K] \geq n = [K(\alpha, \beta) : K]$. Da $\gamma \in K(\alpha, \beta)$ folgt $K(\gamma) \subseteq K(\alpha, \beta)$ und damit insgesamt $K(\gamma) = K(\alpha, \beta)$. □

17 Galois-Theorie

17.1 Definition

Eine algebraische Körpererweiterung ${}^{L}/{}_{K}$ heißt eine **Galois-Erweiterung** (oder galoissch), wenn sie normal und separabel ist. Dann heißt $\mathrm{Gal}({}^{L}/{}_{K}) := \mathrm{Aut}({}^{L}/{}_{K})$ die **Galois-Gruppe** von ${}^{L}/{}_{K}$.

17.2 Bemerkung

Sei E ein Zwischenkörper von ${}^{L}/{}_{K}$.

(i) Ist ${}^{L}/{}_{K}$ separabel, so ist auch ${}^{E}/{}_{K}$ und ${}^{L}/{}_{E}$ separabel.

Beweis für Letzteres: Sei $\alpha \in L$ und $p_\alpha^E \in E[X]$ das Minimalpolynom von α über E und p_α^K das Minimalpolynom von α über K. Dann gilt $p_\alpha^E \mid p_\alpha^K$ in $E[X]$. Da p_α^K separabel ist, ist auch p_α^E separabel.

(ii) Ist ${}^{L}/{}_{K}$ normal, so ist auch ${}^{L}/{}_{E}$ normal. Beweis: Gleiches Argument wie eben.

(iii) Ist ${}^{L}/{}_{K}$ galoissch, so ist auch ${}^{L}/{}_{E}$ galoisch.

17.3 Proposition 1

Sei ${}^{L}/{}_{K}$ eine endliche Galoiserweiterung. Dann gilt $|\mathrm{Gal}({}^{L}/{}_{K})| = [L : K]$.

Beweis
Nach dem Satz vom primitiven Element (16.15) gibt es $\alpha \in L$ mit $L = K(\alpha)$. Da ${}^{L}/{}_{K}$ normal ist, zerfällt p_α über L in Linearfaktoren. Da ${}^{L}/{}_{K}$ separabel ist, besitzt p_α $n = [L : K] = \mathrm{grad}\, p_\alpha$-viele Nullstellen in L. Nach dem Fortsetzungssatz gibt es genau n-viele K-Homomorphismen $\sigma_i : {}^{L}/{}_{K} \to {}^{L}/{}_{K}$ (Diese wenden durch $\sigma_i(\alpha)$ bestimmt; die $\sigma_i(\alpha)$ sind genau die Nullstellen von p_α).

Da ${}^{L}/{}_{K}$ algebraisch (also sogar endlich) ist, sind die σ_i Automorphismen. Es folgt $\mathrm{Gal}({}^{L}/{}_{K}) = \{\sigma_1, \ldots, \sigma_n\}$. Insbesondere

$$|\mathrm{Gal}({}^{L}/{}_{K})| = n = [L : K]$$ □

17.4 Definition

Sei G eine Untergruppe von $\mathrm{Aut}({}^{L}/{}_{K})$. Dann heißt $L^G := \{\alpha \in L \mid \sigma(\alpha) = \alpha \text{ für alle } \sigma \in G\}$ der **Fixkörper** von G.

17.5 Bemerkung

Für $\alpha, \beta \in L^G$ und $\sigma \in G$ gilt:

- $\sigma(\alpha + \beta) = \sigma(\alpha) + \sigma(\beta) = \alpha + \beta$, also $\alpha + \beta \in L^G$.
- $\sigma(\alpha \cdot \beta) = \sigma(\alpha) \cdot \sigma(\beta) = \alpha \cdot \beta$, also $\alpha \cdot \beta \in L^G$.
- $\sigma(-\alpha) = -\sigma(\alpha) = -\alpha$, also $-\alpha \in L^G$.
- Falls $\alpha \neq 0$: $\sigma(\alpha^{-1}) = \sigma(\alpha)^{-1} = \alpha^{-1}$, also $\alpha^{-1} \in L^G$.
- Für alle $\lambda \in K$ ist $\sigma(\lambda) = \lambda$, also $K \subseteq L^G$.

L^G ist also ein Zwischenkörper von ${}^{L}/{}_{K}$.

17.6 Proposition 2

Sei ${}^L/_K$ eine Körpererweiterung. Sei G eine endliche Untergruppe von $\mathrm{Aut}({}^L/_K)$. Sei $E := L^G$. Dann ist ${}^L/_E$ eine endliche Galois-Erweiterung mit $\mathrm{Gal}({}^L/_E) = G$. Insbesondere ist $[L : E] = |G|$.

Beweis
Zu $\alpha \in L$ sei $G_\alpha = \{\sigma \in G \mid \sigma(\alpha) = \alpha\}$ die Standgruppe von α und

$$f_\alpha := \prod_{\sigma G_\alpha \in {}^G/_{G_\alpha}} \big(X - \sigma(\alpha)\big)$$

Für $\tau \in G$ gilt

$$f_\alpha^\tau = \prod_{\sigma G_\alpha \in {}^G/_{G_\alpha}} \big(X - \tau\sigma(\alpha)\big) = \prod_{\sigma G_\alpha \in {}^G/_{G_\alpha}} \big(X - \sigma(\alpha)\big) = f_\alpha$$

Es folgt $f_\alpha \in E[X]$. Für $\sigma, \tau \in G$ gilt

$$\sigma(\alpha) = \tau(\alpha) \iff \tau^{-1}\sigma(\alpha) = \alpha \iff \tau^{-1}\sigma \in G_\alpha \iff \tau G_\alpha = \sigma G_\alpha$$

Daher sind die Nullstellen von f_α paarweise verschieden. Sei $p_\alpha \in E[X]$ das Minimalpolynom von α. Da $f_\alpha(\alpha) = 0$ gilt $p_\alpha \mid f_\alpha$. Damit hat p_α keine doppelten Nullstellen und zerfällt über L in Linearfaktoren. Daher ist ${}^L/_E$ separabel und normal. Wegen $f_\alpha(\alpha) = 0$ ist ${}^L/_E$ auch algebraisch. Insgesamt ist ${}^L/_E$ eine Galois-Erweiterung.

Wir zeigen als nächstes $[L : L^G] \leq |G|$. Angenommen: $[L : L^G] \gneq |G|$. Dann gibt es einen Zwischenkörper E von ${}^L/_{L^G}$ mit ${}^E/_{L^G}$ endlich und $[E : L^G] \gneq |G|$. Da mit ${}^L/_{L^G}$ auch ${}^E/_{L^G}$ separabel ist, gibt es nach dem Satz vom primitiven Element (16.15) $\alpha \in E$ mit $E = L^G(\alpha)$. Es ist

$$[L^G(\alpha) : L^G] = \mathrm{grad}\, p_\alpha \overset{f_\alpha(\alpha)=0}{\leq} \mathrm{grad}\, f_\alpha \leq |G| \lightning$$

Es gilt also $[L : L^G] \leq |G|$. Nach Proposition 1 (17.3) ist $[L : L^G] = |\mathrm{Gal}({}^L/_{L^G})|$. Es ist aber G eine Untergruppe von $\mathrm{Gal}({}^L/_{L^G})$. Es folgt $G = \mathrm{Gal}({}^L/_{L^G})$ (da $|\mathrm{Gal}({}^L/_{L^G})| \leq |G|$). □

17.7 Bemerkung

Sei ${}^L/_K$ eine Körpererweiterung. Seien

$$\begin{aligned} \mathcal{Z}({}^L/_K) &= \text{ die Menge aller Zwischenkörper von } {}^L/_K \\ \mathcal{U}({}^L/_K) &= \text{ die Menge aller Untergruppen von } \mathrm{Aut}({}^L/_K) \end{aligned}$$

Wir haben Abbildungen:

$$\begin{aligned} \mathrm{ug} : \mathcal{Z}({}^L/_K) \to \mathcal{U}({}^L/_K) &\quad \mathrm{ug}(E) := \mathrm{Aut}({}^L/_E) \\ \mathrm{zw} : \mathcal{U}({}^L/_K) \to \mathcal{Z}({}^L/_K) &\quad \mathrm{zw}(G) := L^G \end{aligned}$$

Diese erfüllen

$$\begin{aligned} H \leq G &\Longrightarrow \mathrm{zw}(H) \supseteq \mathrm{zw}(G) \\ E \subseteq F &\Longrightarrow \mathrm{ug}\,(E) \geq \mathrm{ug}(F) \end{aligned}$$

17.8 Hauptsatz der Galois-Theorie (für endliche Galois-Erweiterungen)

Sei ${}^L/_K$ eine endliche Galois-Erweiterung. Dann gelten:

(1) ug und zw sind zueinander inverse Abbildungen zwischen der Menge der Untergruppen von $\mathrm{Gal}({}^L/_K)$ der Menge der Zwischenkörper von ${}^L/_K$.

