Einführung in die Algebra

Wintersemester 2017/18

Alexander Esgen Lukas Kempf Luise Puhlmann

27. Juni 2018

Inhaltsverzeichnis

I Gruppen **3**
1 Grundlegendes . . . 3
2 Satz von Lagrange und Normalteiler . . . 8
3 Zyklische Gruppen . . . 13
4 Auflösbare Gruppen . . . 15
5 Gruppenoperationen . . . 18
6 p-Gruppen und Sylow-Sätze . . . 21

II Ringe **25**
7 Allgemeines . . . 25
8 Faktorielle Ringe . . . 40
9 Maximale Ideale: Existenz . . . 44
10 Einschub: Chinesischer Restsatz . . . 45
11 Lokalisierung . . . 46
12 Satz von Gauß . . . 48
13 Kreisteilungspolynome . . . 51

III Körpertheorie **54**
14 Körpererweiterungen . . . 54
15 Algebraische Körpererweiterung . . . 57
16 Algebraischer Abschluss . . . 62
17 Endliche Körper . . . 69
18 Zerfällungskörper . . . 73

IV Galoistheorie **77**
19 Normale und separable Körpererweiterungen . . . 77
20 Galoisgruppen . . . 86
21 Galoiserweiterungen . . . 87

22 Galoiskorrespondenz 89
23 Fundamentalsatz der Algebra 91
24 Zyklotomische Körper 91
25 Inverses Galoisproblem 96
26 Auflösbarkeit von algebraischen Gleichungen 98

Dies ist eine Mitschrift der Vorlesung „Einführung in die Algebra“von Prof. Dr. Catharina Stroppel an der Universität Bonn, gehalten im Wintersemester 2017/18.

[9. Oktober 2017]

Organisatorisches

- Website der Vorlesung: http://www.math.uni-bonn.de/people/palmer/A1.html
- Assistent: Dr. Martin Palmer
- Abgabe der Übungsblätter: Donnerstag vor der Vorlesung
- Beginn der Übungsgruppen: Zweite Vorlesungswoche
- Literatur: siehe Homepage

I. Gruppen

1. Grundlegendes

Definition 1.1. Eine Gruppe ist eine Menge G zusammen mit einer Abbildung

$$\begin{aligned} \circ\colon G \times G &\longrightarrow G \\ (g,h) &\longmapsto g \circ h \end{aligned}$$

(genannt Gruppenoperation), sodass gilt:

(G1) $(a \circ b) \circ c = a \circ (b \circ c)$ $\forall a,b,c \in G$ (Assoziativität)

(G2) $\exists e \in G$ mit $g \circ e = g = e \circ g$ $\forall g \in G$ (Neutrales Element)

(G3) $\forall g \in G$ $\exists g^{-1}$ sodass $g \circ g^{-1} = e = g^{-1} \circ g$ (Inverse Elemente)

Bemerkung.

- Das neutrale Element e ist eindeutig.
- Inverse Elemente g^{-1} sind eindeutig.
- Es reicht sogar, die Existenz von Linksneutralem und Linksinversem oder Existenz von Rechtsneutralem und Rechtsinversem zu fordern.
- Es gelten die Kürzungsregeln:

$$\begin{aligned} a \circ c = b \circ c &\quad\Leftrightarrow\quad a = b \qquad \forall a,b,c \in G \\ c \circ a = c \circ b &\quad\Leftrightarrow\quad a = b \qquad \forall a,b,c \in G \end{aligned}$$

Definition 1.2. $(G, \circ)$ heißt abelsch, falls $g \circ h = h \circ g$ für alle $g, h \in G$ gilt.

Beispiel 1. Einige Beispiele für Gruppen:

- $(\mathbb{Z}, +)$
- Für einen Körper $(K, +, \cdot)$ sind $(K, +)$ und $(K^* = K \setminus \{0\}, \cdot)$ Gruppen.
- Ist $(V, +, \cdot)$ ein K-Vektorraum, so ist $(V, +)$ eine Gruppe.
- Für einen Körper K und $n \in \mathbb{N}$ ist $\mathrm{GL}_n(K)$ eine Gruppe mit der Matrixmultiplikation als Verknüpfung.
- Sei M eine nichtleere Menge sowie $S_M \coloneqq \{f \colon M \to M \mid f \text{ invertierbar}\}$. Dann ist $(S_M, \circ)$ eine Gruppe, wobei $\circ$ die Komposition von Abbildungen ist. Der Spezialfall $M = \{1, \dots n\},\ n \in \mathbb{N}$ ergibt die symmetrische Gruppe S_n der Ordnung $n!$.
- Sei $(G, \circ)$ eine Gruppe und $a \in G$ fest gewählt. Dann ist $(G, \circ_a)$ eine Gruppe, wobei $g \circ_a h = g \circ a \circ h$.

Definition 1.3. Sei $(G, \circ)$ eine Gruppe. Dann ist die Anzahl $|G|$ der Elemente von G die Ordnung von G.

Definition 1.4. Sei $(G, \circ)$ eine Gruppe. Eine Teilmenge $H \subseteq G$ heißt Untergruppe, falls $H \neq \emptyset$ und aus $h_1, h_2 \in H$ bereits $h_1 \circ h_2^{-1} \in H$ folgt. Wir schreiben dann $H < (G, \circ)$ oder $H < G$.

Bemerkung. $H < (G, \circ)$ gilt genau dann, wenn gilt:

(UG0) $e \in H$

(UG1) $h_1, h_2 \in H \Rightarrow h_1 \circ h_2 \in H$

(UG2) $h \in H \Rightarrow h^{-1} \in H$

Offensichtlich sind Untergruppen wieder Gruppen.

Beispiel 2.

- $2\mathbb{Z} < (\mathbb{Z}, +)$
- $n \in \mathbb{N}$; $\mathrm{O}(n) = \{A \in \mathrm{GL}_n(\mathbb{R}) | AA^T = \mathbb{1}_n\} < \mathrm{GL}_n(\mathbb{R})$ die orthogonale Gruppe
- $n \in \mathbb{N}$; $\mathrm{U}(n) = \{A \in GL_n(\mathbb{C}) | A\overline{A}^T = \mathbb{1}_n\} < \mathrm{GL}_n(\mathbb{C})$ die unitäre Gruppe
- $\mathrm{SL}_n(K) = \{A \in \mathrm{GL}_n(K) | \det(A) = 1\} < \mathrm{GL}_n(K)$
- $\mathrm{SO}(n) = \mathrm{O}(n) \cap \mathrm{SL}_n(\mathbb{R}) < \mathrm{O}(n)$
- Spezielle unitäre Gruppe

- $\mathrm{H}(3,\mathbb{R}) = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \right\}$: Obere Dreiecksmatrizen, nur Einsen auf der Diagonalen (Heisenberggruppe)

Definition 1.5. Sei $(G, \circ)$ eine Gruppe. Sei $\emptyset \neq N \subseteq G$. Dann ist $\langle N \rangle$ die (bezüglich Inklusion) kleinste Untergruppe von G, die N enthält (aus $H < G$ mit $N \subseteq H$ folgt also $\langle N \rangle \subseteq H$). Wir nennen $\langle N \rangle$ die von N erzeugte Untergruppe von $(G, \circ)$.

Bemerkung. $\langle N \rangle$ ist wohldefiniert, denn seien $H_1, H_2 < G$ mit $N \subseteq H_1, N \subseteq H_2$, dann liegt N in $H_1 \cap H_2$ und es gilt $H_1 \cap H_2 < G$. Also eine existiert kleinste Untergruppe, die N enthält; $\langle N \rangle$ ist wohldefiniert.

Definition 1.6. Sei G eine Gruppe und $N \subseteq G$.

1. N erzeugt die Gruppe G, falls $\langle N \rangle = G$. In diesem Fall heißt N Erzeugendensystem der Gruppe G.

2. $(G, \circ)$ heißt endlich erzeugt als Gruppe, falls ein $N \subseteq G$ mit $|N|$ endlich und $G = \langle N \rangle$ existiert.

Bemerkung. Sei $(G, \circ)$ eine Gruppe sowie $N \subseteq G$. Dann wird G genau dann von N erzeugt (also $G = \langle N \rangle$), wenn für alle $g \in G$ Elemente $n_1, \ldots, n_r \in G$ mit $r \in \mathbb{N}_0$ existieren, sodass $g = n_1 \circ \cdots \circ n_r$ (mit $g = e$, falls $r = 0$) und $n_i \in N$ oder $n_i^{-1} \in N$ für alle $1 \leq i \leq r$ gelten.

Beweis.

„$\Leftarrow$“: Sei $g \in G$ und $g = n_1 \circ \cdots \circ n_r$ wie oben. Daraus folgt $g \in \langle N \rangle$, da $n_1, \ldots, n_r \in \langle N \rangle$ und damit auch $g \in \langle N \rangle$, weil $\langle N \rangle$ eine Gruppe ist. Deshalb folgt $G \subseteq \langle N \rangle$, also $G = \langle N \rangle$.

„$\Rightarrow$“: Sei $G = \langle N \rangle$. Wir behaupten $H \coloneqq \{g \in G \mid g \text{ von obiger Form}\} < G$, was der aufmerksame Leser sich in einer ruhigen Minute selber überlegen möge.

Da $\langle N \rangle \subseteq H$ nach Definition von $\langle N \rangle$ gilt und $\langle N \rangle$ eine Gruppe ist, muss also $\langle N \rangle = H$ wegen Minimalität gelten, da $N \subseteq H$ gilt. Nach Voraussetzung folgt $G = H$. Also hat jedes $g \in G$ die obige Form. □

Beispiel 3. Beispiele für Erzeugendensysteme:

- $\{\text{Transpositionen}\} \subseteq S_n$, d.h. (i, j) mit $1 \leq i < j \leq n$ erzeugen die Gruppe S_n.
- $\{\text{Einfache Transpositionen}\} \subseteq S_n$, d.h. (i, j) mit $1 \leq i < j = i + 1 \leq n$ erzeugt S_n.

Definition 1.7. Eine Gruppe G heißt zyklisch, falls ein $g \in G$ existiert, sodass $\langle \{g\} \rangle = G$ gilt, also G von einem Element erzeugt wird.

Man beachte $\langle \{g\} \rangle = \{e, g, g^{-1}, g^2, g^{-2}, \ldots\} = \{g^i \mid i \in \mathbb{Z}\}$.

Beispiel 4. $(\mathbb{Z}, +)$ ist zyklisch mit $\mathbb{Z} = \langle\{1\}\rangle = \langle\{-1\}\rangle$.

Definition 1.8. Seien $(G, \circ)$ und $(G', \circ')$ Gruppen. Ein Gruppenhomomorphismus von G nach G' ist eine Abbildung $f\colon G \to G'$ mit $f(g \circ h) = f(g) \circ' f(h)$ für alle $g, h \in G$.

f ist ein Gruppenisomorphismus, falls f zusätzlich invertierbar ist. Wir schreiben $(G, \circ) \cong (G', \circ')$, falls ein Gruppenisomorphismus von G nach G' existiert und nennen die Gruppen isomorph.

Eigenschaften von Gruppenhomomorphismen. Sei $f\colon G \to G'$ ein Gruppenhomomorphismus von G nach G'. Dann gilt:

(E1) f ist genau dann ein Gruppenisomorphismus, wenn f^{-1} ein Gruppenisomorphismus ist. Nach Definition existiert f^{-1}; es ist somit $f^{-1}(g' \circ' h') = f^{-1}(g') \circ f^{-1}(h')$ für alle $g', h' \in G$ zu zeigen. Seien also $g', h' \in G'$. Es existieren $g, h \in G$ mit $f(g) = g', f(h) = h'$. Es folgt

$$f^{-1}(g' \circ' h') = f^{-1}(f(g) \circ' f(h)) = f^{-1}(f(g \circ h)) = g \circ h = f^{-1}(g') \circ f^{-1}(h').$$

(E2) f bildet das neutrale Element auf das neutrale Element ab.

[9. Oktober 2017]

[12. Oktober 2017]

(E3) f bildet Inverse auf Inverse ab.

(E4) Sei $(G'', \circ'')$ eine weitere Gruppe sowie $f'\colon G' \to G''$ ein Gruppenhomomorphismus von $(G', \circ')$ nach $(G'', \circ'')$. Dann ist $f' \circ f$ ein Gruppenhomomorphismus, da

$$(f' \circ f)(g \circ h) = f'(f(g \circ h)) = f'(f(g) \circ' f(h)) = (f' \circ f)(g) \circ'' (f' \circ f)(h)$$

für alle $g, h \in G$ gilt.

Beispiel 5. Beispiele für Gruppenhomomorphismen:

- $\mathrm{id}_G\colon G \to G,\ g \mapsto g$ ist ein Gruppenhomomorphismus von $(G, \circ)$ nach $(G, \circ)$.

  Achtung: id_G ist kein Gruppenhomomorphismus von $(G, \circ)$ nach $(G, \circ_a)$, falls $a \neq e$.

- $\det\colon \mathrm{GL}_n(K) \to K^*$ für einen Körper K ist ein Gruppenhomomorphismus.

- $f\colon \mathbb{R}^* \to \mathbb{R}_{\geq 0},\ x \mapsto |x|$ ist ein Gruppenhomomorphismus von $(\mathbb{R}^*, \cdot)$ nach $(\mathbb{R}_{\geq 0}, \cdot)$.

- $x \mapsto \exp(x)$ ist ein Gruppenhomomorphismus von $(\mathbb{Z}, +)$ nach $(\mathbb{R}^*, \cdot)$.

- Betrachte $G = \left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \middle| a \in \mathbb{Z} \right\} < \mathrm{GL}_n(\mathbb{R}, \cdot)$ und $f\colon \mathbb{Z} \to G,\ a \mapsto \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$. Das ist ein Gruppenhomomorphismus von $(\mathbb{Z}, +)$ nach $(G, \text{Matrixmultiplikation})$. Es ist sogar ein Gruppenisomorphismus mit dem Inversen $\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \mapsto a$.
- *Trivialer Gruppenhomomorphismus*: Schicke alles auf das neutrale Element.
- Sei $(G, \circ)$ eine Gruppe und $a \in G$. Dann ist $f\colon G \to G,\ g \mapsto g \circ a^{-1}$ ein Gruppenhomomorphismus von $(G, \circ)$ nach $(G, \circ_a)$.