(2) Für $E \in \mathcal{Z}(L/K)$ gilt $[L : E] = |\mathrm{Gal}(L/E)|$.

(3) Sei E ein Zwischenkörper von L/K. Dann ist E/K genau dann normal (und damit galoissch), falls $H := \mathrm{ug}(E) = \mathrm{Gal}(L/E)$ ein Normalteiler von $\mathrm{Gal}(L/K)$ ist. In diesem Fall ist $\mathrm{Gal}(L/E)$ der Kern des surjektiven Gruppenhomomorphismus $\mathrm{Gal}(L/K) \to \mathrm{Gal}(E/K), \sigma \mapsto \sigma\big|_E$. Insbesondere ist

$$\mathrm{Gal}(E/K) \cong \mathrm{Gal}(L/K)/\mathrm{Gal}(L/E).$$

Beweis

(1) Sei $H \leq \mathrm{Gal}(L/K)$. Dann ist nach Proposition 2 (17.6) $H = \mathrm{Gal}(L/L^H)$. Also $\mathrm{ug} \circ \mathrm{zw}(H) = H$. Sei $E \in \mathcal{Z}(L/K)$. Dann ist sicher $E \subseteq L^{\mathrm{Gal}(L/E)}$. Nach Proposition 1& 2 gilt

$$[L : L^{\mathrm{Gal}(L/E)}] \overset{\text{Prop. 1 \& 2}}{=} |\mathrm{Gal}(L/E)| \overset{\text{Prop. 1}}{=} [L : E]$$

Es folgt $E = L^{\mathrm{Gal}(L/E)}$. Also ist $\mathrm{zw} \circ \mathrm{ug}(E) = E$.

(2) Haben wir schon in Proposition 1 (17.3) gesehen.

(3) Sei $E \in \mathcal{Z}(L/K)$ und E/K normal. In Kapitel 14 haben wir gesehen, dass sich jedes $\sigma \in \mathrm{Gal}(L/K)$ zu einem Element $\sigma\big|_E \in \mathrm{Gal}(E/K)$ einschränkt (Da $\sigma(E) \subseteq E$). Wir erhalten einen Gruppenhomomorphismus

$$\mathrm{Gal}(L/K) \xrightarrow{\varphi} \mathrm{Gal}(E/K) \text{ mit } \varphi(\sigma) := \sigma\big|_E$$

und es ist $\mathrm{Kern}\,\varphi = \mathrm{Gal}(L/E)$. Insbesondere ist $\mathrm{Gal}(L/E)$ normal in $\mathrm{Gal}(L/K)$. Weiter gilt

$$|\mathrm{Im}\,\varphi| = \frac{|\mathrm{Gal}(L/K)|}{|\mathrm{Gal}(L/E)|} = \frac{[L : K]}{[L : E]} = [E : K] = |\mathrm{Gal}(E/K)|$$

Also ist φ surjektiv.

Sei umgekehrt $H \trianglelefteq \mathrm{Gal}(L/K)$ eine normale Untergruppe. Sei $E = L^H$. Sei $\alpha \in E$ und $\sigma \in \mathrm{Gal}(L/K)$. Für $\tau \in H = \mathrm{Gal}(L/E)$ gilt

$$\tau\big(\sigma(\alpha)\big) = \sigma \underbrace{\sigma^{-1}\tau\sigma}_{\in H,\text{ da } H \text{ normal}} (\alpha) \overset{\alpha \in E = L^H}{=} \sigma(\alpha)$$

Es folgt $\sigma(\alpha) \in E = L^H$. Also $\sigma(E) = E$. Sei $G := \left\{\sigma\big|_E \,\middle|\, \sigma \in \mathrm{Gal}(L/K)\right\} \leq \mathrm{Aut}(E/K)$. Dann ist

$$K \subseteq E^G \subseteq L^{\mathrm{Gal}(L/K)} = K$$

Also $E^G = K$. Nach Prop. 2 (17.6) ist $E/K = E/E^G$ dann galoissch und insbesondere normal. $\square$

17.9 Definition

Sei $f \in K[X]$ separabel. Sei L der Zerfällungskörper von f (Dann ist L/K galoissch.). Dann heißt $\mathrm{Gal}_K(f) := \mathrm{Gal}(L/K)$ die **Galois-Gruppe** von f über K.

17.10 Beispiel

Sei $f = X^3 - 2 \in \mathbb{Q}[X]$. Der Zerfällungskörper von f ist $\mathbb{Q}(\sqrt[3]{2}, \zeta\sqrt[3]{2}, \zeta^2\sqrt[3]{2}) = \mathbb{Q}(\sqrt[3]{2}, \zeta)$ mit $\zeta = e^{2\pi i/3}$.
Behauptung: $\mathrm{Gal}_{\mathbb{Q}}(f) \cong S_3$.

Beweis

Sei $Z := \left\{\sqrt[3]{2}, \zeta\sqrt[3]{2}, \zeta^2\sqrt[3]{2}\right\}$ die Menge der Nullstellen von f. Für $\sigma \in \mathrm{Gal}_{\mathbb{Q}}(f)$ gilt $\sigma(Z) = Z$. Wir erhalten also eine Wirkung der Gruppe $\mathrm{Gal}_{\mathbb{Q}}(f)$ auf Z. In anderen Worten erhalten wir einen Gruppenhomomorphismus $\varphi : \mathrm{Gal}_{\mathbb{Q}}(f) \to S_Z \cong S_3$. Da $\mathbb{Q}(\sqrt[3]{2}, \zeta) = \mathbb{Q}(Z)$ ist φ injektiv. Da $|\mathrm{Gal}_{\mathbb{Q}}(f)| = [\mathbb{Q}(\sqrt[3]{2}, \zeta) : \mathbb{Q}] = 6 = |S_3|$ folgt $\mathrm{Gal}_Q(f) \cong S_3$. $\square$

17.11 Bemerkung

Ist $f \in K[X]$ separabel und $n = \deg f$, so hat f im Zerfällungskörper L von f n verschiedene Nullstellen. Wir erhalten eine Wirkung von $\mathrm{Gal}_K(f)$ auf der Menge der Nullstellen und einen injektiven Gruppenhomomorphismus $\mathrm{Gal}_K(f) \to S_n$ (Injektivität: $L = K(M)$). Insbesondere

$$[L : K] = |\mathrm{Gal}_K(f)| \leq |S_n| = n!$$

17.12 Beispiel

Der Zerfällungskörper von $X^4 - 2 \in \mathbb{Q}[X]$ ist $\mathbb{Q}(\sqrt[4]{2}, i)$. Es ist

$$\Big[\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}\Big] = \Big[\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}(\sqrt[4]{2})\Big] \cdot \Big[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}\Big] = 2 \cdot 4 = 8$$

Insbesondere $|\mathrm{Gal}_{\mathbb{Q}}(X^4 - 1)| = 8$, aber $|S_4| = 24$.

18 Der Fundamentalsatz der Algebra

18.1 Definition

Ein Körper K heißt **algebraisch abgeschlossen**, wenn jedes Polynom $f \in K[X]$ von Grad ≥ 1 eine Nullstelle in K besitzt.

18.2 Bemerkung

Ist K algebraisch abgeschlossen, so zerfällt jedes Polynom über K in Linearfaktoren.

18.3 Bemerkung

K ist genau dann algebraisch abgeschlossen, wenn es keine endliche Körpererweiterung L/K gibt mit $[L : K] \geq 2$. (Übung)

18.4 Fundamentalsatz der Algebra

Der Körper $\mathbb{C}$ ist algebraisch abgeschlossen.