Lemma 1.1. *Sei $n \in \mathbb{Z}$.*

1. *Dann existiert genau ein Gruppenhomomorphismus* $\mathrm{can}\colon \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ *von* $(\mathbb{Z}, +)$ *nach* $(\mathbb{Z}/n\mathbb{Z}, +)$ *mit* $\mathrm{can}(1) = \overline{1}$.
2. *Falls $n \neq 0$, so existiert kein nichttrivialer Gruppenhomomorphismus $f\colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}$.*

Beweis.

1. Eindeutigkeit: Sei $f\colon \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ ein Gruppenhomomorphismus. Dann folgt $f(0) = \overline{0}$ und falls $f(1) = \overline{1}$, so gilt $f(n) = f(1 + \ldots 1) = n \cdot f(1)$ für alle $n \in \mathbb{N}$ und damit auch $f(-n) = -nf(1)$. Dadurch ist f eindeutig definiert.

   Gruppenhomomorphismus: Es gilt dann $\mathrm{can}(x) = \overline{x}$ für alle $x \in \mathbb{Z}$ und da $\mathrm{can}(x + y) = \overline{x + y} = \overline{x} + \overline{y} = \mathrm{can}(x) + \mathrm{can}(y)$ ist das auch ein Gruppenhomomorphismus.
2. Sei $n \neq 0$, $f\colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}$ ein Gruppenhomomorphismus und $f(\overline{1}) = x$. Dann gilt (o.B.d.A. $n \in \mathbb{N}$) $0 = f(\overline{0}) = f(\overline{n}) = f(\overline{1} + \ldots \overline{1}) = nf(\overline{1}) = nx$, also $x = 0$. Somit ist f ein trivialer Gruppenhomomorphismus. □

Lemma 1.2. *Sei $(G, \circ)$ eine Gruppe.*

1. *Sei* $\mathrm{Aut}(G) := \{f\colon G \to G \mid f$ *Gruppenisomorphimus von* $(G, \circ)$ *nach* $(G, \circ)\}$. *Dann ist* $\mathrm{Aut}(G)$ *eine Gruppe, die Automorphismengruppen von G.*
2. *Betrachte die Abbildung* $\mathrm{Konj}\colon G \to \mathrm{Aut}(G),\ g \mapsto \mathrm{Konj}(g)$, *wobei* $\mathrm{Konj}(g)(h) = g \circ\ h \circ g^{-1}$ *für alle $h \in G$. Dann ist* Konj *ein Gruppenhomomorphismus von G nach* $\mathrm{Aut}(G)$, *welcher im Allgemeinen nicht injektiv ist.*

Beweis. Einfaches Nachrechnen. □

Bemerkung.

1. Falls $(G, \circ)$ abelsch ist, dann ist jede Konjugation die Identität.
2. $\mathrm{Konj}(g) = \mathrm{id}_G \Leftrightarrow g \in Z(G) := \{x \in G \mid x \circ y = y \circ x\ \ \forall y \in G\}$

Konvention: Von jetzt an schreiben wir meist gh statt $g \circ h$ und G statt $(G, \circ)$.

Satz 1.3. *Sei $f\colon G \to G'$ ein Gruppenhomomorphismus. Dann gilt:*

$$\begin{array}{lll} \ker(f) & \coloneqq \{g \in G \mid f(g) = e\} & < G \quad \textit{Kern von } f \\ \operatorname{im}(f) & \coloneqq \{g' \in G' \mid \exists g \in G : f(g) = g'\} & < G' \quad \textit{Bild von } f \end{array}$$

Beweis. Einfaches Nachrechnen. □

Beispiel 6.

1. $\ker(\mathrm{can}\colon \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}) = n\mathbb{Z} < \mathbb{Z}$
2. $\ker(\mathrm{Konj}\colon G \to \mathrm{Aut}(G)) = Z(G) < G$
3. $\ker(\det\colon \mathrm{GL}_n(K) \to K^*) = \mathrm{SL}_n(K)$

Übung: Ein Gruppenhomomorphismus$f$ ist genau dann injektiv, wenn $\ker f = \{e\}$.

Satz 1.4 (Satz von Cayley)**.** *Sei G eine Gruppe. Dann ist*

$$\begin{aligned} \Phi\colon G &\longrightarrow S_G \\ g &\longmapsto \Phi(g) \end{aligned}$$

mit $\Phi(g)(h) = gh$ für alle $h \in G$ ein injektiver Gruppenhomomorphismus. (Damit kann man G als Untergruppe einer Permutationsgruppe „realisieren“.)

Beweis.

Wohldefiniertheit: $\Phi(g)$ ist invertierbar mit Inversem $h \mapsto g^{-1}h$.

Gruppenhomomorphismus: Zu zeigen: $\Phi(g_1g_2) = \Phi(g_1) \circ \Phi(g_2)$, also $\Phi(g_1g_2)(h) = \Phi(g_1)(\Phi(g_2)(h))$ für alle $h \in G$. Es gilt $\Phi(g_1g_2)(h) = g_1g_2h$ und $\Phi(g_1)(\Phi(g_2)(h)) = \Phi(g_1)(g_2h) = g_1g_2h$, was zu zeigen war.

Injektivität: Es reicht zu zeigen, dass der Kern trivial ist. Sei $g \in \ker\Phi \Leftrightarrow \Phi(g) = e = \mathrm{id}_G \Leftrightarrow \Phi(g)(h) = h\ \forall h \in G \Leftrightarrow gh = h\ \forall h \in G \Leftrightarrow g = e$. □

2. Satz von Lagrange und Normalteiler

Definition 2.1. Sei G eine Gruppe, $H < G$ eine Untergruppe und $a \in G$. Dann ist:

- $aH = \{ah \mid h \in H\} \subseteq G$ die Linksnebenklasse von H zu a
- $Ha = \{ha \mid h \in H\} \subseteq G$ die Rechtsnebenklasse von H zu a

Meist arbeiten wir mit Linksnebenklassen und nennen sie einfach Nebenklassen.

Aus der Linearen Algebra wissen wir folgendes:

1. Zwei Nebenklassen sind gleich oder disjunkt d.h. $aH \cap bH \neq \emptyset \Leftrightarrow aH = bH \Leftrightarrow b^{-1}a \in H$.

2. Die Abbildung $aH \to H,\ ah \mapsto h$ ist bijektiv. Alle Nebenklassen haben somit dieselbe Kardinalität.

3. Es gilt
$$G = \bigcup_{g \in G} gH = \dot{\bigcup_{b \in R}} bH,$$
wobei $R \subseteq G$, sodass die bH mit $b \in R$ genau ein Repräsentantensystem für die verschiedenen Nebenklassen bilden.

4. $g \in aH \Leftrightarrow g^{-1} \in Ha^{-1}$ (dadurch ergibt sich eine Bijektion zwischen Links- und Rechtsnebenklassen)

Definition 2.2. Bezeichne mit G/H die Menge der Linksnebenklassen von G bezüglich H und mit $H\backslash G$ die Menge der Rechtsnebenklassen. Dann gilt $|G/H| = |H\backslash G|$ (nach dem 4. Beispiel oben). Wir nennen diese Zahl den Index, auch $(G : H)$, von H in G.

Satz 2.1 (Satz von Lagrange)**.** *Sei G eine eine endliche Gruppe sowie $H < G$ eine Untergruppe. Dann gilt*
$$|G| = |H| \cdot (G : H).$$
Insbesondere: $|G| = p$ Primzahl $\Rightarrow H = \{e\}$ oder $H = G$.

Beweis. Die Formel folgt direkt aus Beispiel 3, 2 und der Definition des Index.
Falls nun $|G| = p$ gilt, so muss auch $|H| = 1$ oder $|H| = p$ gelten, woraus $H = \{e\}$ oder $H = G$ folgt. □

Noch mehr Wissen aus der Linearen Algebra: Falls G abelsch ist, dann ist G/H wieder eine Gruppe mit Gruppenoperation
$$\begin{aligned} \circ \colon G/H \times G/H &\longrightarrow G/H \\ (aH, bH) &\longmapsto abH \end{aligned}$$

Im Allgemeinen (falls G nicht abelsch ist) ist $\circ$ nicht wohldefiniert (siehe Übungsblatt 2).

Definition 2.3. Sei G eine Gruppe. Eine Untergruppe $H < G$ heißt Normalteiler, falls
$$\forall g \in G, h \in H : g \circ h \circ g^{-1} \in H$$
gilt. Wir schreiben dann $H \lhd G$.

Bemerkung. Falls G abelsch, dann ist jede Untergruppe Normalteiler.

Lemma 2.2. *Sei $f \colon G \to G'$ ein Gruppenhomomorphismus. Dann gilt* $\ker(f) \lhd G$.

Beweis. Sei $g \in G$ und $h \in \ker f$. Dann gilt:
$$\begin{aligned} & f(ghg^{-1}) = f(g)f(h)f(g)^{-1} = f(g)f(g)^{-1} = e \\ & \Rightarrow ghg^{-1} \in \ker f \\ & \Rightarrow \ker f \lhd G \end{aligned}$$
□

[9. Oktober 2017]
[16. Oktober 2017]

Satz 2.3. *Sei G eine Gruppe, $N \lhd G$ ein Normalteiler. Dann gilt:*

1. *G/N bildet Gruppe mit $\circ\colon G/N \times G/N \to G/N, \quad (aN, bN) \mapsto abN$.*
2. *Die Abbildung*

$$\begin{aligned} \mathrm{can}\colon G &\longrightarrow G/N \\ g &\longmapsto gN \end{aligned}$$

ist ein surjektiver Gruppenhomomorphismus.

Beweis.

1. Es gilt $(aN \circ bN) \circ cN = abN \circ cN = abcN = aN \circ (bN \circ cN) \Rightarrow$ (G1). Offensichtlich ist $eN = N$ neutrales Element $\Rightarrow$ (G2). $a^{-1}N$ ist das Inverse zu $aN \Rightarrow$ (G3).

   Jetzt ist noch die Wohldefiniertheit zu zeigen. Sei also $a_1N = a_2N$ und $b_1N = b_2N$. Daraus sollte $a_1b_1N = a_2b_2N$ folgen.

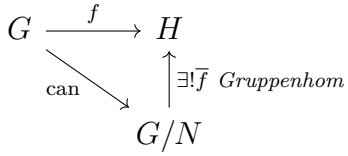
   Tatsächlich gilt $a_1^{-1}a_2 \in N$ und $b_1^{-1}b_2 \in N$. Dann gilt auch $(a_1b_1)^{-1}(a_2b_2) = b_1^{-1}a_1^{-1}a_2b_2$, wobei $a_1^{-1}a_2 \in N$ und

$$\begin{aligned} & b_1^{-1}a_1^{-1}a_2b_2 = b_1^{-1}b_2(b_2^{-1}a_1^{-1}a_2b_2) \in N \\ \Rightarrow\ & (a_1b_1)^{-1}a_2b_2 \in N \\ \Rightarrow\ & a_1b_1N = a_2b_2N \end{aligned}$$

2. Surjektivität ist klar nach (3); um zu zeigen, dass das ein Gruppenhomomorphismus ist, muss man das einfach nachrechnen. □

Bemerkung. Somit gilt, dass Normalteiler genau die Kerne von Gruppenhomomorphismen sind.

Satz 2.4 (Homomorphiesatz)**.** *Sei $f\colon G \to H$ ein Gruppenhomomorphismus. Sei $N \lhd G$ ein Normalteiler. Dann: $N \subseteq \ker(f) \Leftrightarrow \exists!$ Gruppenhomomorphismus $\overline{f}\colon G/N \to H$, sodass $\overline{f} \circ \mathrm{can} = f$. Also*

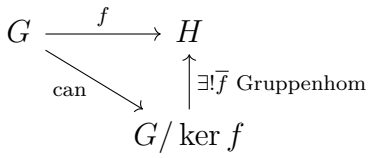


Beweis. „⇐“: $\ker(\text{can}) = \{g \in G | gN = N\} = \{g \in G | g \in N\} = N \Rightarrow f(N) = \overline{f}(\text{can}(N)) = \overline{f}(e) = e \Rightarrow N \subseteq \ker(f)$.
„⇒“: Eindeutigkeit: Es muss für $\overline{f}$ gelten: $\overline{f}(aN) = \overline{f}(\text{can}(a)) = f(a)\ \forall aN \in G/N \Rightarrow \overline{f}$ eindeutig bestimmt durch f.

Existenz: Wir setzen $\overline{f}(aN) := f(a)\ \forall aN \in G/N$. Das ist offensichtlich wohldefiniert. Nachrechnen ergibt, dass es auch ein Gruppenhomomorphismus ist. □

Korollar 2.5. *Sei $f\colon G \to H$ ein Gruppenhomomorphismus. Dann gilt $G/\ker f \cong \operatorname{im} f$.*

Beweis. $\ker f \lhd G$ nach Lemma 2.2 $\Rightarrow G/\ker f$ ist eine Gruppe nach Satz 2.3. $\operatorname{im} f$ ist eine Gruppe nach Satz 1.3. Setze $N \coloneqq \ker f$. Klar: $N \subseteq \ker f$. Also existiert nach Satz 2.4 ein $\overline{f}$, sodass



Also haben wir $\overline{f}\colon G/\ker f \to \operatorname{im} f$ ein Gruppenhomomorphismus. Er ist surjektiv, weil can surjektiv ist.
Behauptung: $\overline{f}$ ist injektiv.

Es gilt $\overline{f}(aN) = f(a) = e \Leftrightarrow a \in \ker f = N$. Also $\ker \overline{f} = \{N\}$, was das neutrale Element in $G/\ker f$ ist. Also ist $\overline{f}$ injektiv. $\Rightarrow \overline{f}$ ist Gruppenisomorphismus. □

Satz 2.6 (1. Isomorphiesatz)**.** *Sei G eine Gruppe, $H < G$, $N \lhd G$. Es gilt:*

1. $HN \coloneqq \{hn | h \in H, n \in N\} < G$
2. $N \lhd HN$, $(H \cap N) \lhd H$
3. $H/(H \cap N) \cong HN/N$ *mit dem Gruppenisomorphismus* $h(H \cap N) \mapsto hN$

Beweis.