18.5 Bemerkung

Wir wissen schon (teilweise mit Mitteln der Analysis):

a) Jedes Polynom $f \in \mathbb{C}[X]$ vom Grad 2 hat eine Nullstelle in $\mathbb{C}$. (quadratische Erweiterung)

b) Jedes Polynom $f \in \mathbb{R}[X]$ von ungeradem Grad besitzt eine Nullstelle in $\mathbb{R}$. (ZWS)

18.6 Lemma

a) Es gibt keine Körpererweiterung $L/\mathbb{C}$ mit $[L : \mathbb{C}] = 2$.

b) Sei $L/\mathbb{R}$ eine Körpererweiterung $L/\mathbb{R}$ von ungeradem Grad $[L : \mathbb{R}] \geq 3$. Dann gilt $L = \mathbb{R}$.

Beweis

a) Angenommen doch. Sei $\alpha \in L \setminus \mathbb{C}$. Dann ist $p_\alpha \in \mathbb{C}[X]$ ein irreduzibles Polynom vom Grad$= 2$. $\lightning$

b) Sei $\alpha \in L$. Dann ist auch $\mathbb{R}(\alpha)/\mathbb{R}$ eine Körpererweiterung von ungeradem Grad. Damit ist $p_\alpha \in \mathbb{R}[X]$ ein irreduzibles Polynom von ungeradem Grad. Es folgt $\deg p_\alpha = 1$ und $\alpha \in \mathbb{R}$. $\square$

18.7 Bemerkung

Ist $L/\mathbb{C}$ eine endliche Körpererweiterung. Da $\operatorname{char} \mathbb{C} = 0$ ist $L/\mathbb{C}$ separabel. Es gibt eine endliche Körpererweiterung N/L, so dass $N/\mathbb{C}$ normal und damit galoissch ist. Um den Fundamentalsatz zu beweisen, genügt es daher zu zeigen, dass es keine (endlichen) Galoiserweiterungen von $\mathbb{C}$ gibt.

18.8 Lemma 2

Sei ${}^{L}/_{\mathbb{R}}$ eine endliche Galoiserweiterung. Dann gilt $[L : \mathbb{R}] = 2^k$ mit $k \in \mathbb{N}$.

Beweis
Sei H eine 2-Sylowuntergruppe von $G := \mathrm{Gal}({}^{L}/_{\mathbb{R}})$. Dann gilt $|H| = 2^k$ und $[G : H]$ ist ungerade. Sei $E := L^H$. Mit dem Hauptsatz der Galois-Theorie (17.8) folgt: $\mathrm{Gal}({}^{L}/_{E}) = H$ und $[L : E] = |H| = 2^k$. Ebenfalls mit dem Hauptsatz der Galois-Theorie folgt

$$[L : \mathbb{R}] = |G| = |H| \cdot [G : H].$$

Es folgt, dass $[E : \mathbb{R}] = [G : H]$ ungerade ist. Damit folgt $E = \mathbb{R}$. Also $[L : \mathbb{R}] = [L : E] = 2^k$. □

18.9 Proposition

Sei p eine Primzahl und P eine p-Gruppe. Dann gibt es eine Folge $\{e\} = N_0 \trianglelefteq N_1 \trianglelefteq N_2 \trianglelefteq \ldots \trianglelefteq N_k = P$ von Normalteilern mit $|N_i| = p^i$.

Beweis
Sei $|P| = p^k$. Induktion nach k. Für $k = 0$ ist nicht zu zeigen.
Induktionsschritt: $k - 1 \mapsto k$ Sei $|P| = p^k$.
Da P eine p-Gruppe ist, ist das Zentrum von P nichttrivial (Kapitel 3). Sei $z \in P$ ein nicht-triviales zentrales Element. Da $\mathrm{ord}(z)$ die Ordnung von P teilt, gilt $\mathrm{ord}(z) = p^l$ für ein l. Dann ist $g := z^{p^{l-1}}$ ein nicht-triviales zentrales Element der Ordnung p. Dann ist $N_1 := \langle g \rangle$ ein Normalteiler mit $|N_1| = p$.

Nun wenden wir die Induktionsannahme auf $Q := {}^{P}/_{N_1}$ an (Es ist $|Q| = \frac{|P|}{|N_1|} = p^{k-1}$). Wir erhalten Normalteiler:

$$\{e\} = M_0 \trianglelefteq M_1 \trianglelefteq \ldots \trianglelefteq M_{k-1} = Q$$

mit $|M_i| = p^i$. Sei $\pi : P \to Q$ die Quotientenabbildung. Dann sind die $N_i := \pi^{-1}(M_{i-1})$ für $i = 1, \ldots, k$ die gesuchten Normalteiler. □

18.10 Korollar

Sei p eine Primzahl und ${}^{L}/_{K}$ eine Galoiserweiterung von Grad p^k. Dann gibt es eine Folge von Zwischenkörpern

$$K = E_0 \subseteq E_1 \subseteq \ldots \subseteq E_k = L$$

mit $[E_i : K] = p^i$ und $[E_i : E_{i-1}] = p$.

Beweis
Für $P := \mathrm{Gal}({}^{L}/_{K})$ gilt nach dem Hauptsatz $|P| = [L : K] = p^k$. Mit Proposition 18.9 folgt:

$$\exists \{e\} = N_0 \trianglelefteq N_1 \trianglelefteq \ldots \trianglelefteq N_k = P \quad \text{mit } |N_i| = p^i$$

Setze nun $E_i := L^{N_{k-i}}$. Dann $K = E_0 \subseteq E_1 \subseteq \ldots \subseteq E_k = L$ und nach dem Hauptsatz folgt

$$[E_i : K] = \frac{[L : K]}{[L : E_i]} = \frac{p^k}{p^{k-i}} = p^i.$$ □

18.11 Beweis des Fundamentalsatzes

Sei ${}^{L}/_{\mathbb{C}}$ eine endliche Körpererweiterung. Zu zeigen ist $L = \mathbb{C}$. Es ist auch ${}^{L}/_{\mathbb{R}}$ eine endliche Körpererweiterung. Sei ${}^{N}/_{L}$ eine Körpererweiterung für die ${}^{N}/_{\mathbb{R}}$ normal und damit galoissch ist. Wegen Lemma 2 (18.8) ist der Grad von ${}^{N}/_{\mathbb{R}}$ und damit der auch der Grad von ${}^{N}/_{\mathbb{C}}$ eine 2er-Potenz. Da ${}^{N}/_{\mathbb{R}}$ galoissch ist, ist auch ${}^{N}/_{\mathbb{C}}$ galoissch und die Galoisgruppe von ${}^{N}/_{\mathbb{C}}$ eine 2-Gruppe, $\mathrm{Gal}({}^{N}/_{\mathbb{C}}) = 2^k$. Ist $k = 0$ so folgt mit dem Hauptsatz der Galoistheorie $N = \mathbb{C}$ und damit $L = \mathbb{C}$.

Angenommen $k \geq 1$. Nach dem Korollar gibt es dann einen Zwischenkörper E von ${}^{N}/_{\mathbb{C}}$ mit $[E : \mathbb{C}] = 2$ im Widerspruch zu Lemma 1 (18.6) a). □

19 Einheitswurzeln

19.1 Definition

Sei K ein Körper. $\zeta \in K$ heißt eine **n-te Einheitswurzel**, falls $\zeta^n = 1$. Die n-ten Einheitswurzeln bilden eine Gruppe $E_n(K)$ bezüglich Multiplikation in K. ζ heißt eine **primitive n-te Einheitswurzel** falls $\zeta^n = 1$ aber $\zeta^k \neq 1$ für $0 < k \leq n-1$. Die Menge der primitiven Einheitswurzeln bezeichnen wir mit $PE_n(K)$.

19.2 Bemerkung

$\zeta \in E_n(K)$ ist genau dann eine primitive Einheitswurzel, wenn ζ ein Erzeuger von $E_n(K)$ ist, also $\langle\zeta\rangle = E_n(K)$.

19.3 Beispiel

$$\begin{aligned} E_n(\mathbb{C}) &= \left\{ e^{2\pi i k/n} \,\middle|\, 0 \leq k \leq n-1 \right\} \cong \mathbb{Z}/n\mathbb{Z} \\ PE_n(\mathbb{C}) &= \left\{ e^{2\pi i k/n} \,\middle|\, 1 \leq k \leq n-1, \operatorname{ggT}(k,n) = 1 \right\} \end{aligned}$$

19.4 Bemerkung

Für die Einheitengruppe des Rings $\mathbb{Z}/n\mathbb{Z}$ gilt

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{k + n\mathbb{Z} \mid 1 \leq k \leq n-1, \operatorname{ggT}(k,n) = 1\}.$$

Insbesondere ist $|PE_n(\mathbb{C})| = |(\mathbb{Z}/n\mathbb{Z})^\times|$.

19.5 Definition

Für $n \in \mathbb{N}_{>0}$ setzen wir $\varphi(n) := |(\mathbb{Z}/n\mathbb{Z})^\times|$. Die so erklärte Funktion $\varphi : \mathbb{N}_{>0} \to \mathbb{N}_{>0}$ heißt die **Eulersche φ-Funktion**. Es ist $\varphi(n) = |PE_n(\mathbb{C})|$.

19.6 Lemma

(i) Ist p eine Primzahl so gilt $\varphi(p) = p - 1$ und $\varphi(p^\nu) = (p-1) \cdot p^{\nu-1}$.

(ii) Ist $\operatorname{ggT}(n,m) = 1$ so gilt $\varphi(n \cdot m) = \varphi(n) \cdot \varphi(m)$.

(iii) Ist $n = p_1^{\nu_1} \cdot \ldots \cdot p_r^{\nu_r}$ die Primfaktorzerlegung von n mit paarweise verschiedenen Primzahlen p_i so gilt

$$\varphi(n) = \prod_{i=1}^{r} (p_i - 1) \cdot p_i^{\nu_i - 1}$$

Beweis

(i) Es ist $\operatorname{ggT}(p^\nu, k) > 1$ genau dann wenn $p \mid k$. Es folgt

$$\begin{aligned} \varphi(p^\nu) = |\left\{ k \,\middle|\, 1 \leq k \leq p^\nu - 1, p \nmid k \right\}| &= (p^\nu - 1) - |\left\{ k \,\middle|\, 1 \leq k \leq p^\nu - 1, p \mid k \right\}| \\ &= (p^\nu - 1) - |\{p, 2 \cdot p, \ldots, (p^{\nu-1} - 1) \cdot p\}| \\ &= (p^\nu - 1) - (p^{\nu-1} - 1) = p^\nu - p^{\nu-1} = (p-1)p^{\nu-1}. \end{aligned}$$

(ii) Nach dem Chinesischen Restsatz (6.18) gibt es einen Ringisomorphismus $\mathbb{Z}/n\cdot m\mathbb{Z} \xrightarrow{\cong} \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$, $k + nm\mathbb{Z} \mapsto (k + n\mathbb{Z}, k + m\mathbb{Z})$, da n und m teilerfremd sind. Wegen

$$(\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z})^{\times} = (\mathbb{Z}/n\mathbb{Z})^{\times} \times (\mathbb{Z}/m\mathbb{Z})^{\times}$$

folgt die Behauptung.

(iii) folgt aus (i) und (ii) □

19.7 Korollar

$$|PE_n(\mathbb{C})| = \varphi(n)$$

19.8 Definition

Sei $\zeta \in PE_n(\mathbb{C})$. Dann heißt $\mathbb{Q}_n := \mathbb{Q}(\zeta)$ der **n-te Kreisteilungskörper**.

19.9 Bemerkung

Mit ζ liegen alle n-ten Einheitswurzeln in $\mathbb{Q}_n$. $\mathbb{Q}_n$ ist der Zerfällungskörper von $X^n - 1 \in \mathbb{Q}[X]$. Insbesondere ist $\mathbb{Q}_n/\mathbb{Q}$ normal. Da algebraische Erweiterungen von $\mathbb{Q}$ $(\operatorname{char} \mathbb{Q} = 0)$ immer separabel sind, ist $\mathbb{Q}_n/\mathbb{Q}$ eine Galois-Erweiterung.

19.10 Lemma 1

Es gibt einen injektiven Gruppenhomomorphismus

$$\psi : \operatorname{Gal}(\mathbb{Q}_n/\mathbb{Q}) \to (\mathbb{Z}/n\mathbb{Z})^{\times}$$

Beweis
Sei $\sigma \in \operatorname{Gal}(\mathbb{Q}_n/\mathbb{Q})$. Dann permutiert σ die Nullstellen von $X^n - 1$ und induziert einen Gruppenhomomorphismus $\sigma|_{E_n(\mathbb{C})} : E_n(\mathbb{C}) \to E_n(\mathbb{C})$. Insbesondere gilt $\sigma(PE_n) \subseteq PE_n$. Sei $\zeta := e^{2\pi i/n} \in PE_n$. Definiere nun $\psi(\sigma) := k + n\mathbb{Z}$ durch $\sigma(\zeta) = \zeta^k$. Da $\mathbb{Q}_n = \mathbb{Q}(\zeta)$ gilt

$$\sigma = \mathrm{id} \iff \sigma(\zeta) = \zeta \iff k + n\mathbb{Z} = 1_{\mathbb{Z}/n\mathbb{Z}}$$

Für $\sigma, \tau \in \operatorname{Gal}(\mathbb{Q}_n/\mathbb{Q})$ mit $\sigma(\zeta) = \zeta^k$ und $\tau(\zeta) = \zeta^l$ gilt

$$\sigma \circ \tau(\zeta) = \sigma(\zeta^l) = \sigma(\zeta)^l = \zeta^{k \cdot l}$$

Daher ist ψ ein Gruppenhomomorphismus und somit injektiv wegen $(\star)$. □

19.11 Definition

$$\Phi_n := \prod_{\zeta \in PE_n(\mathbb{C})} (X - \zeta)$$

heißt das **n-te Kreisteilungspolynom**. Es ist $\deg \Phi_n = \varphi(n)$ und die primitiven Einheitswurzeln sind gerade die Nullstellen von Φ_n.

19.12 Lemma

Seien $f \in \mathbb{Z}[X], g \in \mathbb{C}[X]$ normiert mit $f \cdot g \in \mathbb{Z}[X]$. Dann gilt $g \in \mathbb{Z}[X]$.

Beweis
Nach einem Korollar zum Gauß-Lemma (8.14) genügt es zu zeigen $g \in \mathbb{Q}[X]$. Sei $f = a_n X^n + a_{n-1}X^{n-1} + \ldots + a_0$ und $g = b_m X^m + b_{m-1}X^{m-1} + \ldots + b_0$. O.B.d.A. können wir $a_0 \neq 0$ annehmen. (Sonst ersetzen wir f durch $f \cdot X^{-l}$ für geeignetes l.)

Mit $f \cdot g \in \mathbb{Z}[X]$ folgt $\sum_{i+j=k} a_i \cdot b_j \in \mathbb{Z}$ für alle k. Insbesondere ist

$$b_k - \frac{1}{a_0} \sum_{i=1}^{k} a_i \cdot b_{k-i} \in \mathbb{Q}.$$

Per Induktion folgt $b_k \in \mathbb{Q}$ für alle k. Also $g \in \mathbb{Q}[X]$. □

19.13 Lemma 2

$$\Phi_n \in \mathbb{Z}[X]$$

Beweis
Es ist

$$X^n - 1 = \prod_{\zeta \in E_n} (X - \zeta) = \prod_{d|n} \prod_{\substack{\zeta \in E_n \\ \operatorname{ord}(\zeta)=d}} (X - \zeta) = \prod_{d|n} \prod_{\zeta \in PE_d} (X - \zeta) = \prod_{d|n} \Phi_d.$$

Wir zeigen nun $\Phi_n \in \mathbb{Z}[X]$ per Induktion nach n. Für $n = 1$ ist $\Phi_1 = X - 1 \in \mathbb{Z}[X]$. Für $n > 1$ ist

$$\Phi_n \cdot \underbrace{\prod_{d|n,\, d \neq n} \Phi_d}_{\text{I.A.: } \in \mathbb{Z}[X]} = \underbrace{X^n - 1}_{\in \mathbb{Z}[X]}$$

Die Behauptung folgt aus dem vorigen Lemma. □

19.14 Satz

a) Φ_n ist irreduzibel in $\mathbb{Q}[X]$.

b) $[\mathbb{Q}_n : \mathbb{Q}] = \varphi(n)$.

c) $\operatorname{Gal}(\mathbb{Q}_n/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$.