1. $HN \neq \emptyset$, da $e = ee \in HN$. Seien $h_1n_1, h_2n_2 \in HN$ $(h_i \in H, n_i \in N)$. Dann ist $h_1n_1(h_2n_2)^{-1} = h_1n_1n_2^{-1}h_2^{-1} = h_1h_2^{-1}h_2n_1n_2^{-1}h_2^{-1}$, wobei $n_1n_2^{-1} \in N$. Somit gilt auch $h_2n_1n_2^{-1}h_2^{-1} \in N$, da $N \lhd G$. Da $h_1h_2^{-1} \in H$ ist der gesamte Ausdruck Element von HN.

2. Zunächst zeigen wir, dass $N \lhd HN$. Es gilt $N \subseteq HN$, da $n = en$. Daraus folgt, dass $N < HN$ weil $N < G$; analog auch $N \lhd HN$, weil $N \lhd G$.

   Noch zu zeigen: $(H \cap N) \lhd H$. Es ist offensichtlich, dass $(H \cap N) \subseteq H$ und $(H \cap N) < H$, weil $(H \cap N) < G$. Sei $x \in H \cap N$, $h \in H$. Dann gilt $hxh^{-1} \in H$, weil $H < G$ und $hxh^{-1} \in N$ gilt, da $N \lhd G$. Also $hxh^{-1} \in (H \cap N) \Rightarrow H \cap N \lhd H$

3. Betrachte

$$\begin{aligned} f\colon H &\longrightarrow HN \xrightarrow{\text{can}} HN/N \\ h &\longmapsto he \end{aligned}$$

Es lässt sich leicht nachprüfen, dass f ein Gruppenhomomorphismus ist. Für $x \in H$ gilt $x \in \ker(f) \Leftrightarrow xeN = N \Leftrightarrow x = xe \in \ker(\text{can}) = N \Leftrightarrow x \in (H \cap N)$. Also existiert nach dem Homomorphiesatz ein Gruppenhomomorphismus $\overline{f}$:

$$\overline{f}\colon H/(H \cap N) \longrightarrow (HN)/N$$

Dieser ist nach Konstruktion injektiv.

Surjektiv: Sei $hnN \in (HN)/N$ mit $h \in H, n \in N$. Dann gilt aber: $hnN = hN$ und dann $f(h) = hN$. Somit gilt $\overline{f} \circ \text{can}(h) = \overline{f}(\text{can}(h)) = hN$ woraus folgt, dass $hN \in \text{im}\, f$. Folglich ist $\overline{f}$ surjektiv und deshalb ein Gruppenisomorphismus. □

Anmerkung zu Beweis des Homomorphiesatzes: Wo wird in „⇒“verwendet, dass $N \subseteq \ker f$? Es wird benötigt für die Wohldefiniertheit von $\overline{f}$.

Satz 2.7 (2. Isomorphiesatz)**.** *Sei G eine Gruppe; $N_1 \lhd G$, $N_2 \lhd G$, $N_1 \subseteq N_2$. Dann gilt $N_1 \lhd N_2$ und $N_2/N_1 \lhd G/N_1$ und es gilt:*

$$(G/N_1)/(N_2/N_1) \cong G/N_2$$

durch den Isomorphismus $(gN_1)N_2/N_1 \mapsto gN_2$.

Beweis. G/N_1 ist eine Gruppe, weil $N_1 \lhd G$. Analog für N_2. Auch gilt $N_2/N_1 \subseteq G/N_1$. Aus $N_1 \subseteq N_2$ folgt, dass $N_1 \lhd N_2$, weil $N_1 \lhd G$. Sei

$$\begin{aligned} f\colon G/N_1 &\longrightarrow G/N_2 \\ gN_1 &\longmapsto gN_2 \end{aligned}$$

Das ist wohldefiniert: Seien $g, h \in G$.

$$\begin{aligned} &gN_1 = hN_1 \\ &\Rightarrow g^{-1}h \in N_1 \subseteq N_2 \\ &\Rightarrow gN_2 = hN_2 \\ &\Rightarrow \text{wohldefiniert} \end{aligned}$$

Klar: f ist surjektiv und $gN_1 \in \ker(f) \Leftrightarrow gN_2 = N_2 \Leftrightarrow g \in N_2$. Also gilt $\ker(f) = \{gN_1 | g \in N_2\} = N_2/N_1$. Also insbesondere $N_2/N_1 \lhd G/N_1$. Nach dem Korollar des Homomorphiesatzes erhalten wir einen Gruppenhomomorphismus

$$\overline{f}\colon (G/N_1)/\ker f (= N_2/N_1) \longrightarrow \text{im}\, f = G/N_2 \text{ (da } f \text{ surjektiv)}$$

Nach Kosntruktion ist $\overline{f}$ injektiv, also erhalten wir den gewünschten Gruppenisomorphismus mit $\overline{f}(gN_1 \cdot (N_2/N_1)) = f(gN_1) = gN_2$. □

Anwendungen

1. *Anzahlformel:* Sei G eine endliche Gruppe, $H < G$, $N \lhd G$. Dann gilt

$$|HN| = \frac{|H||N|}{|H \cap N|}$$

   Denn nach dem Satz von Lagrange ist $|H| = |H \cap N|(H : H \cap N)$ und $|HN| = |N|(HN : N)$. Nach dem 1. Isomorphiesatz ist $(H : H \cap N) = (HN : N)$. ✓

2. Sie $(G, \circ) = (\mathbb{Z}, +)$, $m, n \in \mathbb{N}$ und $m|n$. Wir wissen: $m\mathbb{Z} < \mathbb{Z}$ und $n\mathbb{Z} < \mathbb{Z}$ (sogar Normalteiler, weil G abelsch ist). Klar ist: $n\mathbb{Z} \subseteq m\mathbb{Z}$ (insbesondere auch $n\mathbb{Z} \lhd m\mathbb{Z}$). Dann gilt
$$(\mathbb{Z}/n\mathbb{Z})/(m\mathbb{Z}/n\mathbb{Z}) \cong \mathbb{Z}/m\mathbb{Z}$$

3. Zyklische Gruppen

Wir schreiben kurz $\langle g \rangle$ statt $\langle \{g\} \rangle$.

Satz 3.1. *Untergruppen von zyklischen Gruppen sind zyklisch.*

Beweis. Sei G eine zyklische Gruppe; $G = \langle g \rangle$ mit $g \in G$. Sei $H < G$.

Fall 1 $H = \{e\} = \langle e \rangle$, also zyklisch

Fall 2 $H \neq \{e\} \Rightarrow \exists m \in \mathbb{Z} \setminus \{0\} : e \neq g^m \in H \Rightarrow \exists n \in \mathbb{N} : e \neq g^n \in H$ (weil $H < G$). Wähle $n := \min\{j \in \mathbb{N} | e \neq g^j \in H\}$. Behauptung: $H = \langle g^n \rangle$.

„$\supseteq$“: Klar, da $g^n \in H$

„$=$“: Angenommen, Gleichheit gilt nicht. Also $\exists s \in \mathbb{Z} : g^s \in H \setminus \langle g^n \rangle$ (beachte $G = \langle g \rangle$). Schreibe $s = an + r$ für $a, r \in \mathbb{Z}$ und $0 \leq r < n$. Falls $r = 0$, dann $s = an$ und $g^s = g^{an} = (g^n)^a \in \langle g^n \rangle$ Widerspruch!

Falls $r > 0$: Dann $g^r = (g^{an})^{-1} g^{an} g^r = ((g^n)^a)^{-1} g^s \in H$ (Widerspruch zur Minimalität)

Somit war die Annahme falsch und H ist zyklisch. □

[16. Oktober 2017]

[19. Oktober 2017]

Lemma 3.2. *Bilder von zyklischen Gruppen unter Gruppenhomomorphismen sind zyklisch.*

Beweis. Sei $f : G \to G'$ ein Gruppenhomomorphismus und sei G zyklisch, also $G = \langle g \rangle$ für ein $g \in G \Rightarrow G = \{g^i | i \in \mathbb{Z}\}$ also $f(G) = \{f(g^i) | i \in \mathbb{Z}\} = \{(f(g^i)) | i \in \mathbb{Z})\} = \langle f(g) \rangle \Rightarrow \operatorname{im} f = \langle f(g) \rangle$ zyklisch. □

Lemma 3.3. *Sei G endliche Gruppe $|G| = n < \infty$. Sei $g \in G$ mit $G = \langle g \rangle$ (also G zyklisch). Sei* $\operatorname{ord}(g) = \min\{j \in \mathbb{N} | g^j = e\}$. *Dann gilt:* $\operatorname{ord}(g) = n$.

Definition 3.1. Allgemeiner: Sei G irgendeine Gruppe, $g \in G$. Dann definiere

$$\operatorname{ord}(g) \coloneqq \begin{cases} \min\{j \in \mathbb{N} | g^j = e\} & \text{falls das existiert} \\ \infty & \text{sonst} \end{cases}$$

Wir nennen $\operatorname{ord}(g)$ die Ordnung von $g \in G$.

Beweis von Lemma 3.3. 1. Behauptung: $\operatorname{ord}(g)$ existiert. Angenommen es existiert nicht, also $g^j \neq g \ \forall j \in \mathbb{N} \Rightarrow g^i \neq g^j$ falls $i \neq j$, $i, j \in \mathbb{N}$ (denn sonst gilt $g^{i-j} = e = g^{j-i}$ mit $i - j \in \mathbb{N}$ oder $j - i \in \mathbb{N}$). Also $|G| = \infty \Rightarrow$ Widerspruch.

Jetzt ist noch zu zeigen, dass $n = \operatorname{ord}(g)$ gilt. Dazu sei $S \coloneqq \left\{g, g^2, \ldots, g^{\operatorname{ord}(g)} = e\right\} \subset G$.

2. Behauptung: $S < G$. Klar: $e \in S$. Sei $g^a, g^b \in S$. Schreibe $a - b = k \cdot \operatorname{ord}(g) + r$, wobei $k, r \in \mathbb{Z}, 0 \leq r < \operatorname{ord}(g)$. Daraus folgt

$$g^a \left(g^b\right)^{-1} = g^{a-b} = g^{k \cdot \operatorname{ord}(g) + r} = \left(g^{\operatorname{ord}(g)}\right)^k g^r = e^k g^r = e g^r = g^r \in S$$

weil $0 \leq r < \operatorname{ord}(g)$. Da $g \in S$, gilt $\langle g \rangle \subset S$. Weil $S < G$ ist klar, dass $S \subset \langle g \rangle$, also $\langle g \rangle = S$.

3. Behauptung: $|S| = \operatorname{ord}(g)$. Seien $g^i, g^j \in S$ mit $1 \leq i, j \leq \operatorname{ord}(g)$ und $g^i = g^j$. Also $g^{i-j} = e = g^{j-i}$, was ein Widerspruch zur Minimaltität von $\operatorname{ord}(g)$ ist außer $i = j$. Folglich sind die $g^i (1 \leq i \leq \operatorname{ord}(g))$ paarweise verschieden, was die Behauptung zeigt. □

Bemerkung. Sei G irgendeine Gruppe, $g \in G$. Dann gilt: $\operatorname{ord}(g) = |\langle g \rangle|$ und nach Satz von Lagrange denn $\operatorname{ord}(g)$ teilt $|G|$, falls $|G|$ endlich.

Satz 3.4 (Klassifikation zyklischer Gruppen)**.** *Je zwei zyklische Gruppen der selben Ordnung sind isomorph. Genauer gilt für G zyklische Gruppe:*

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

Beweis. Sei $G = \langle g \rangle$ mit $g \in G$. Sei $f : \mathbb{Z} \to G : j \mapsto g^j$. Dann ist f ein Gruppenhomomorphismus (nachrechnen) und surjektiv, da $G = \langle g \rangle$.

Fall 1 $|G| = \infty$. Dann muss f injektiv sein, damit f ein Isomorphismus ist und damit $\mathbb{Z} \cong G$. Falls f nicht injektiv ist, dann $\exists i, j \in \mathbb{Z}, i \neq j$ mit $g^i = g^j$, als $g^{i-j} = e = g^{j-i}$. Folglich ist $\operatorname{ord}(g) < \infty$. Damit wäre G nach 3.3 endlich, was ein Widerspruch ist.

Fall 2 $|G| = n$ endlich. Dann folgt aus 3.3:

$$\operatorname{ord}(g) = n \Rightarrow g^n = e \Rightarrow g^{nk} = (g^n)^k = e^k = e \ \forall k \in \mathbb{Z} \Rightarrow n\mathbb{Z} \subset \ker F$$

Nach dem Homomorphiesatz gilt dann:

$$\begin{array}{ccc} \mathbb{Z} & \xrightarrow{f} & G \\ & \searrow^{\text{can}} & \uparrow \exists!\ \overline{f}\ \text{Gruppenhom} \\ & & \mathbb{Z}/n\mathbb{Z} \end{array}$$

Also $\overline{f} : \mathbb{Z}/n\mathbb{Z} \to G$. Da $|\mathbb{Z}/n\mathbb{Z}| = n = |G|$ muss diese surjektive Abbildung schon ein Isomorphismus sein. □

4. Auflösbare Gruppen

Definition 4.1. Eine Normalreihe eine Gruppe G ist eine Kette von Untergruppen der Form $\{e\} = G_0 \lhd G_1 \lhd \ldots \lhd G_n = G$. Man nennt die Quotientengruppe G_i/G_{i-1} die Faktoren der Normalreihe.

Definition 4.2. Eine Gruppe heißt auflösbar, falls eine Normalreihe mit abelschen Faktoren existiert.

Beispiel 1.