Beweis
Gilt a), so ist Φ_n das Minimalpolynom für (jedes) $\zeta \in PE_n$ und b) folgt. Wegen Lemma 1 (19.10) und

$$|\operatorname{Gal}(\mathbb{Q}_n/\mathbb{Q})| = [\mathbb{Q}_n : \mathbb{Q}] \overset{\text{b)}}{=} \varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$$

ist c) eine Folgerung aus b). Es bleibt a) zu zeigen.

Sei $\zeta \in PE_n$. Wegen $\Phi_n(\zeta) = 0$ gilt $p_\zeta \mid \Phi_n$. Da $\deg \Phi_n = |PE_n| = |\{\zeta^k \mid \operatorname{ggT}(k,n) = 1\}|$ genügt es zu zeigen $p_\zeta(\zeta^k) = 0$ für alle k mit $\operatorname{ggT}(k,n) = 1$. Wir betrachten zunächst den Fall, dass $k = p$ für eine zu n teilerfremde Primzahl p ist.

Sei $g \in \mathbb{Q}[X]$ mit $p_\zeta \cdot g = X^n - 1 =: h$. Nach Gauß gilt $g, p_\zeta \in \mathbb{Z}[X]$. Angenommen $p_\zeta(\zeta^p) \neq 0$. Dann folgt $g(\zeta^p) = 0$ und ζ ist eine Nullstelle von $g(X^p)$. Wieder mit Gauß folgt $p_\zeta \mid g(X^p)$ in $\mathbb{Z}[X]$. Wir werden nun folgende Beobachtung benutzen: In $\mathbb{F}_p$ gilt

$$(a+b)^p = a^p + b^p,$$

da alle anderen Binomialkoeffzienten Vielfache von p sind. Daher gilt $f(X^p) = f(X)^p$ für $f \in \mathbb{F}_p[X]$. Sei

$$\mathbb{Z}[X] \to {}^{\mathbb{Z}}/_{p\mathbb{Z}}[X] \;\;,\;\; f \mapsto \overline{f}$$

der von $\mathbb{Z} \to {}^{\mathbb{Z}}/_{p\mathbb{Z}}$ induzierte Ringhomomorphismus. Wegen $p_\zeta \mid g(X^p)$ folgt $\overline{p}_\zeta \mid \overline{g}^p$. Folglich besitzen $\overline{p}_\zeta$ und $\overline{g}$ eine gemeinsame Nullstelle. Aber wegen $\overline{h}' = n \cdot X^{n-1}$ hat $\overline{h} = \overline{p}_\zeta \cdot \overline{g}$ keine doppelte Nullstelle. $\lightning$

Also $p_\zeta(\zeta^p) = 0$.

Sei nun k mit $\operatorname{ggT}(n,k) = 1$ beliebig. Dann ist $k = p_1 \cdot \ldots \cdot p_r$ wobei $p_1, \ldots, p_r$ Primzahlen sind, die n nicht teilen. Wegen $p_\zeta(\zeta^{p_1}) = 0$ ist p_ζ auch das Minimalpolynom von ζ^{p_1} und es folgt

$$p_\zeta(\zeta^{p_1 \cdot p_2}) = p_{\zeta^{p_1}}\Big((\zeta^{p_1})^{p_2}\Big) = 0$$

Induktiv folgt $p_\zeta(\zeta^k) = 0$. $\square$

20 n-Teilung des Kreises

20.1 Satz (Charakterisierung von Konstruierbarkeit)

Sei $\alpha \in \mathbb{C}$ algebraisch über $\mathbb{Q}$. Sei L der Zerfällungskörper von $p_\alpha \in \mathbb{Q}[X]$. Dann sind äquivalent

1) $\alpha \in \mathcal{A}(\{0,1\})$
2) $[L:\mathbb{Q}]$ ist eine Potenz von 2.

Beweis

2) $\Rightarrow$ 1): Als Zerfällungskörper ist ${}^{L}/{}_{\mathbb{Q}}$ normal. Wegen $\operatorname{char}\mathbb{Q} = 0$ ist ${}^{L}/{}_{\mathbb{Q}}$ auch separabel und damit galoissch. In Kapitel 18 haben wir gesehen, dass es dann eine Folge von Zwischenkörpern $\mathbb{Q} = K_0 \subseteq K \subseteq K_1 \subseteq \ldots \subseteq K_n = L$ gibt mit $[K_i : \mathbb{Q}] = 2^i$. Insbesondere $[K_i : K_{i-1}] = 2$ und ${}^{K_i}/{}_{K_{i-1}}$ eine quadratische Erweiterung. Damit folgt $\alpha \in \mathcal{A}(\{0,1\})$ nach 10.11.

1) $\Rightarrow$ 2: Sei $\alpha \in \mathcal{A}(\{0,1\})$. Nach 10.11 existiert eine Folge $\mathbb{Q} = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_k$ mit $\alpha \in K_k$, $K_i = K_i(\omega_i)$ mit $\omega_i^2 \in K_{i-1}$. Sei p_i das Minimalpolynom von ω_i über $\mathbb{Q}$. Sei $f_i = p_1 \cdot \ldots \cdot p_i$ und Z_i der Zerfällungskörper von f_i. Dann $K_i \subseteq Z_i$ und $\mathbb{Q} \subseteq Z_1 \subseteq \ldots \subseteq Z_k$.
<u>Behauptung:</u> $[Z_i : Z_{i-1}]$ ist eine Potenz von 2. Dann ist auch $[Z_k : \mathbb{Q}]$ eine Potenz von 2. Da ${}^{Z_k}/{}_{\mathbb{Q}}$ normal ist und $\alpha \in K_k \subseteq Z_k$ enthält Z_k den Zerfällungskörper L von p_α. Damit ist auch $[L:\mathbb{Q}]$ eine Potenz von 2 (da $[L:\mathbb{Q}] \mid [Z_k:\mathbb{Q}]$). Es bleibt die Behauptung zu beweisen.

Seien $\omega_i = \alpha_1, \ldots, \alpha_s$ die Nullstellen von p_i. Nach dem Fortsetzungssatz für normale Körpererweiterungen (14.16) gibt es $\sigma_j \in \operatorname{Gal}({}^{Z_i}/{}_{\mathbb{Q}})$ mit $\sigma_j(\alpha_1) = \alpha_j$. Da ${}^{Z_{i-1}}/{}_{\mathbb{Q}}$ normal ist, gilt $\sigma_j(Z_{i-1}) = Z_{i-1}$ nach 15.4. Es ist $\alpha_1^2 = \omega_i^2 \in K_{i-1} \subseteq Z_{i-1}$. Daher $\alpha_j^2 = \sigma_j(\alpha_1^2) \in \sigma_j(Z_{i-1}) = Z_{i-1}$. Damit auch

$$Z_{i-1} \subseteq Z_{i-1}(\alpha_1) \subseteq Z_{i-2}(\alpha_1,\alpha_2) \subseteq \ldots \subseteq Z_{i-1}(\alpha_1,\ldots,\alpha_s) = Z_i$$

eine Folge von quadratischen Körpererweiterungen. Daher ist $[Z_i : Z_{i-1}]$ eine Potenz von 2. □

20.2 Satz (Gauß)

Das regelmäßige n-Eck ist genau dann mit Zirkel und Lineal konstruierbar, wenn $n = 2^e \cdot p_1 \cdot \ldots \cdot p_r$ mit beliebigem e und paarweise verschiedenen Primzahlen $p_1, \ldots, p_r$ der Form $p_i = 1 + 2^{k_i}$.

Beweis
Sei $\zeta := e^{2\pi i/n}$. Es ist $\mathbb{Q}_n := \mathbb{Q}(\zeta)$ der Zerfällungskörper von p_ζ und es gilt nach Kapitel 19 $[\mathbb{Q}_n : \mathbb{Q}] = \varphi(n)$. Ist $n = 2^e \cdot p_1^{e_1} \cdot \ldots \cdot p_r^{e_r}$ die Primfaktorzerlegung von n, so gilt

$$\varphi(n) = 2^{e-1} \cdot p_1^{e_1-1} \cdot (p_1 - 1) \cdot \ldots \cdot p_r^{e_r-1} \cdot (p_r - 1)$$

Es ist also $\varphi(n)$ genau dann eine Potenz von 2, wenn $e_1 = \ldots = e_r = 1$ und $(p_i - 1)$ für $i = 1, \ldots, r$ eine Potenz von 2 ist, also $p_i = 2^{k_i} + 1$. Mit dem vorigen Satz (20.1) folgt die Behauptung. □

20.3 Lemma

Sei $m \in \mathbb{N}$ und $1 + 2^m$ eine Primzahl. Dann ist m eine Potenz von 2.