1. Abelsche Gruppen sind auflösbar: $\{e\} \lhd G$ und $G/\{e\} \cong G$, also abelsch
2. Sei $G = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in \mathrm{GL}_2(K) \right\} < \mathrm{GL}_2(K)$. Behauptung: G ist auflösbar. Dazu betrachtet man $G' = \left\{ \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \in \mathrm{GL}_2(K) \right\} < \mathrm{GL}_2(K)$, wobei G' insbesondere eine Gruppe ist.
$$f : G \longrightarrow G' : \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \longmapsto \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}$$
was ein Gruppenepimorphismus ist (nachrechnen). Es gilt:
$$\ker f = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} | b \in K \right\} \lhd G$$
Folglich gilt $\ker f \cong (K, +)$, sodass $\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \mapsto b$, weil $\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & b' \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & b+b' \\ 0 & 1 \end{pmatrix}$ als Gruppenhomomorphismus offensichtlich bijektiv ist. Damit ist $\ker f$ abelsch und G' somit auch.
$$\Rightarrow \{e\} = G_0 \lhd \ker f = G_1 \lhd G_2 = G$$
und $\ker f/\{e\}$ abelsch, sowie auch $G/\ker f \cong \operatorname{im} f = G'$ abelsch. Somit ist G auflösbar.

3. S_4 ist auflösbar. Betrachte

$$S_4 > A_4 := \{\pi \in S_4 | \operatorname{sgn}(\pi) = 1\}$$

Nach LA 1 ist sgn ein Gruppenhomomorphismus und damit $A_4 = \ker(\operatorname{sgn}) < S_4$. Es gilt $S_4 \lhd A_4$, weil $A_4 = \ker(\operatorname{sgn})$ oder weil $(S_4 - A_4) = 2$, was dann nach Blatt 2 folgt. Betrachte nun

$$A_4 > V_4 := \left\{ e, \underbrace{(1,2)(3,4)}_{a}, \underbrace{(1,3)(2,4)}_{b}, \underbrace{(1,4)(2,3)}_{c} \right\}$$

Gruppentafel:

	a	b	c
a	e	c	b
b	c	e	a
c	b	a	e

Dann gilt $A_4 \lhd V_4$, da folgendes gilt:

$$\forall \pi \in S_4 : \pi \circ \underbrace{(a_1, a_2)(a_3, a_4)}_{\tau} \circ \pi^{-1} = (\pi(a_1), \pi(a_2))(\pi(a_3), \pi(a_3))$$

weil

$$\begin{aligned}
\pi(a_1) &\overset{\pi^{-1}}{\longmapsto} a_1 \overset{\tau}{\mapsto} a_2 \overset{\pi}{\mapsto} \pi(a_2) \\
\pi(a_2) &\longmapsto a_2 \mapsto a_1 \mapsto \pi(a_1) \\
\pi(a_3) &\longmapsto a_3 \mapsto a_4 \mapsto \pi(a_4) \\
\pi(a_4) &\longmapsto a_4 \mapsto a_3 \mapsto \pi(a_3)
\end{aligned}$$

also $V_4 \lhd A_4$. Folglich haben wir

$$\{e\} = G_0 \lhd V_4 = G_1 \lhd A_4 = G_2 \lhd S_4 = G_3$$

$G_1/G_0 \cong V_4$ ablesch

$G_2/G_1 \cong \mathbb{Z}/2\mathbb{Z}$ also abelsch, da jede Gruppe H der Ordunung 2 zyklisch mit $H = \langle g \rangle (g \neq e)$ ist und dann nach Klassifikationssatz $H \cong \mathbb{Z}/2\mathbb{Z}$

G_3/G_2 Wir wissen, dass $|G_3/G_2| = 3$. Dann behaupten wir, dass $G_3/G_2 \cong \mathbb{Z}/3\mathbb{Z}$. Jede Gruppe H mit $|H| = 3$ ist zyklisch, denn $\langle g \rangle < H (g \neq e)$. Nach dem Satz von Lagrange gilt $\langle g \rangle = H$, weil $\langle g \rangle \neq e$ und 3 prim ist. Also folgt die Aussage aus dem Klassifikationssatz.

Daraus folgt, dass S_4 auflösbar ist.

Satz 4.1. *Untergruppen und Bilder unter Gruppenhomomorphismen von auflösbaren Gruppen sind auflösbar.*

Beweis. Sei G auflösbar. Dann existiert eine Auflösung

$$\{e\} = G_0 \lhd G_1 \lhd \ldots \lhd G_n = G, \qquad G_i/G_{i-1} \text{ abelsch.}$$

Untergruppe:

1. Sei $U < G$. Behauptung: $\{e\} = G_0 \cap U \lhd (G_1 \cap U) \lhd \ldots \lhd (G_n \cap U) = U$. Es ist klar, dass $(G_{i-1} \cap U) \subset (G_i \cap U)$. Auch klar ist, dass $G_i \cap U$ eine Gruppe ist und $(G_{i-1}) < (G_i \cap U)$. Jetzt ist noch zu zeigen, dass $(G_{i-1} \cap U) \lhd (G_i \cap U)$. Sei $x \in G_{i-1} \cap U$ und sei $y \in G_i \cap U$. Dann folgt, dass $\underbrace{yxy^{-1}}_{\in G_{i-1}} \in U$, weil $x, y \in U, U < G$, weil $x \in G_{i-1}, y \in G_i$ und $G_{i-1} \lhd G_i$. Daraus folgt, dass $yxy^{-1} \in U \cap G_{i-1}$, was zu zeigen war.
2. Behauptung: $G_i \cap U/G_{i-1} \cap U$ abelsch. Nach dem 1. Isomorphiesatz gilt $G_i \cap U/G_{i-1} \cap U \cong (U \cap G_i)G_{i-1}/G_{i-1} \lhd G_i/G_{i-1}$ abelsch. Daraus folgt die Behauptung.

[19. Oktober 2017]

[23. Oktober 2017]

Bild: Sei $f\colon G \to G'$ Gruppenhomomorphismus. Behauptung: $\{e\} = f(G_0) \lhd f(G_1) \lhd \ldots \lhd f(G_n) = f(G)$ ist eine Normalreihe mit $f(G_i)/f(G_{i-1})$ abelsch.

Sei $y' = f(y) \in f(G_i)$ mit $y \in G_i$. Dann gilt $y' f(G_{i-1})(y')^{-1} = f(yG_{i-1}y^{-1}) \subseteq f(G_i) \Rightarrow f(G_{i-1}) \lhd f(G_i)$ für alle i. Betrachte nun

$$\alpha\colon G_i \xrightarrow{f} f(G_i) \xrightarrow{\text{can}} f(G_i)/f(G_{i-1}).$$

Dies ist ein Gruppenhomomorphismus, welcher offensichtlich surjektiv ist. Da $G_{i-1} \subseteq \ker\alpha$, existiert Gruppenhomomorphismus $\overline{\alpha}\colon G_i/G_{i-1} \to f(G_i)/f(G_{i-1})$ nach dem Homomorphiesatz. $\overline{\alpha}$ ist surjektiv, da auch α surjektiv ist. Weil G_i/G_{i-1} abelsch ist, ist auch $f(G_i)/f(G_{i-1})$ abelsch. Somit folgt die Behauptung.

□

Definition 4.3. Sei G eine Gruppe, $M \coloneqq \{ghg^{-1}h^{-1} | g, h \in G\}$; dann heißt $[G, G] = \langle M \rangle$ Kommutatorgruppe.

Bemerkung. Nach dem 2. Übungsblatt gilt $[G, G] \lhd G$. $[G, G] \lhd G$ ist sogar der kleinster Normalteiler, sodass $G/[G, G]$ abelsch (denn: sei $N \lhd G, a, b \in G, aNbN = bNaN \Leftrightarrow abN = baN \Leftrightarrow a^{-1}b^{-1}ab \in N \Leftrightarrow [G, G] \subseteq N$).

Betrachte zu einer Gruppe die abgeleitete Reihe:

$$\underbrace{G}_{D^0(G)} \rhd \underbrace{[G, G]}_{D^1(G)} \rhd \underbrace{[D^1(G), D^1(G)]}_{D^2(G)} \rhd \ldots. \tag{*}$$

Satz 4.2. *G auflösbar $\Leftrightarrow \exists m \in \mathbb{N} : D^m(G) = \{e\}$.*

Beweis.

„$\Leftarrow$“ Die abgeleitete Reihe (*) ist nach Definition eine Normalreihe und die Faktoren sind abelsch nach der Bemerkung.

„$\Rightarrow$“ Sei G auflösbar und $\{e\} = G_0 \lhd G_1 \lhd \dots G_n = G$ mit abelschen Faktoren. Nach der Bemerkung gilt G_n/G_{n-1} abelsch $\Rightarrow [G_n, G_n] \subseteq G_{n-1}$.

Behauptung: $D^i(G) \subseteq G_{n-i}$. Dies ist für $i = 0; 1$. $D^{i+1}(G) = [D^i(G), D^i(G)] \subseteq [G_{n-1}, n-1] \subseteq G_{n-i-1}$ nach Bemerkung. Also existiert ein $n \in N$ sodass $D^n(G) \subseteq G_0 = \{e\} \Rightarrow \exists m \coloneqq n$ mit $D^m(G) = \{e\}$. □

5. Gruppenoperationen

Definition 5.1. Sei G eine Gruppe, $X \neq \emptyset$ eine Menge. Eine Operation von G auf X ist eine Abbildung

$$\begin{aligned} \Phi \colon G \times X &\longrightarrow X \\ (g, x) &\longmapsto g.x = \Phi(g, x) \end{aligned}$$

sodass

(O1) $e.x = x$ für alle $x \in X$

(O2) $g.(h.x) = (gh).x$ für alle $g, h \in G, x \in X$

Kurz: G operiert auf X; wir schreiben $G \circlearrowright X$.

Bemerkung. Existenz von Φ ist äquivalent zur Existenz von $\Phi' \colon G \to S_X$ Gruppenhomomorphismus mit $\Phi'(g)(x) \coloneqq g.x$ (nachprüfen!)

Definition 5.2. Gegeben $G \circlearrowright X$, $G \circlearrowright Y$, $f \colon X \to Y$ Abbildung. f heißt G-Homomorphismus, falls $f(g.x) = g.f(x)$ für alle $g \in G$ und $x \in X$.

Definition 5.3. $G \circlearrowright X$, $x \in X$. Dann

1. $G.x = \{g.x \mid g \in G\}$ Bahn von x
2. $G_x = \{g \in G \mid g.x = x\}$ Stabilisator von x
3. $X^G = \{x \in X \mid \forall g \in G \;\; g.x = x\}$ Menge der Fixpunkte

Bemerkung. $x \sim y \Leftrightarrow \colon y \in G.x$ ist eine Äquivalenzrelation:

- $x \sim x$ klar, weil $x = e.x \in G.x$
- $x \sim y \Rightarrow \exists g \in G : g.x = y \Rightarrow x = g^{-1}.y \Rightarrow x \in G.y \Rightarrow y \sim x$

- $x \sim y, y \sim z \Rightarrow x \sim z$ klar nach (O2)

Also $X = \dot{\bigcup}_{\text{Bahnen}}^{\text{versch.}}$.

Definition 5.4. G operiert transitiv, falls genau eine Bahn existiert. Die Operation Φ heißt treu, falls Φ' (siehe obige Bemerkung) injektiv ist.

Beispiel 1.

0. $\mathrm{SO}(\mathbb{R}) \circlearrowright \mathbb{R}^2$ durch Drehungen um $(0,0)$. Hier gibt es unendlich viele Bahnen.

   TOLLES BILD - to be inserted

1. G Gruppe, $H < G$, $X = G$. Es sei $H \circlearrowright G$ durch
   a) $h.x := hx$ (linksreguläre Operation)
   b) $h.x := xh^{-1}$ (rechtsreguläre Operation)
   c) $h.x := hxh^{-1}$ (Konjugation)

   für alle $x \in X, h \in H$ definiert, wobei sich die folgenden Eigenschaften ergeben:
   a)
   - treu (nach dem Satz von Cayley)
   - transitiv $\Leftrightarrow G = H$
   - Bahnen = Rechtsnebenklassen
   - $X^H = \emptyset \Leftrightarrow H \neq \{e\}$, sonst sind alle $x \in X$ Fixpunkte

   b) wie a), außer Links- statt Rechtsnebenklassen als Bahnen

   c)
   - Bahnen = Konjugationsklassen
   - $X^H = \{x \in X \mid \forall h \in H : h.x = x\} = \underbrace{\{x \in X \mid \forall h \in H : hxh^{-1} = x\}}_{\substack{\textit{Zentralistator} \\ \text{bzgl. Konjugation auf } H}}$
   - Spezialfall $H = G$: $X^H = Z(G)$.

2. Sei G eine Gruppe, $X = \{H < G\}$ und sei $G \circlearrowright X$ definiert durch Konjugation als

$$g.H := gHg^{-1} = \{ghg^{-1} \mid h \in H\} \in X.$$

   - Bahnen = Konjugationsklassen von Untergruppen
   - Stabilisator von $H \in X$: $G_H = \{g.H = H\}$, heißt auch *Normalisator* von H in G, schreib $N_G(H)$.
   - $X^G = \{H < G \mid \forall g \in G : g.H = H\} = \{H < G \mid \forall g \in G : gHg^{-1} = H\} = \{H \lhd G\}$

3. Sei G eine Gruppe, $H < G$, $X = G/H$. Dann $G \circlearrowright X$ durch $g.(aH) = gaH$ für alle $g \in G, a \in G$; heißt *Linkstranslation.*
   - transitiv, da $\forall a, b \in G : \exists g \in G : g(aH) = bH$.

- Im Allgemeinen nicht treu, da

$$\ker \Phi' = \underbrace{\bigcap_{x \in G} xHx^{-1}}_{\text{kleinster Normalteiler}} .$$

Lemma 5.1. *$G \circlearrowright X$. Dann*

1. *$\forall x \in X : G_x < G$*
2. *$f : G/G_x \to G.x, gG_x \mapsto g.x$ ist wohldefiniert, bijektiv und ein G-Homomorphismus (wobei G links wie in Beispiel 3 oben und rechts durch $G \circlearrowright X$ operiert).*
3. *$|G.x| = (G : G_x)$, wobei $(G : G_x) = \infty$, falls $|G/G_x| = \infty$.*

Beweis.

1. Übung
2. Es ist klar, dass f surjektiv ist. Zur Injektivität: Sei $f(g_1G_x) = f(g_2G_x)$. Das ist äquivalent zu $g_1.x = g_2.x \Leftrightarrow g_1^{-1}g_2.x = x \Leftrightarrow g_1^{-1}g_2 \in G_x \Leftrightarrow g_1G_x = g_2G_x$ für alle $g_1, g_2 \in G, x \in X$. Also ist f wohldefiniert und bijektiv.