Beweis
Ist m keine Potenz von 2, so können wir $m = k \cdot p$ mit $p > 2$ ungerade schreiben. Dann ist[3]

$$(1 + 2^m) = 1 - (-2^k)^p = (1 + 2^k)\Big(1 + (-2)^k + (-2)^{2\cdot k} + \ldots + (-2)^{(p-1)\cdot k}\Big) \qquad \square$$

[3] besser bei `http://de.wikipedia.org/wiki/Fermat-Zahl`

20.4 Bemerkung

$F_k = 1 + 2^{(2^k)}$ heißt die k-te **Fermatsche Zahl**. Es sind $F_0 = 3, F_1 = 5, F_2 = 17, F_3 = 257, F_4 = 65537$ Primzahlen. F_5 ist keine Primzahl mehr. Es ist nicht bekannt, ob es weitere Fermatsche Primzahlen gibt.

21 Auflösen von algebraischen Gleichungen über $\mathbb{Q}$, II.

In Kapitel 21 seien alle Körper Unterkörper von $\mathbb{C}$.

21.1 Definition

Eine endliche Körpererweiterung L/K heißt **auflösbar**, wenn es eine endliche Körpererweiterung E/L gibt, so dass E/K galoissch ist mit auflösbarer[4] Galois-Gruppe $\mathrm{Gal}(E/K)$.

21.2 Bemerkung

G auflösbar, $H \leq G$, so ist auch H auflösbar. Ist $N \trianglelefteq G$, so gilt: G auflösbar $\iff$ $N, G/N$ auflösbar.

21.3 Wiederholung

- L/K heißt Radikalerweiterung $:\Leftrightarrow \alpha \in L : L = K(\alpha), \alpha^d \in K, d \in \mathbb{N}$
- L/K heißt durch Radikale auflösbar, wenn es eine Kette von Körpern gibt mit $K = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_r$ mit $L \subseteq K_r$ und K_i/K_{i-1} für $i = 1, \ldots, r$ eine Radikalerweiterung ist.

21.4 Bemerkung

Ist L/K galoissch und E/L endlich mit E/K galoissch und $\mathrm{Gal}(E/K)$ auflösbar, so ist $\mathrm{Gal}(L/K)$ auflösbar, da nach dem Hauptsatz der Galoistheorie (17.8) gilt

$$\mathrm{Gal}(L/K) \cong \mathrm{Gal}(E/K)/\mathrm{Gal}(E/L)$$

Also gilt für L/K endlich galoissch: L/K auflösbar $\iff$ $\mathrm{Gal}(L/K)$ auflösbar

21.5 Satz

Sei L/K eine endliche Körpererweiterung. Dann sind äquivalent

(1) L/K ist durch Radikale auflösbar

(2) L/K ist auflösbar.

21.6 Korollar

Sei L/K eine endliche Galoiserweiterung. Dann gilt

$$L/K \text{ ist durch Radikale auflösbar} \iff \mathrm{Gal}(L/K) \text{ ist auflösbar}$$

Beweis

Folgt aus 21.4 und 21.5. □

[4] G heißt auflösbar, wenn es eine Folge von Normalteilern $\{e\} = N_0 \trianglelefteq N_1 \trianglelefteq \ldots \trianglelefteq N_k = G$ gibt, so dass für $i = 1, \ldots, k$ N_i/N_{i-1} abelsch ist; siehe auch 12.11

21.7 Lemma 1

Seien L, K, F Unterkörper von $\mathbb{C}$ mit $K \subseteq L$, $K \subseteq F$, L/K endlich. Sei $E := F(L)$. Dann gilt

$$\begin{tikzcd} L \arrow[r, hook] & F(L) \\ K \arrow[u, hook] \arrow[r, hook] & F \arrow[u, hook] \end{tikzcd}$$

a) Ist L/K durch Radikale auflösbar, so ist auch E/F durch Radikale auflösbar.

b) Ist L/K auflösbar, so ist auch E/F auflösbar.

Beweis

a) Sei L/K durch Radikale auflösbar. Dann existiert $K = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_r$ mit $L \subseteq K_r$ und $\exists \alpha_i \in K_i, d_i \in \mathbb{N}$ mit $K_i = K_{i-1}(\alpha_i)$ und $\alpha_i^{d_i} \in K_{i-1}$. Es folgt $K_r = K(\alpha_1, \ldots, \alpha_r)$ und

$$E = F(L) \subseteq F(K_r) = F\big(K(\alpha_1, \ldots, \alpha_r)\big) = F(\alpha_1, \ldots, \alpha_r)$$

Setze nun $F_i := F(\alpha_1, \ldots, \alpha_i)$. Dann $F = F_0 \subseteq F_1 \subseteq \ldots \subseteq F_r$ mit $E \subseteq F_r$, $F_i = F_{i-1}(\alpha_i)$ mit $\alpha_i^{d_i} \in K_{i-1} \subseteq F_{i-1}$. Daher ist auch E/F durch Radikale auflösbar.

b) Sei L/K auflösbar. Wir können o.B.d.A. annehmen, dass L/K galoissch ist mit $\mathrm{Gal}(L/K)$ auflösbar. Insbesondere ist L der Zerfällungskörper eines Polynoms $p \in K[X]$ (siehe 15.4). Dann ist $E = F(L)$ der Zerfällungskörper von p über F. Insbesondere ist E/F normal, endlich und damit galoissch. Es bleibt zu zeigen: $\mathrm{Gal}(E/F)$ ist auflösbar.

Da L/K normal ist, erhalten wir durch Einschränkung auf L einen Gruppenhomomorphismus $\mathrm{Aut}(E/K) \to \mathrm{Aut}(L/K) = \mathrm{Gal}(L/K)$. Da $\mathrm{Gal}(E/F) \leq \mathrm{Aut}(E/K)$ erhalten wir einen Gruppenhomomorphismus

$$\psi : \mathrm{Gal}(E/F) \to \mathrm{Gal}(L/K), \quad \sigma \mapsto \sigma\big|_L$$

Ist $\sigma|_L = \mathrm{id}$ so folgt $\sigma = \mathrm{id}$, da σ ein F-Homomorphismus ist und $E = F(L)$. Damit ist ψ injektiv und

$$\mathrm{Gal}(E/F) \cong \mathrm{Bild}\,\psi \leq \mathrm{Gal}(L/K).$$

Damit ist $\mathrm{Gal}(E/F)$ isomorph zu einer Untergruppe einer auflösbaren Gruppe also auflösbar. □

21.8 Lemma 2

Seien $K \subseteq L \subseteq M$ Unterkörper von $\mathbb{C}$. Sei M/K endlich. Dann gilt

a) M/K durch Radikale auflösbar $\iff$ L/K und M/L durch Radikale auflösbar.

b) M/K auflösbar $\iff$ L/K und M/L auflösbar.

Beweis

a) "$\Longrightarrow$" folgt direkt aus der Definition.