   Nun muss noch gezeigt werden, dass f ein G-Homorphismus ist: Es gilt $f(h.(gG_x)) = h.f(gG_x)$ für alle $x \in X, h, g \in G$. Aber $f(h.(gG_x)) = hgG_x = (hg).x = h.g.x = h.f(gG_x)$
3. Es gilt nun $|G.x| \overset{2.}{=\!=} |G/G_x| = (G : G_x)$ □

Satz 5.2 (Bahnenformel)**.** *Sei G eine Gruppe, X eine endliche Menge und sei $G \circlearrowright X$ eine Gruppenoperation. Dann gilt:*

$$|X| = \sum_{i \in I} (G : G_{x_i}) = |X^G| + \sum_{\substack{i \in I, \\ x_i \notin X^G}} (G : G_{x_i}) \ ,$$

wobei $(x_i)_{i \in I}$ Elemente in X sind, sodass die Bahnen ein Repräsentantensystem der Bahnen bilden.

Beweis. Es gilt $|X| = |\bigcup_{i \in I} G.x_i| = \sum_{i \in I} |G.x_i| = \sum (G : G_{x_i})$, woraus der 1. Teil der Gleichung folgt. Teilt man nun die Bahnen $G.x_i$ in solche auf mit genau einem Element ($\Leftrightarrow x_i \in X^G$) und solchen mit ≥ 2 Elementen, so folgt $x_i \in X^G \Leftrightarrow G_{x_i} = G \Leftrightarrow (G : G_{x_i}) = 1$. Daraus folgt sofort der 2. Teil der Gleichung. □

Satz 5.3. *Sei G eine endliche Gruppe. $G \circlearrowright G$ durch Konjugation. Sei $(x_i)_{i \in I}$ so gewählt, dass die Bahnen ein Repräsentantensystem für Konjugationsklassen sind. Dann gilt:*

$$|G| = |Z(G)| + \sum_{\substack{i \in I, \\ x_i \notin Z(G)}} (G : C_G(x_i)) \ ,$$

wobei $C_G(x_i) = \{g \in G \mid gx_ig^{-1} = x_i\}$ der Zentralisator von x_i in G ist.

Beweis. Die Formel folgt direkt aus der Bahnenformel, da $C_G(x_i) = G_{x_i}$ mit der Konjugation als Operation und $x \in X^G \Leftrightarrow g.x = x\ \forall g \in G \Leftrightarrow gxg^{-1} = x\ \forall g \in G_{x_i} \Leftrightarrow x \in Z(G)$. □

[19. Oktober 2017]

[26. Oktober 2017]

6. p-Gruppen und Sylow-Sätze

Definition 6.1. Sei p prim (insbesondere ≥ 2). Eine p-Gruppe ist eine Gruppe G mit $|G| = p^r$ für ein $r \in \mathbb{N}_0$. Insbesondere ist $|G|$ endlich.

Satz 6.1. *Sei $G \neq \{e\}$ eine p-Gruppe. Dann gilt $|Z(G)| \neq |\{e\}| = 1$. Insbesondere hat G eine nicht-triviale abelsche Untergruppe.*

Beweis. Nach Satz 5.3 hat man

$$\underbrace{|G|}_{\text{durch } p \text{ teilbar}} = |Z(G)| + \underbrace{\sum_{\substack{i \in I,\\ x_i \notin Z(G)}} (G : G_{x_i})}_{A}.$$

Nach dem Satz von Lagrange ist A durch p teilbar oder gleich 1, weil G eine p-Gruppe ist. Letzters kann aber nicht sein, da $(G : G_{x_i}) = 1 \Leftrightarrow G = G_{x_i} \Leftrightarrow x_i \in Z(G)$, Widerspruch. Also sind die Summanden $(G : G_{x_i})$ und somit auch A durch p teilbar. Damit teilt p auch $|Z(G)| \Rightarrow |Z(G)| \geq 2 \Rightarrow Z(G) \neq \{e\}$. □

Satz 6.2. *Sei G eine p-Gruppe. Dann existiert eine Normalreihe der Form*

$$\{e\} = G_0 \lhd \ldots \lhd G_n = G$$

für ein $n \in \mathbb{N}$, sodass $G_i/G_{i-1} \cong \mathbb{Z}/p\mathbb{Z}$ $(1 \leq i \leq n)$. Insbesondere ist G auflösbar.

Beweis. Übungsblatt 3. □

Definition 6.2. Sei G eine endliche Gruppe, p eine Primzahl. Sei $|G| = p^r m$ mit $p \nmid m$. $H < G$ heißt p-Sylowgruppe, falls $|H| = p^r$. Wir definieren

$$\mathrm{Syl}_p(G) := \{H < G \mid H \text{ ist Sylowgruppe}\}.$$

Satz 6.3 (Sylowsätze)**.** *Sei p eine Primzahl, G eine endliche Gruppe, $|G| = p^r m$ mit $p \nmid m$.*

1. *$\forall 0 \leq k \leq r\colon \exists H < G$ mit $|H| = p^k$*
2. *Sei $U < G$ eine p-Gruppe. Dann $\exists g \in G$, sodass $U < gSg^{-1}$ für alle $S \in \mathrm{Syl}_p(G)$ gilt.*

3. *Sei* $n_p = |\operatorname{Syl}_p(G)|$. *Dann gilt*
   - $n_p \equiv 1 \pmod{p}$
   - $n_p \mid m$

Beweis.

1. Sei $1 \leq k \leq r$. Der Fall $k = 0$ ist klar mit $H = \{e\}$. Sei $X = \{A \subseteq G \mid |A| = p^k\}$, wobei $|X| = \binom{p^r m}{p^k}$. Nach Übungsblatt 3 gilt: $p^{r-k+1} \nmid |X|$.

   Nun $G \circlearrowright X$ durch $g.A := gA = \{ga \mid a \in A\}$ für alle $g \in G, A \in X$. (klar: $|gA| = p^k$, also $gA \in X$). Nachrechnen: (O1), (O2) gelten (offensichtlich).

   Nach der Bahnenformel folgt $|X| = \sum_{i \in I}(G : G_{x_i})$, wobei $\exists i \in I$, sodass $p^{r-k+1} \nmid (G : G_{x_i})$, weil $p^{r-k+1} \nmid |X|$. Wähle solch ein $x_i =: A' \in X$.

   Behauptung: Es gilt $G_{A'} < G$ mit $|G_{A'}| = p^k$. Dann würde 1) folgen mit $H = G_{A'}$. Es ist klar, dass $G_{A'} < G$ gilt. Nach dem Satz von Lagrange folgt dann: $|G| = |G_{A'}|(G : G_{A'})$, wobei p^r die linke Seite der Gleichung teilt, und im Index auf der rechten Seite p höchstens $r - k$-mal vorkommt.

   Deshalb gilt: p^k teilt $|G_{A'}|$ und somit $p^k \leq |G_{A'}|$. Sei $a \in A'$. Dann muss $G_{A'}.a = \{g.a \mid g \in G_{A'}\} \subseteq G_{A'}.A' \subseteq A'$ nach Definition von $G_{A'}$ gelten.

   Also folgert man $|G_{A'}| = |G_{A'}.a| \leq |A'| = p^k$. (nach der Definition von $G_{A'}.a$ und $A' \in X$). Somit erhält man $|G_{A'}| = p^k$, wodurch die Behauptung und somit auch die erste Aussage gezeigt ist.

2. Sei $U < G$ mit $|U| = p^s$ für ein $s \in \mathbb{N}$. Sei $S \in \operatorname{Syl}_p(G)$. Sei $U \circlearrowright G/S$ wie in Beispiel Punkt 3 auf Seite 19 durch Linksmultiplikation gegeben. Es gilt nun

$$u.(gS) = ugS \qquad \forall u \in U, g \in G$$
$$m = |G/S| = \sum_{i \in I}(U : U_{x_i})$$

   nach Definition von $S \in \operatorname{Syl}_p(G)$ und dem Satz von Lagrange. Die zweite Gleichheit folgt aus Satz 5.2.

   Weil $p \nmid m$, existiert ein $i \in I$ sodass $p \nmid (U : U_{x_i})$. Wähle ein solches $x_i =: aS$. Nach dem Satz von Lagrange ist

$$p^s = |U| = |U_{aS}|(U : U_{aS}).$$

   Also $(U : U_{aS}) = 1$. Also gilt $U = U_{aS}$. Damit folgt

$$\begin{aligned} & u.aS = aS && \forall a \in U \\ \Leftrightarrow \quad & (ua)S = aS && \forall u \in U \\ \Leftrightarrow \quad & a^{-1}uaS = S && \forall u \in U \\ \Leftrightarrow \quad & a^{-1}ua \in S && \forall u \in U \\ \Leftrightarrow \quad & u \in aSa^{-1} && \forall u \in U \end{aligned}$$

   Setze $g := a$ und erhalte $U < gSg^{-1}$.

3. Übungsblatt 3. □

Konsequenzen. Sei G eine endliche Gruppe, p eine Primzahl.

1. Je zwei p-Sylowuntergruppen in G sind zueinander konjugiert, also
$$S, S' \in \mathrm{Syl}_p(G) \Rightarrow \exists g \in G : S' = gSg^{-1}.$$

   Beweis. Nach Sylowsatz 2 folgt $\exists g \in G$ mit $S' < gSg^{-1}$. Da $|S'| = |gSg^{-1}|$ nach Definition der p-Sylowgruppe gilt, folgt $S' = gSg^{-1}$. □

   Beachte: Falls $n_p = |\mathrm{Syl}_p(G)| = 1$ gilt, also $\exists!$ p-Sylowgruppe S, dann ist $S \lhd G$. Denn $\forall g \in G$ ist gSg^{-1} wieder eine p-Sylowgruppe, also $gSg^{-1} = S$.

2. (Cauchy) Falls $p \mid |G|$ gilt, dann existiert ein $g \in G$ mit $\mathrm{ord}(g) = p$.

   Beweis. Nach Sylowsatz 1 existiert $H < G$ mit $|H| = p$. Wähle ein $g \in H$, $g \neq e$. Dann ist $\langle g \rangle < H$ und $\langle g \rangle \neq \{e\}$, also $\langle g \rangle = H$ nach dem Satz von Lagrange. Aus Abschnitt 3 folgt $\mathrm{ord}(g) = |H| = p$. □

3. Es gilt: G ist p-Gruppe $\Leftrightarrow$ Jedes Element $g \in G$ hat Ordnung p^s für ein geeignetes $s \in \mathbb{N}_0$ (abhängig von g).

   Beweis.

   „$\Rightarrow$“ Sei $g \in G$, sei $\mathrm{ord}(g) = n$. Aus Abschnitt 3 folgt $|\langle g \rangle| = n$. Daraus folgt $n \mid |G|$ nach dem Satz von Lagrange. Da G eine p-Gruppe ist, muss nun $n = p^s$ für ein $s \in \mathbb{N}_0$ gelten.

   “$\Leftarrow$“ Zu zeigen: $|G| = p^r$ für ein $r \in \mathbb{N}_0$. Angenommen $q \mid |G|$ für q Primzahl $p \neq q$. Nach dem Satz von Cauchy existiert $g \in G$ mit $\mathrm{ord}(g) = q$. Das ist ein Widerspruch. □

   Bemerkung. p-Gruppen mit unendlicher Ordnung kann man definieren als Gruppen mit $\mathrm{ord}(g) = p^r$, $r \in \mathbb{N}_0$ von p für alle $g \in G$.

Anwendungen. Vorbemerkung: Sei G eine Gruppe, $|G| = p$ prim. Dann folgt $G \cong \mathbb{Z}/p\mathbb{Z}$. (Denn wähle $g \in G$, $g \neq e$. Es gilt $\langle g \rangle < G$ und nach dem Satz von Lagrange ist $|\langle g \rangle| = p = |G|$, also ist $G = \langle g \rangle$ zyklisch und somit $G \cong \mathbb{Z}/p\mathbb{Z}$ nach Klassifikation von zyklischen Gruppen.)

Satz 6.4. *Sei G eine Gruppe, $|G| = pq$ mit $p \neq q$ Primzahl. Dann ist G auflösbar.*

Beweis. Ohne Beschränkung der Allgemeinheit sei $p > q$. Nach Sylowsatz 3 gilt: $n_p \mid q$, also $n_p \in \{1, q\}$ und $n_p \equiv 1 \pmod{p}$.

Dann gilt $n_p = 1$, weil $p > q$. Nach Punkt 1 der Konsequenzen der Sylowsätze gilt $\exists!$ p-Sylowgruppe S und $S \lhd G$. Nach der Definition von p-Sylowgruppe und weil $|G| = pq$ ist, gilt $|S| = p$. Also erhalten wir eine Normalreihe
$$\{e\} \lhd S \lhd G$$
mit $S/\{e\} \cong S \cong \mathbb{Z}/p\mathbb{Z}$ und $|G/S| = q$, also $G/S \cong \mathbb{Z}/q\mathbb{Z}$.

Die Faktoren sind folglich abelsch und somit ist G auflösbar. □

Satz 6.5. *Sei G eine Gruppe, $|G| = pq$ mit p, q prim sowie $p < q$ und $p \nmid q - 1$. Dann folgt $G \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$.*

Beweis. Nach Sylowsatz 3 gilt $n_p \in \{1, q\}, n_q \in \{1, p\}$ und $n_p \equiv 1 \pmod{p}$, $n_q \equiv 1 \pmod{q}$. Da $p < q$ ist, gilt $n_q = 1$. Also existiert genau eine q-Sylowgruppe $Q \lhd G$. Falls $n_p = q$ dann gilt $q \equiv 1 \pmod{p}$. Daraus folgt $p \mid (q - 1)$, was im Widerspruch zur Voraussetzung steht. Also ist $n_p = 1$, womit genau eine p-Sylowgruppe mit $P \lhd G$ existiert.

Behauptung: Sei $x \in P, y \in Q$. Dann gilt $xy = yx$. $xyx^{-1}y^{-1}$ liegt in Q, da $xyx^{-1} \in Q$, weil Q ein Normalteiler ist und $y^{-1} \in Q$ per Definition. Analog gilt $xyx^{-1}y^{-1} \in P$, da $x \in P$ und $yx^{-1}y^{-1} \in P$. Somit liegt $xyx^{-1}y^{-1}$ in $P \cap Q$. Aber es gilt $P \cap Q = \{e\}$, da $|P \cap Q| \mid p = |P|$ und $|P \cap Q| \mid q = |Q|$. Somit folgt die Behauptung.

Betrachte nun

$$\begin{aligned} \Phi \colon P \times Q &\longrightarrow G \\ (x, y) &\longmapsto xy \end{aligned}$$

Φ ist ein wohldefinierter Gruppenhomomorphismus, denn

$$\begin{aligned} \Phi((x, y) \circ (x', y')) = \Phi((xx', yy')) = xx'yy' \\ \Phi((x, y)) \circ \Phi((x', y')) = xyx'y' = xx'yy' \text{ (nach Behauptung)} \end{aligned}$$

Außerdem ist Φ injektiv, denn $\Phi((x, y)) = e \Leftrightarrow xy = e \Leftrightarrow x = y^{-1} = e$, weil $P \cap Q = \{e\}$. Φ ist surjektiv, weil $|P \times Q| = |P| \cdot |Q| = pq = |G|$. Somit liefert Φ einen Gruppenisomorphismus $P \times Q \cong G$, also $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \cong G$. □

Korollar 6.6. *Sei G eine Gruppe, $|G| = 15$. Dann gilt $G \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \cong \mathbb{Z}/15\mathbb{Z}$ und G ist zyklisch.*

Beweis. Wir wissen $G \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$. Behauptung: $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \cong \mathbb{Z}/15\mathbb{Z}$. Sei nämlich $g = (\overline{1}, \overline{1}) \in \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$. Dann gilt:

$$\operatorname{ord}(g) = \min\{j \mid (\overline{1}, \overline{1}) + \cdots + (\overline{1}, \overline{1}) = (\overline{0}, \overline{0}) \in \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}\} = 15$$

Folglich gilt $|\langle g \rangle| = 15$ und damit ist $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ zyklisch. Der Isomorphismus ist durch

$$\begin{aligned} \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} &\longrightarrow \mathbb{Z}/15\mathbb{Z} \\ g = (\overline{1}, \overline{1}) &\longmapsto \overline{1} \end{aligned}$$

gegeben. □

[26. Oktober 2017]

[30. Oktober 2017]

II. Ringe

7. Allgemeines

Definition 7.1. Ein Ring (mit 1) ist eine Menge R zusammen mit zwei Abbildungen

$$\begin{aligned} +, \cdot \colon R \times R &\longrightarrow R \\ (a,b) &\longmapsto a+b \qquad \text{Addition} \\ \text{bzw. } (a,b) &\longmapsto a \cdot b \qquad \text{Multiplikation,} \end{aligned}$$

sodass gilt:

(R1) $(R,+)$ ist eine abelsche Gruppe.

(R2) $\forall a,b,c \in R$ gilt $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ (also $\cdot$ ist assoziativ)

(R3) $\forall a,b,c \in R$ gilt:

$$\begin{aligned} a \cdot (b+c) &= (a \cdot b) + (a \cdot c) \\ (b+c) \cdot a &= (b \cdot a) + (c \cdot a) \end{aligned} \qquad \text{(Distributivität)}$$

(R4) $\exists 1 = 1_R \in R$, sodass $a \cdot 1 = a = 1 \cdot a$ für alle $a \in R$ (Neutrales bezüglich $\cdot$)

Bemerkung.

1. Wir bezeichnen mit 0 oder 0_R das neutrale Element und mit $(-a)$ das Inverse zu $a \in R$ bezüglich $+$.
2. Das Element $1 \in R$ ist eindeutig (denn sei $1'$ ein anderes, dann ist $1 = 1 \cdot 1' = 1'$).
3. In einem Ring gilt: $a \cdot 0 = 0 = 0 \cdot a$ für alle $a \in R$, denn $a \cdot 0 = a \cdot (0 + 0 = (a \cdot 0) + (a \cdot 0) \Rightarrow 0 = a \cdot 0$; analog für $0 \cdot a$.

Definition 7.2. Ein Ring $(R,+,\cdot)$ heißt kommutativ, falls $a \cdot b = b \cdot a$ für alle $a,b \in R$

Beispiel 1.

1. Jeder Körper $(K,+,\cdot)$ ist ein kommutativer Ring (aber Ringe haben im Allgemeinen keine multiplikativ Inversen).
2. (aus LA) Sei V ein K-Vektorraum, K ein Körper, dann ist $(\mathrm{End}_K(V),+,\cdot)$ ein Ring mit $(f+g)(v) = f(v)+g(v)$ und $(f \cdot g)(v) = (f \circ g)(v)$ (Hintereinanderausführung) mit $f,g \in \mathrm{End}_K(V), v \in V$ mit $0_{\mathrm{End}_K(V)} =$ Nullabbildung; $1_{\mathrm{End}_K(V)} = \mathrm{id}_V$.
3. Nullring: $R = \{0 = 1\}$ mit $0+0=0$ und $0 \cdot 0 = 0$.
4. Es gilt folgende Umkehrung von 1.: wenn $(R,+,\cdot)$ ein kommutativer Ring ist, $R \neq \{0\}$, jedes $x \in R$ mit $x \neq 0$ besitzt Inverses x^{-1} bezüglich $\cdot$; dann ist $(R,+,\cdot)$ Körper

5. $(R, +, \cdot)$ Ring. Betrachte

$$R[t] = \left\{ \sum_{i=0}^{\infty} a_i t^i \,\middle|\, a_i \in R, \text{ nur endlich viele } a_i \neq 0 \right\} = \left\{ \sum_{i=0}^{n} a_i t^i \,\middle|\, a_i \in R, n \in \mathbb{N}_0 \right\},$$

die Polynome mit Koeffizienten in R. Dann ist $(R[t], +, \cdot)$ ein Ring mit $0_{R[t]} =$ Nullpolynom, d.h. $a_i = 0$ für alle i. $1_{R[t]}$ ist das Polynom $p(t) = \sum_{i=0}^{\infty} a_i t^i$ mit $a_0 = 1$ und $a_i = 0$ für $i \geq 1$. Es gilt: $(R[t], +, \cdot)$ ist kommutativ $\Leftrightarrow$ $(R, +, \cdot)$ ist kommutativ.

Definition 7.3. Sei $(R, +, \cdot)$ ein Ring. $R' \subseteq R$ heißt Unterring, falls

(UR1) $1_R \in R'$

(UR2) $\forall a, b \in R' : a + (-b) \in R', a \cdot b \in R'$

Beispiel 2. Sei $(R, +, \cdot)$ ein Ring. $Z(R) \coloneqq \{a \in R | a \cdot x = x \cdot a \ \forall x \in R\}$ ist das Zentrum des Ringes; dieses ist ein Unterring. Warnung: $Z(R) \neq Z((R, +))$ im Allgemeinen.

Definition 7.4. Seien $(R, +, \cdot)$ und $(S, +, \cdot)$ Ringe. Eine Abbildung $\varphi \colon R \to S$ ist Ringhomomorphismus, falls gilt:

(RH1) $\varphi(a + b) = \varphi(a) + \varphi(b)$

(RH2) $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$

(RH3) $\varphi(1_R) = \varphi(1_S)$

für alle $a, b \in R$.

Falls φ zusätzlich bijektiv ist, ist φ ein Ringisomorphismus.

Bemerkung. Sei $\varphi \colon R \to S$ ein Ringhomomorphismus. Dann ist $R \to S$ ein Gruppenhomomorphismus von $(R, +)$ nach $(S, +)$ wegen (RH1).

Lemma 7.1.

1. *Ist $\varphi \colon R \to S$ ein Ringisomorphismus, dann ist auch $\varphi^{-1} \colon S \to R$ ein Ringisomorphismus*
2. *Seien $\varphi_1 \colon R \to S, \varphi_2 \colon S \to T$ Ringhomomorphismen. Dann ist auch $\varphi_2 \circ \varphi_1 \colon R \to T$ ein Ringhomomorphismus*

Beweis. Nachrechnen. □

Lemma 7.2. *Sei $\varphi \colon R \to S$ Ringhomomorphismus. Dann ist $\operatorname{im} \varphi \subseteq S$ ein Unterring.*

Beweis. Es gilt $\varphi(1_R) = 1_S \in \operatorname{im} \varphi \Rightarrow$ (UR1).

Seien $s_1, s_2 \in \operatorname{im} \varphi$.

$$\begin{aligned} &\Rightarrow \exists r_1, r_2 \in R : \varphi(r_1) = s_1, \varphi(r_2) = s_2 \\ &\Rightarrow s_1 \cdot s_2 = \varphi(r_1) \cdot \varphi(r_2) = \varphi(r_1 \cdot r_2) \in \operatorname{im} \varphi \\ &\Rightarrow s_1 \cdot s_2 \in \operatorname{im} \varphi \end{aligned}$$

Außerdem gilt:

$$s_1 + (-s_2) = \varphi(r_1) + (-\varphi(r_2)) = \varphi(r_1) + \varphi(-r_2) = \varphi(r_1 + (-r_2)) \in \operatorname{im}\varphi$$

Somit gilt (UR2) und es sind alle Unterringaxiome erfüllt. □

Warnung: Wir setzen für $\varphi\colon R \to S$ als Ringhomomorphismus

$$\ker\varphi := \{r \in R \mid \varphi(r) = 0_S\}.$$

Dann ist $\ker\varphi \subseteq R$ genau dann ein Unterring, falls S der Nullring ist. Denn:
„⇒“: Sei $\ker\varphi$ ein Unterring. Dann gilt per Definition $1_R \in \ker\varphi$. Somit muss auch $0_S = \varphi(1_R) = 1_S$ gelten. Deshalb gilt für alle $s \in S$, dass $s = s \cdot 1_S = s \cdot 0_S = 0_S$.
„⇐“: Sei $S = \{0\}$. Dann ist $\ker\varphi$ bereits ganz R und dies ist offensichtlich ein Unterring.

Definition 7.5. Sei $(R, +, \cdot)$ ein Ring. $I \subseteq R$ heißt Ideal, falls gilt:

(I1) $I < (R, +)$

(I2) a) $a \cdot x \in I$ für alle $x \in I, a \in R$
b) $x \cdot a \in I$ für alle $x \in I, a \in R$

Falls nur (I1), (I2a) erfüllt sind, heißt I Linksideal; falls nur (I1) und (I2b) erfüllt sind, heißt I Rechtsideal.

Beispiel 3.

1. $(\mathbb{Z}, +, \cdot)$ ist Ring. Sei nun $n \in \mathbb{Z}$, dann ist $I = n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\} \subseteq \mathbb{Z}$ ein Ideal, denn: $n\mathbb{Z} < (\mathbb{Z}, +)$, also folgt (I1); und für $a \in \mathbb{Z}$ und $x = nk \in n\mathbb{Z}$ gilt: $ax = ank = nak \in I$; $xa = nka = nak \in I$ und damit folgt (I2).

2. $(R, +, \cdot)$ Ring; $(R[t], +, \cdot)$ wie in Beispiel oben;

$$I = \left\{ p(t) \in R[t] \,\middle|\, p(t) = \sum_{i=0}^{\infty} a_i t^i \wedge a_0 = 0 \right\}$$

enthält die Polynome ohne konstanten Term. Dann ist $I \subseteq R[t]$ ein Ideal (nachprüfen).

Lemma 7.3. *Sei $\varphi\colon R \to S$ ein Ringhomomorphismus. Dann ist $\ker\varphi \subseteq R$ ein Ideal.*

Beweis. Es gilt $\ker\varphi < (R, +)$ nach Satz 1.3, womit (I1) erfüllt ist. Sei nun $a \in R, x \in \ker\varphi$. Dann gilt $\varphi(ax) = \varphi(a)\varphi(x) = \varphi(a) \cdot 0_S = 0_S$ und somit liegt ax im Kern. Das funktioniert analog auch für xa, womit auch (I2) erfüllt ist. □

Beispiel 4. Sei $(R[t], +, \cdot)$ wie in Beispiel 3. Sei $a \in R$.

$$\begin{aligned} \mathrm{ev}_a \colon R[t] &\longrightarrow R \\ p(t) = \sum_{i=0}^{\infty} b_i t^i &\longmapsto p(a) = \sum_{i=0}^{\infty} b_i a^i \\ (b_i \in R;\ \text{fast alle } b_i = 0) &\qquad \left(\text{mit } a^i = \prod_{k=1}^{i} a\right) \end{aligned}$$

heißt Auswertungs- oder Evaluationsabbildung. Nachrechnen ergibt, dass ev_a ein Ringhomomorphismus ist.

Es gilt $\ker(\mathrm{ev}_a) = \{p(t) \in R[t] \mid p(a) = 0_R\}$. Das sind genau die Polynome, die a als Nullstelle haben. Wir wissen, dass $\ker(\mathrm{ev}_a) \subseteq R[t]$ ein Ideal ist nach Lemma 7.3.

Spezialfall: Sei $a = 0_R$. Dann gilt $\ker \mathrm{ev}_0 = I$ wie in Beispiel 3 Teil 2). Insbesondere ist I ein Ideal.

Bemerkung. Seien nun ein Ring $(R, +, \cdot)$ und ein Ideal $I \subseteq R$ gegeben. Insbesondere, nach $(I1)$, ist $I < (R, +)$ und sogar $I \lhd (R, +)$, weil $(R, +)$ abelsch ist. Somit ist R/I wieder eine Gruppe mit den Nebenklassen in $(R, +)$ bezüglich I als Elemente. Nebenklassen sind von der Form $\overline{a} = \{a + x \mid x \in I\}$, $a \in R$ und die Gruppenoperation auf R/I ist $\overline{a} \circ \overline{b} = \overline{a + b}$.

Satz 7.4. *Seien R, I wie in der Bemerkung gegeben. Dann wird $(R/I, \circ)$ zu einem Ring $(R/I, \circ, \odot)$, wobei die Multiplikation gegeben ist durch $\overline{a} \odot \overline{b} = \overline{a \cdot b}$. Letzteres ist dabei die Multiplikation in R.*

Beweis.

(R1) $(R/I, +)$ ist eine abelsche Gruppe (nach Abschnitt 1).