"$\Longleftarrow$" Ist L/K durch Radikale auflösbar, so gibt es eine Folge $K = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_r$ von Radikalerweiterungen mit $L \subseteq K_r$. Mit M/L ist nach Lemma 1 (21.7) auch $M(K_r)/K_r$ durch Radikale auflösbar. Es gibt also eine Folge $K_r \subseteq K_{r+1} \subseteq \ldots \subseteq K_R$ von Radikalerweiterungen mit $M \subseteq M(K_r) \subseteq K_R$. Insgesamt beweist die Folge

$$K = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_r \subseteq K_{r+1} \subseteq \ldots \subseteq K_R,$$

dass M/K durch Radikale auflösbar ist.

b) "$\Longrightarrow$" Sei M/K auflösbar. Wir können o.B.d.A annehmen, dass M/K eine endliche Galoiserweiterung mit auflösbarer Galois-Gruppe $\mathrm{Gal}(M/K)$ ist (Sonst vergrößern wir M). Dann ist auch L/K auflösbar. Mit M/K ist auch M/L eine endliche Galois-Erweiterung. Weiter ist $\mathrm{Gal}(M/L)$ als Untergruppe der auflösbaren Gruppe $\mathrm{Gal}(M/K)$ auflösbar.

$$\begin{tikzcd} M \arrow[r, hook] & M' \\ & L' \arrow[u, hook] \\ K \arrow[uu, hook] \arrow[r, "="] & K \arrow[u, hook] \end{tikzcd}$$

"$\Longleftarrow$" Ist ${}^{L}\!/\!_{K}$ auflösbar, so gibt es ${}^{L'}\!/\!_{L}$ endlich mit ${}^{L'}\!/\!_{K}$ galoissch und $\mathrm{Gal}({}^{L'}\!/\!_{K})$ auflösbar. Mit ${}^{M}\!/\!_{L}$ ist nach Lemma 1 (21.7) auch ${}^{L'(M)}\!/\!_{L'}$ auflösbar. Es gibt also ${}^{M'}\!/\!_{L'(M)}$ endlich mit ${}^{M'}\!/\!_{L'}$ galoissch mit auflösbarer Galois-Gruppe $\mathrm{Gal}({}^{M'}\!/\!_{L'})$. Angenommen ${}^{M'}\!/\!_{K}$ ist galoissch. Dann $\mathrm{Gal}({}^{M'}\!/\!_{L'}) \trianglelefteq \mathrm{Gal}({}^{M'}\!/\!_{K})$ und

$$\mathrm{Gal}({}^{M'}\!/\!_{K}) / \mathrm{Gal}({}^{M'}\!/\!_{L'}) \trianglelefteq \mathrm{Gal}({}^{L'}\!/\!_{K}).$$

Da ${}^{M'}\!/\!_{K}$ endlich und separabel ist, gibt es $\alpha_1 \in M'$ mit $M' = K(\alpha_1)$ (Satz vom primitiven Element, 16.15). Sei Z der Zerfällungskörper von $p_{\alpha_1} \in K[X]$. Also $p_{\alpha_1} = (X-\alpha_1)\cdot\ldots\cdot(X-\alpha_r)$ und $Z = K(\alpha_1,\ldots,\alpha_r)$. Es ist $M' \subseteq Z$ und ${}^{Z}\!/\!_{K}$ ist eine endliche Galois-Erweiterung. Es ist L' ein Zwischenkörper von ${}^{Z}\!/\!_{K}$. Da ${}^{L'}\!/\!_{K}$ normal ist, ist nach dem Hauptsatz der Galoistheorie (17.8) die Restriktionsabbildung $\mathrm{Gal}({}^{Z}\!/\!_{K}) \twoheadrightarrow \mathrm{Gal}({}^{L'}\!/\!_{K})$ surjektiv mit Kern $\mathrm{Gal}({}^{Z}\!/\!_{L'})$. Es ist $\mathrm{Gal}({}^{L'}\!/\!_{K})$ auflösbar.

Bleibt zu zeigen: $\mathrm{Gal}({}^{Z}\!/\!_{L'})$ ist auflösbar. Nach Fortsetzungssatz gibt es $\sigma_j \in \mathrm{Gal}({}^{Z}\!/\!_{K})$ mit $\sigma_j(\alpha_1) = \alpha_j$. Sei $\sigma_j(M') =: M'_j$. Da ${}^{L'}\!/\!_{K}$ normal ist, ist $\sigma_j(L') = L'$. ${}^{M'}\!/\!_{L'}$ normal impliziert ${}^{M'_j}\!/\!_{L'}$ normal. Aus $\mathrm{Gal}({}^{M'}\!/\!_{L'})$ auflösbar folgt $\mathrm{Gal}({}^{M'_j}\!/\!_{L'})$ auflösbar. Für jedes j erhalten wir Restriktionsabbildungen

$$\psi_j : \mathrm{Gal}({}^{Z}\!/\!_{L'}) \to \mathrm{Gal}({}^{M'_j}\!/\!_{L'})$$

Sei $\psi : \mathrm{Gal}({}^{Z}\!/\!_{L'}) \to \mathrm{Gal}({}^{M'_1}\!/\!_{L'}) \times \ldots \times \mathrm{Gal}({}^{M'_r}\!/\!_{L'})$ das Produkt der ψ_j. Da $\alpha_i \in M'_i$ und $Z = K(\alpha_1,\ldots,\alpha_r)$ ist ψ injektiv. Damit ist $\mathrm{Gal}({}^{Z}\!/\!_{L'})$ auflösbar. □

21.9 Beweis von 21.5

(1) $\Rightarrow$ (2): Sei ${}^{L}\!/\!_{K}$ durch Radikale auflösbar. Dann gibt es $K = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_n$ und $\alpha_1 \in K_i$, $d_i \in \mathbb{N}$ mit $K_i = K_{i-1}(\alpha_i)$, $\alpha_i^{d_i} \in K_{i-1}$ und $L \subseteq K_n$. Sei $N := d_1 \cdot \ldots \cdot d_n$. Sei $\zeta \in PE_n(\mathbb{C})$. Betrachte

$$K = K_0 \subseteq K_1(\zeta) \subseteq \ldots \subseteq K_n(\zeta)$$

Es ist ${}^{\mathbb{Q}_N}\!/\!_{\mathbb{Q}}$ auflösbar, da $\mathrm{Gal}({}^{\mathbb{Q}_N}\!/\!_{\mathbb{Q}}) \cong ({}^{\mathbb{Z}}\!/\!_{n\mathbb{Z}})^\times$ abelsch ist. Mit Lemma 1 (21.7) folgt, dass ${}^{K_0(\zeta)}\!/\!_{K}$ auflösbar ist. Wegen Lemma 3 (21.10) sind ${}^{K_1(\zeta)}\!/\!_{K_0(\zeta)}, \ldots, {}^{K_n(\zeta)}\!/\!_{k_{n-1}(\zeta)}$ auflösbar. Mit Lemma 2 b) und einer Induktion folgt, dass ${}^{K_n(\zeta)}\!/\!_{K}$ auflösbar ist. Damit ist auch ${}^{L}\!/\!_{K}$ auflösbar, denn $L \subseteq K_n \subseteq K_n(\zeta)$. □

(2) $\Rightarrow$ (1): Siehe Bosch "Algebra" S. 265

21.10 Lemma 3

Sei $L = K(\alpha)$ mit $\alpha^n \in K, \alpha \neq 0$. Weiter gelte $E_n(\mathbb{C}) \subseteq L$. Dann ist ${}^{L}\!/\!_{K}$ auflösbar.

Beweis
Die Nullstellen von $X^n - \alpha^n \in K[X]$ sind genau die $\zeta \cdot \alpha$ mit $\zeta \in E_n(\mathbb{C})$. Da $E_n(\mathbb{C}) \subseteq K \subseteq K(\alpha)$ ist $K(\alpha)$ der Zerfällungskörper von $X^n - \alpha^n$ und damit endlich und galoissch. Die Galois-Gruppe $\mathrm{Gal}({}^{L}\!/\!_{K})$ wirkt auf den Nullstellen von $X^n - \alpha^n$. Zu $\sigma \in \mathrm{Gal}({}^{L}\!/\!_{K})$ gibt es also $\zeta_\sigma \in E_n(\mathbb{C})$ mit $\sigma(\alpha) = \zeta_\sigma \cdot \alpha$.

Behauptung: $\psi : \mathrm{Gal}({}^{L}\!/\!_{K}) \to E_n\mathbb{C}, \sigma \mapsto \zeta_\sigma$ ist ein Gruppenhomomorphismus.
$\sigma\tau(\alpha) = \sigma(\zeta_\tau \cdot \alpha) = \zeta_\tau \cdot \sigma(\alpha) = \zeta_\tau \cdot \zeta_\sigma \cdot \alpha$. Also $\zeta_{\sigma\tau} = \zeta_\sigma \cdot \zeta_\tau$. Wegen $L = K(\alpha)$ ist ψ injektiv. Da $E_n(\mathbb{C})$ abelsch ist, ist auch $\mathrm{Gal}({}^{L}\!/\!_{K})$ abelsch und damit auflösbar. □

22 Eine nicht-auflösbare Gleichung

22.1 Definition

Der Kern der **Signum-Abbildung** $\operatorname{sgn} : S_n \to \{\pm 1\}$ heißt die **n-te alternierende Gruppe** A_n.