(R2) Seien $\overline{a}, \overline{b}, \overline{c} \in R/I$. $(\overline{a} \odot \overline{b}) \odot \overline{c} = (\overline{ab}) \odot \overline{c} = \overline{(ab)c} = \overline{a(bc)} = \overline{a} \odot \overline{bc} = \overline{a} \odot (\overline{b} \odot \overline{c})$.

(R3) Seien $\overline{a}, \overline{b}, \overline{c} \in R/I$. Dann $\overline{a} \odot (\overline{b} \circ \overline{c}) = \overline{a} \odot \overline{b + c} = \overline{a \cdot (b + c)} = \overline{ab + ac} = \overline{ab} \circ \overline{ac} = \overline{a} \odot \overline{b} \circ \overline{a} \odot \overline{c}$. Analog für den zweiten Teil von (R3).

(R4) Sei $\overline{a} \in R/I$. Dann gilt $\overline{a} \odot \overline{1_R} = \overline{a 1_R} = \overline{a} = \overline{1_R \cdot a} = \overline{1_R} \odot \overline{a}$. Somit ist $\overline{1_R}$ das neutrale Element für $\odot$.

Nun ist noch die Wohldefiniertheit von $\odot$ zu prüfen. Also ist zu zeigen: für $\overline{a} = \overline{a'}$ und $\overline{b} = \overline{b'}$ folgt $\overline{a} \odot \overline{b} = \overline{a'} \odot \overline{b'}$ mit $\overline{a}, \overline{b}, \overline{a'}, \overline{b'} \in R/I$. Sei also $\overline{a} = \overline{a'}$ und $\overline{b} = \overline{b'}$. Dann existieren $x, y \in I$ mit $a + (-a') = x$ und $b + (-b') = y$ nach (I1). Es gilt

$$a \cdot b = (a' + x) \cdot (b' + y) = (a'b') + (a'y) + (xb') + (xy)$$

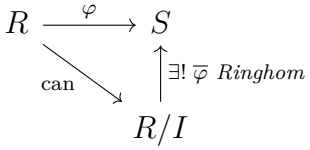
wobei $(a'y) + (xb') + (xy) \in I$, weil I ein Ideal ist. Somit liegt auch $(ab) + (-a'b')$ in I und es folgt $\overline{ab} = \overline{a'b'}$. □

[30. Oktober 2017]
[2. November 2017]

Wir wissen: Sei $(R, +, \cdot)$ ein Ring, $I \subseteq R$ ein Ideal. Dann ist $(R/I, +, \odot)$ ein Ring mit $\overline{a} \odot \overline{b} = \overline{ab}$. Wir nennen $(R/I, +, \odot)$ den Quotientenring von R nach/modulo I. Im Folgenden schreiben wir kurz R statt $(R, +, \cdot)$ etc.

Satz 7.5 (Homomorphiesatz)**.** *Sei R ein Ring, $I \subseteq R$ ein Ideal.*

1. *Die Abbildung* $\mathrm{can}\colon R \to R/I, a \mapsto \overline{a}$ *ist Ringhomomorphismus.*
2. *Sei $\varphi\colon R \to S$ Ringhomomorphismus mit $I \subseteq \ker \varphi$, dann $\exists!\, \overline{\varphi}\colon R/I \to S$ Ringhomomorphismus, sodass $\overline{\varphi} \circ \mathrm{can} = \varphi$. Also:*



Beweis. Übungsblatt 3. □

Definition 7.6. Sei R ein kommutativer Ring und $I, J \subseteq R$ Ideale. Dann ist

- $I + J = \{x + y \mid x \in I, y \in J\} \subseteq R$ die Summe von I und J
- $I \cap J = \{x \mid x \in I, x \in J\} \subseteq R$ der Schnitt von I und J
- $I \cdot J = \{\sum_{i=1}^{n} a_i b_i \mid a_i \in I, b_i \in J, n \in \mathbb{N}\}$ das Produkt von I und J

Das sind alles Ideale in R (nachprüfen!).

Definition 7.7. Sei R ein kommutativer Ring, $a, b \in R$.

1. $(a) = \{ra \mid r \in R\}$ ist das von a erzeugte Ideal.
2. b teilt a (in R), falls $\exists r \in R : a = br = rb$
3. a ist Nullteiler, wenn $\exists r \in R, r \neq 0$ mit $ra = ar = 0$. R ist nullteilerfrei, falls 0 der einzige Nullteiler ist. R heißt Integritätsbereich, falls R nullteilerfrei und $R \neq \{0\}$ ist.
4. a heißt Einheit, falls $\exists r \in R$ mit $ar = 1 = ra$ (also a ein multiplikatives Inverses hat). $R^\times = \{c \in R \mid c \text{ Einheit in } R\}$ ist die Einheitengruppe von R.

Bemerkung. (a) ist in der Tat ein Ideal:

(I2) Sei $r' \in R, x = ra \in (a)$. Dann gilt $r'x = r'(ra) = (r'r)a \in (a)$. Genauso für $xr' \in (a)$.

(I1) Seien $x, y \in I$. Dann lassen sich x und y in der Form $x = r'a, y = ra$ schreiben. Folglich gilt $x + (-y) = (r'a) + (-ra) = (r' + (-r))a \in (a)$. Wir benutzen dabei $-(ra) = (-r)a$, weil $(ra) + ((-r)a) = (r + (-r))a = 0a = 0$ gilt.

Bemerkung. $R^\times$ ist eine Gruppe bezüglich $\cdot$ (Übung).

Definition 7.8. Ein Ideal der Form (a) wie oben heißt Hauptideal. Ein kommutativer Ring $R \neq \{0\}$ heißt Hauptidealring, wenn R nullteilerfrei und jedes Ideal in R ein Hauptideal ist (also von der Form (a) ist): $\forall I \subseteq R$ Ideal $\exists a \in R : I = (a)$

Beispiel 5. Wir betrachten $(\mathbb{Z}, +, \cdot)$. Behauptung: Das ist ein Hauptidealring.

- Es ist klar, dass $\mathbb{Z} \neq \{0\}$ und dass $\mathbb{Z}$ nullteilerfrei ist.
- Sei $I \subseteq \mathbb{Z}$ ein Ideal. Falls $I = \{0\}$, dann muss $I = (0)$ gelten. Es sei also $I \neq \{0\}$. Dann $\exists x \in I, x \neq 0$. Wähle $n \in \mathbb{N}$ minimal mit $n \in I$. Denn wenn $x \in I$, so liegt nach (I1) auch das Inverse bezüglich der Addition $-x$ in I.

  Wir behaupten nun, dass (n) bereits I ist.

  „$\supseteq$“: Das gilt nach (I2)

  „$\subseteq$“: Sei $y \in I$. Wir schreiben $y = bn + r$ mit $b, r \in \mathbb{Z}$ mit $0 \leq r < n$. Somit gilt $y + (-bn) = r$ und damit würde r in I liegen. Das ist ein Widerspruch zur Minimalität von n außer $r = 0$. Deshalb gilt $y = bn$ und folglich liegt y in (n).

Beispiel 6. $(1) = R$, $(0) = \{0\}$ sind Hauptideale.

Lemma 7.6. *Sei R ein kommutativer Ring, $R \neq \{0\}$.*

1. *R ist genau dann ein Körper, wenn $R^\times = R \setminus \{0\}$*
2. *Für $a, b, c \in R$ gilt*
   a) *$(a) \subseteq (b) \Leftrightarrow b$ teilt a*
   b) *$(a) = R \Leftrightarrow a \in R^\times \Leftrightarrow (a) = (1)$*
   c) *Falls c nicht Nullteiler: $ac = bc \Rightarrow a = b$*
   d) *a Nullteiler $\Rightarrow a \notin R^\times$*

Beweis.

1. Sei R Körper, dann gilt: Für alle $x \in R$, wobei $x \neq 0$, existiert ein x^{-1} mit $xx^{-1} = 1 = x^{-1}x$. Somit liegt x in $R^\times$ und es gilt $R \setminus \{0\} \subseteq R^\times$.

   Angenommen $R^\times = R \setminus \{0\}$. Sei $x \in R$, $x \neq 0$. Dann gilt $x \in R^\times$ und somit existiert ein $r \in R$ mit $xr = 1 = rx$. Folglich ist $r = x^{-1}$ und damit das Inverses zu x. Also ist R ein Körper.

2. a) „$\Rightarrow$“: Sei $(a) \subseteq (b)$. Dann liegt a in (b) und es existiert ein $r \in R$ mit $a = rb$. Folglich gilt b teilt a.

„⇐“: Angenommen b teilt a. Dann existiert ein $r \in R$, sodass $a = rb$. Folglich gilt $r'a = r'(rb) = (r'r)b \in (b)$ $\forall r' \in R$. Somit gilt $(a) \subseteq (b)$.

b) Sei $(a) = R \Rightarrow 1 \in (a) \Rightarrow \exists r \in R : 1 = ra = ar \Rightarrow a \in R^\times$.

Sei $a \in R^\times \Rightarrow \exists r \in R : ra = 1 = ar \Rightarrow 1 \in (a) \Rightarrow r' \cdot 1 = r' \in (a) \forall r' \in R \Rightarrow (a) = R$.

Sei $a \in R^\times \Rightarrow 1 \in (a) \Rightarrow R = (1) \subseteq (a) \Rightarrow (1) = (a)$.

Sei $(1) = (a) \Rightarrow 1 \in (a) \Rightarrow \exists r \in R : ra = 1 = ar \Rightarrow a \in R^\times$.

c)

$$\begin{aligned} & ac = bc \\ \Rightarrow & (a + (-b))c = 0 \\ \Rightarrow & a + (-b) = 0 \\ \Rightarrow & a = b \end{aligned}$$

d) Sei a Nullteiler. Dann existiert ein $r \neq 0$ mit $ra = 0$. Sei nun $a \in R^\times$, dann $\exists b$ mit $ab = 1$. Somit gilt $r = r \cdot 1 = rab = 0 \cdot b = 0$. Somit wäre $r = 0$, was ein Widerspruch ist. □

Beispiel 7. Sei $R = \mathbb{R}[t]$, $I = (t^2)$. Wir behaupten: R/I ist kein Körper. Denn es gilt $\bar{t} \neq \bar{0}$, da $t \notin I$. Andererseits gilt $\overline{t^2} = \bar{0}$, weil $t^2 \in I$. Somit gilt auch $\bar{0} = \overline{t^2} = \bar{t} \odot \bar{t}$, weshalb $\bar{t}$ ein Nullteiler in R/I ist. Insbesondere ist $\bar{t}$ nach Lemma 7.6 keine Einheit. Folglich gilt $(R/I)^\times \neq (R/I) \setminus \{0\}$ und R/I kann kein Körper sein.

Beispiel 8. Sei $R = \mathbb{R}[t], I = (t^2 + 1)$. Dann ist R/I ein Körper.

Beweis. Es ist klar, dass R/I kommutativ ist, weil R kommutativ ist. Sei $x \in R/I, x \neq 0$. Es ist zu zeigen, dass $x \in (R/I)^\times$. In R/I gilt $\overline{t^2 + 1} = \bar{0}$, weil $t^2 + 1$ in I liegt und damit für $j \in \mathbb{Z}_{\geq 2}$ folgendes gilt:

$$\begin{aligned} \overline{t^j} &= \overline{t^{j-2}(t^2+1) + (-t^{j-2})} = \overline{t^{j-2}(t^2+1)}\,\overline{-t^{j-2}} \\ &= \overline{t^{j-2}} \odot \overline{t^2+1} + \overline{-t^{j-2}} = \overline{-t^{j-2}} = -(\overline{t^{j-2}}) \end{aligned}$$

Für $p = \sum_{i=0}^{\infty} a_i t^i \in \mathbb{R}[t]$ gilt: $\bar{p} = \overline{b_0 1 + b_1 t}$ für gewisse $b_0, b_1 \in R$. Also sei o.B.d.A. $x = \overline{b_0 1 + b_1 t}$ mit $b_0^2 + b_1^2 \neq 0$. Sei $q := \frac{1}{b_0^2 b_1^2}(b_0 1 - b_1 t) \in \mathbb{R}[t]$. Das ist wohldefiniert, da $b_0^2 + b_1^2 \neq 0$.

Sei $y := \bar{q}$. Wir behaupten nun, dass $y = x^{-1}$ in R/I liegt. Es gilt:

$$(b_0 1 + b_1 t)q = \frac{1}{b_0^2 + b_1^2}(b_0^2 + b_0 b_1 t - b_1 b_0 t - b_1^2 t^2) = \frac{1}{b_0^2 + b_1^2}(b_0^2 - b_1^2 t^2)$$

Da $\overline{t^2 + 1} = \bar{0}$ und somit $\overline{-t^2} = \bar{1}$, gilt

$$xy = \overline{\frac{1}{b_0^2 + b_1^2}(b_0^2 + b_1^2)} = \bar{1}$$

Also ist $x \in (R/I)^\times$ mit dem Inversen y.
Übung: R/I ist isomorph zu $\mathbb{C}$ (als Körper). □

Definition 7.9. Sei R ein kommutativer Ring, $R \neq \{0\}$. Ein Ideal $I \subsetneq R$ heißt maximal, falls $I \neq R$ und $\nexists J \subsetneq R$ Ideal mit $I \subsetneq J \subsetneq R$ (echte Teilmengen).

Lemma 7.7. *Sei R kommutativer Ring, $R \neq \{0\}$. Dann ist R genau dann ein Körper, wenn $\{0\}$ das einzige (maximale) Ideal ist.*

Beweis.

„⇐“: Sei $\{0\}$ ein maximales Ideal. Dann ist es auch schon das einzige maximale Ideal, denn falls $I \neq \{0\}$ ein maximales Ideal ist, so folgt $\{0\} \subset I \neq R$. Daraus folgt $\{0\} = I$, was im Widerspruch zur Annahme steht.

Sei $a \in R, a \neq 0$. Dann gilt $(0) \subset (a)$ und folglich $(a) = R$. Nach Lemma 7.6 ist dann $R^\times = R \setminus \{0\}$ und somit ist R ein Körper.