22.2 Definition

Sei G eine Gruppe. Die kleinste Untergruppe von G, die alle Elemente der Form $ghg^{-1}h^{-1} =: [g, h]$, $g, h \in G$ enthält, heißt die **Kommutatoruntergruppe** von G und wird mit $[G, G]$ bezeichnet.

22.3 Lemma

Sei $\varphi : G \to A$ ein Gruppenhomomorphismus mit A abelsch. Dann $[G, G] \subseteq \ker \varphi$.

Beweis

$$\varphi([g,h]) = \varphi(ghg^{-1}h^{-1}) = \varphi(g) \cdot \varphi(h) \cdot \varphi(g)^{-1} \cdot \varphi(h)^{-1} = \varphi(g) \cdot \varphi(g)^{-1} \cdot \varphi(h) \cdot \varphi(h)^{-1} = e \qquad \square$$

22.4 Satz

Für $n \geq 5$ ist $[A_n, A_n] = A_n$. $S_n/A_n \cong \{\pm 1\}$

Beweis
S_n wird von den **Transpositionen** $(x\,y)$, $x \neq y \in \{1, \dots, n\}$ erzeugt, d.h. jedes Element in S_n ist ein Produkt von Transpositionen. $\sigma \in A_n$ gilt genau dann, wenn σ ein Produkt einer geraden Anzahl von Transpositionen ist. Es genügt also zu zeigen

$$\forall x \neq y, y' \neq z \text{ ist } (x\,y)(y'\,z) \in [A_n, A_n]$$

O.B.d.A. Sei $x \neq z$. Ist $y = y'$, so gibt es $a \neq b \in \{1, \dots, n\} \setminus \{x, y, z\}$, da $n \geq 5$. Dann gilt

$$\begin{aligned}(x\,y)(y\,z) &= [(x\,y)(y\,a), (x\,z)(z\,b)] \in [A_n, A_n] \\ &= (x\,y)(y\,a)(x\,z)(z\,b)(y\,a)(x\,y)(z\,b)(x\,z)\end{aligned}$$

Ist $y \neq y'$, so

$$(x\,y)(y'\,z) = \underbrace{(x\,y)(y\,y')}_{\in [A_n, A_n]} \underbrace{(y\,y')(y'\,z)}_{\in [A_n, A_n]} \in [A_n, A_n] \qquad \square$$

22.5 Korollar

A_n ist für $n \geq 5$ nicht auflösbar.

Beweis
Angenommen doch: $\{e\} = N_0 \trianglelefteq N_1 \trianglelefteq N_2 \trianglelefteq \dots \trianglelefteq N_k = A_n$ mit N_i/N_{i-1} abelsch. Insbesondere ist A_n/N_{k-1} abelsch und wir haben einen surjektiven Gruppenhomomorphismus $\pi : A_n \twoheadrightarrow A_n/N_{k-1}$. Mit Lemma 22.3 folgt $\trianglelefteq$ *durchstreichen*

$$[A_n, A_n] \subseteq \operatorname{Kern} \pi \Longrightarrow A_n \subseteq \operatorname{Kern} \pi \text{ und } \pi \text{ trivial } ↯$$

22.6 Korollar

Für $n \geq 5$ ist S_n nicht auflösbar.

22.7 Satz

Die Galois-Gruppe von $X^5 - 4X + 2 \in \mathbb{Q}[X]$ ist S_5.

Beweis

$z, \overline{z} \notin \mathbb{R}$, $t_0, t_1, t_2 \in \mathbb{R}$

Sei L der Zerfällungskörper von p. Seien $T = \{t_0, t_1, t_2, z, \overline{z}\}$ die Nullstellen von p. Sei $G := \mathrm{Gal}(L/\mathbb{Q})$. Da $L = \mathbb{Q}(T)$ und G auf T wirkt, können wir G als Untergruppe von $S_T (\cong S_5)$ auffassen. Nach Eisenstein ist p irreduzibel (teste die Primzahl 2). Mit dem Fortsetzungssatz (14.9) folgt: Zu $\alpha, \beta \in T$ gibt es $\sigma \in G$ mit $\sigma(\alpha) = \beta$. Es gibt also nur eine Bahn (siehe 3.5) für die Wirkung von G auf T. Es folgt mit der Bahnengleichung (3.10)

$$\frac{|G|}{|G_{t_0}|} = |Gt_0| = |T| = 5$$

Es folgt $5 \mid |G|$. Damit hat G eine nichttriviale 5-Sylowgruppe. Da $G \leq S_T$ gilt $|G| \mid |S_T| = |S_5| = 120$. Daher hat die 5-Sylowgruppe Ordnung 5. Damit hat jedes nichttriviales Element in ihr Ordnung 5. Insbesondere enthält G ein Element σ von Ordnung 5. Weiter ist die komplexe Konjugation ein Element der Ordnung 2.

22.8 Korollar

Der Zerfällungskörper von $X^5 - 4X + 2 \in \mathbb{Q}[X]$ ist nicht durch Radikale auflösbar.

22.9 Lemma

$p = X^5 - 4X + 2$ hat genau 3 reelle Nullstellen und 2 weitere Nullstellen, z und $\overline{z}$ in $\mathbb{C} \setminus \mathbb{R}$.

Beweis

Betrachte p als differenzierbare Abbildung $\mathbb{R} \to \mathbb{R}$. Es gilt $\lim_{t\to\infty} p(t) = \infty$ und $\lim_{t\to-\infty} = -\infty$. Es ist $p' = 5X^4 - 4 = 5(X^2 - \frac{2}{\sqrt{5}})(X^2 + \frac{2}{\sqrt{5}})$. Also hat p' genau zwei reelle Nullstellen $\pm\frac{\sqrt{2}}{\sqrt[4]{5}}$.

$$p\Big(\frac{\sqrt{2}}{\sqrt[4]{5}}\Big) < 0 \qquad p\Big(-\frac{\sqrt{2}}{\sqrt[4]{5}}\Big) > 0$$

Daher hat p genau 3 reelle Nullstellen. Da $p' \neq 0$ in diesen 3 Nullstellen sind die reellen Nullstellen alle einfache Nullstellen. Da $\deg p = 5$ gibt es noch mindestens eine weitere Nullstelle $z \in \mathbb{C} \setminus \mathbb{R}$. Dann ist auch $\overline{z} \neq z$ eine Nullstelle: $p(\overline{z}) = \overline{p(z)} = 0$. □

22.10 Lemma

Seien $\tau, \sigma \in S_5$ mit $\mathrm{ord}(\sigma) = 5$ und τ eine Transposition. Dann erzeugen σ und τ die Gruppe S_5, d.h. S_5 ist die einzige Untergruppe von S_5, die σ und τ enthält.

Beweis

o.B.d.A. sei $\tau = (1\,2)$. Da $\mathrm{ord}(\sigma) = 5$ gibt es keine echte nicht leere Teilmenge von T von $\{1, \dots, 5\}$ mit $\sigma(T) = T$. Es folgt

$$\{1, \dots, 5\} = \big\{1, \sigma(1), \sigma^2(1), \sigma^3(1), \sigma^4(1)\big\}.$$

Indem wir σ durch eine geeignete Potenz von σ ersetzen dürfen wir annehmen $\sigma(1) = 2$. Nach Umordnung von $3, 4, 5$ können wir annehmen

$$\sigma(i) = \begin{cases} i+1, & \text{falls } i \neq 5 \\ 1, & \text{falls } i = 5 \end{cases}$$

Nun ist $(2\,3) = \sigma(1\,2)\sigma^{-1}$, $(3\,4) = \sigma(2\,3)\sigma^{-1}$, $(4\,5) = \sigma(3\,4)\sigma^{-1}$. Also liegen $(1\,2), (2\,3), (3\,4), (4\,5)$ in der von σ und τ erzeugten Untergruppe von S_5. Durch diese Transpositionen wird aber schon die ganze S_5 erzeugt: Da sich jede endliche Folge von Zahlen durch sukzessive Vertauschungen von benachbarten Zahlen ordnen lässt. $\square$

Index

Die Seitenzahlen *sind mit Hyperlinks zu den entsprechenden Seiten versehen, also anklickbar* ☝

Abbildungsverzeichnis