„⇒“: Sei R ein Körper, $I \subseteq R$ Ideal, $I \neq \{0\}$. Dann existiert ein a in I mit $a \neq 0$. Weil R ein Körper ist, ist $a \in R^\times$. Daraus folgt $(a) = R$ und somit $I = R$. Somit ist $\{0\}$ das einzige Ideal und somit maximal. □

Beispiel 9. Betrachte $R = \mathbb{Z}$ sowie ein Ideal $I \subseteq \mathbb{Z}$. Dann ist I genau dann maximal, wenn $I = (p)$, wobei p prim ist.

Beweis.

„⇒“: Sei $I = (a)$ maximal. Jedes Ideal in $\mathbb{Z}$ kann so geschrieben werden, da $\mathbb{Z}$ ein Hauptidealring ist. Falls $a \neq \pm p$ mit p prim, so existiert $b \in \mathbb{Z}$ mit $b \mid a$ und $b \neq \pm a$, $b \neq \pm 1$. Dann gilt $(a) \subsetneq (b) \subsetneq R$ ($(b) \neq R$, weil $b \neq \pm 1$, also $b \notin \mathbb{Z}^\times$), was im Widerspruch zu I maximal steht, also ist $a = \pm p$ mit p prim.

„⇐“: Sei $I = (a)$ mit $a = \pm p$, p prim. Sei J ein Ideal in R sowie $I \subsetneq J \subsetneq R$. Dann gilt $J = (b)$ für ein $b \in \mathbb{Z}$, da $\mathbb{Z}$ ein Hauptidealring ist, und nach Lemma 7.6 folgt $b \mid a$, $b \neq \pm a$ (weil $I \subsetneq J$) und $b \neq \pm 1$ (weil $(b) \neq R$). Das ist ein Widerspruch zu $a = \pm p$. □

Satz 7.8. *Sei R ein kommutativer Ring, $R \neq \{0\}$, $I \subseteq R$ Ideal. R/I ist genau dann ein Körper, wenn I ein maximales Ideal ist.*

Als Vorbereitung:

Satz 7.9. *Sei $\varphi\colon R \to S$ ein surjektiver Ringhomomorphismus. Dann gibt es eine Bijektion zwischen den Mengen*

$$\left\{ \begin{smallmatrix} \text{Ideale in } R \\ \text{mit } \ker\varphi \subseteq I \end{smallmatrix} \right\} \longleftrightarrow \{\text{Ideale in } S\}$$

durch

$$\begin{array}{rcl} I & \longmapsto & \varphi(I) \\ \underbrace{\varphi^{-1}(J)}_{\{r \in R \mid \varphi(r) \in J\}} & \longmapsto & J \end{array}$$

Beweis. Behauptung: $\varphi(I) \subseteq S$ ist ein Ideal.

(I1) Das ist klar, weil Bilder von Gruppen unter Gruppenhomomorphismen wieder Gruppen sind.

(I2) Es ist zu zeigen: Falls $x \in \varphi(I), r \in S$ dann gilt $rx \in \varphi(I), xr \in \varphi(I)$. Weil φ surjektiv ist, existiert ein $r' \in R$ mit $\varphi(r') = r$. Nach Annahme existiert ein $y \in I$ mit $\varphi(y) = x$. Dann gilt $\varphi(r'y) = \varphi(r')\varphi(y) = rx \in \varphi(I)$, weil I ein Ideal ist. Genauso gilt $\varphi(yr') = xr \in \varphi(I)$. Somit ist $\varphi(I)$ ein Ideal.

Behauptung: $\varphi^{-1}(J) \subseteq R$ ist ein Ideal mit $\ker\varphi \subseteq \varphi^{-1}(J)$.

(I1) Sei $\varphi^{-1}(J) \subseteq R$ ein Ideal. Dann gilt $\ker\varphi \subseteq \varphi^{-1}(J)$, weil $\ker\varphi = \varphi^{-1}(\{0\})$ und $0 \in J$ für jedes Ideal J. Es ist klar, dass $\varphi^{-1}(J)$ eine Untergruppe von R ist, da φ ein Gruppenhomomorphismus ist.

(I2) Sei $r \in R, x \in \varphi^{-1}(J)$; es ist zu zeigen, dass $rx, xr \in \varphi^{-1}(J)$. Es gilt $\varphi(rx) = \varphi(r)\varphi(x) \in J$. Genauso gilt $\varphi(xr) \in J$. Also liegen rx und xr in $\varphi^{-1}(J)$, womit die Behauptung gezeigt ist.

[2. November 2017]

[6. November 2017]

Sei nun $I \subseteq R$ ein Ideal mit $I \supseteq \ker\varphi$ und $J \subseteq S$ ein Ideal. Es bleibt zu zeigen:

$\varphi^{-1}(\varphi(I)) = I$:

„$\supseteq$“ $x \in I \Rightarrow \varphi(x) \in \varphi(I) \Rightarrow x \in \varphi^{-1}(\varphi(I))$

„$\subseteq$“

$$\begin{aligned} & x \in \varphi^{-1}(\varphi(I)) \\ \Rightarrow & \varphi(x) \in \varphi(I) \\ \Rightarrow & \exists y \in I \text{ mit } \varphi(x) = \varphi(y) \\ \Rightarrow & \varphi(x + (-y)) = 0 \\ \Rightarrow & x \in I, \text{ da } y \in I \end{aligned}$$

$\varphi(\varphi^{-1}(J)) = I$:

„⊇“

$$\begin{aligned} & x \in J \\ \Rightarrow & \exists y \in R \text{ mit } \varphi(y) = x \\ \Rightarrow & y \in \varphi^{-1}(J) \text{ und } \varphi(y) = x \\ \Rightarrow & x \in \varphi(\varphi^{-1}(J)) \end{aligned}$$

„⊆“ $x \in \varphi(\varphi^{-1}(J)) \Rightarrow \exists y \in \varphi^{-1}(J) \colon \varphi(y) = x \Rightarrow x \in J$ □

Bemerkung. Beachte: Die Bijektion von Satz 7.9 ist inklusionserhaltend, also

$$\underbrace{I \subseteq I'}_{\substack{\text{Ideale in } R, \\ \text{die } \ker\varphi \text{ enthalten}}} \iff \varphi(I) \subseteq \varphi(I').$$

Beweis von Satz 7.8. Setze $\varphi := \text{can} \colon R \to R/I$ (surjektiv mit $\ker\varphi = I$).

„⇐“ Sei R/I ein Körper. Nach Lemma 7.7 ist $\{0\} \subseteq R/I$ ein maximales Ideal. Dann gilt nach Satz 7.9, dass $\varphi^{-1}(\{0\}) = I$ und $\varphi^{-1}(R/I) = R$ die einzigen Ideale sind, die I enthalten. Somit ist I ein maximales Ideal.

„⇒“ Sei I ein maximales Ideal in R. Dann gibt es genau I und R als Ideale, die I enthalten. Nach Satz 7.9 sind $\{0\} = \varphi(I)$ und $R/I = \varphi(R)$ alle Ideale von R/I. Aus Lemma 7.7 folgt dann, dass R/I ein Körper ist. □

Definition 7.10. Sei R ein kommutativer Ring, $I \subseteq R$ ein Ideal. Dann heißt I Primideal, falls $I \neq R$ und $\forall x, y \in R$ gilt, dass falls xy in I liegt, x oder y das auch tut, also:

$$xy \in I \quad \Longrightarrow \quad x \in I \text{ oder } y \in I.$$

Bemerkung. Falls R ein Integritätsbereich ist, dann ist $\{0\}$ ein Primideal.

Beispiel 10. Sei $R = \mathbb{Z}, a \in \mathbb{Z}$. Dann ist (a) genau dann ein Primideal, wenn a oder $-a$ prim ist, oder $a = 0$.

Beweis.

„⇐“ Sei $a = \pm p$, p prim. Seien $x, y \in R$ mit $xy \in (a)$.

$\Rightarrow p$ teilt xy

$\Rightarrow p$ teilt x oder p teilt y

$\Rightarrow x \in (p) = (a)$ oder $y \in (p) = (a)$

$\Rightarrow (a)$ ist ein Primideal

„⇒“ Sei $(a) \neq (0)$ ein Primideal. Falls $a = \pm 1$, also $(a) = R$, so ist das ein Widerspruch dazu, dass (a) ein Primideal ist. Falls $a \neq \pm 1, a \neq \pm p$ mit p prim, so existieren n, m mit $1 < |n|, |m| < |a|$ sodass $a = nm$. Daraus folgt nun $nm \in (a)$ und $n, m \notin (a)$, was wieder (a) als Primideal widerspricht. □

Bemerkung. Beachte: (0) ist prim in $\mathbb{Z}$, aber nicht maximal. In $\mathbb{Z}$ gilt „I maximal $\Rightarrow$ I prim“.

Satz 7.10. *Sei R ein kommutativer Ring, $R \neq \{0\}$ und $I \subseteq R$ ein Ideal. Dann gilt*

$$I \text{ Primideal} \iff R/I \text{ Integritätsbereich.}$$

Insbesondere folgt

$$\{0\} \text{ Primideal} \iff R \text{ Integritätsbereich.}$$

Beweis.

„$\Rightarrow$“ Da R kommutativ ist, ist auch R/I kommutativ. Sei I ein Primideal. Dann gilt $I \neq R$ und somit $R/I \neq \{0\}$.
Seien $\overline{x}, \overline{y} \in R/I$ mit $\overline{x} \odot \overline{y} = \overline{0}$.

$$\begin{aligned} &\overline{xy} = \overline{0} \\ \Rightarrow &xy \in I \\ \Rightarrow &x \in I \text{ oder } y \in I \\ \Rightarrow &\overline{x} = \overline{0} \text{ oder } \overline{y} = \overline{0} \\ \Rightarrow &R/I \text{ hat keine Nullteiler} \end{aligned}$$

„$\Leftarrow$“ Sei R/I ein Integritätsbereich. Dann ist $R/I \neq \{0\}$. Daraus folgt $I \neq R$. Seien $x, y \in R$ mit $xy \in I$. Dann gilt:

$$\begin{aligned} &\overline{x} \odot \overline{y} = \overline{xy} = \overline{y} \\ \Rightarrow &\overline{x} = \overline{0} \text{ oder } \overline{y} = \overline{0} \\ \Rightarrow &x \in I \text{ oder } y \in I \\ \Rightarrow &I \text{ ist ein Primideal} \end{aligned}$$

□

Korollar 7.11. *Sei $R \neq \{0\}$ ein kommutativer Ring, $I \subseteq R$ ein Ideal. Dann gilt:*

$$I \text{ maximal} \implies I \text{ prim}$$

Beweis. I maximal $\overset{7.8}{\iff}$ R/I Körper $\Rightarrow$ R/I Integritätsbereich $\overset{7.10}{\iff}$ I Primideal □

Korollar 7.12. *Es sei $R = \mathbb{Z}$.*

1. *Dann ist $\mathbb{Z}/n\mathbb{Z}$ Körper genau dann wenn $n = \pm p$ mit p prim.*
2. *$\mathbb{Z}/n\mathbb{Z}$ ist Integritätsbereich genau dann wenn $n = \pm p$ und p prim oder $n = 0$.*

Beweis.

1. Folgt aus Beispiel 9 und Satz 7.10.

2. Für Ringe R, die Integritätsbereich Hauptidealbereich sind, gilt für ein Primideal $I \neq \{0\}$, dass I maximal ist. □

Satz 7.13 (Universelle Eigenschaft von Polynomringen 2)**.** *Sei $\varphi\colon R \to S$ Ringhomomorphismus. Sei $a \in S$. Dann existiert ein eindeutiger Ringhomomorphismus*

$$\begin{aligned} \mathrm{ev}_a\colon R[t] &\longrightarrow S \\ t &\longmapsto a \\ p(t) = \sum_{i=0}^{\infty} b_i t^i &\longmapsto \sum_{i=0}^{\infty} \varphi(b_i) a^i \end{aligned}$$

Beweis. Da wir ev_a im Fall der Existenz bereits eindeutig charakterisiert haben, genügt es, die Existenz zu zeigen.

$$\begin{aligned} \mathrm{ev}_a(1_{R[t]}) &= \mathrm{ev}_a(1t^0) = \varphi(1) \cdot a^0 = 1 \\ \mathrm{ev}_a\left(\sum_{i=0}^{\infty} b_i t^i + \sum_{i=0}^{\infty} c_i t^i\right) &= \mathrm{ev}_a\left(\sum_{i=0}^{\infty} (b_i + c_i) t^i\right) = \sum_{i=0}^{\infty} \varphi(b_i + c_i) a^i \\ &= \sum_{i=0}^{\infty} \varphi(b_i) a^i + \sum_{i=0}^{\infty} \varphi(c_i) a^i = \mathrm{ev}_a\left(\sum_{i=0}^{\infty} b_i t^i\right) + \mathrm{ev}_a\left(\sum_{i=0}^{\infty} c_i t^i\right) \\ \mathrm{ev}_a\left(\left(\sum_{i=0}^{\infty} b_i t^i\right)\left(\sum_{i=0}^{\infty} c_i t^i\right)\right) &= \mathrm{ev}_a\left(\sum_{i=0}^{\infty}\left(\sum_{k=0}^{i} b_{i-k} c_k\right) t^i\right) = \sum_{i=0}^{\infty}\left(\sum_{k=0}^{i} \varphi(b_{i-k})\varphi(c_k)\right) a^i \\ &= \sum_{i=0}^{\infty}\left(\sum_{k=0}^{i} \varphi(b_{i-k}) a^{i-k} \varphi(c_k) a^k\right) = \left(\sum_{i=0}^{\infty} \varphi(b_i) a^i\right)\left(\sum_{i=0}^{\infty} \varphi(c_i) a^i\right) \\ &= \mathrm{ev}_a\left(\sum_{i=0}^{\infty} b_i t^i\right) \cdot \mathrm{ev}_a\left(\sum_{i=0}^{\infty} c_i t^i\right) \end{aligned}$$

Somit ist ev_a tatsächlich ein Ringhomomorphismus. □

Beispiel 11. Sei

$$\begin{aligned} \varphi\colon \mathbb{R} &\hookrightarrow \mathbb{C} \\ x &\longmapsto x \end{aligned}$$

Es existiert ein eindeutiger Ringhomomorphismus

$$\begin{aligned} \mathrm{ev}_i\colon \mathbb{R}[t] &\longrightarrow \mathbb{C} \\ t &\longmapsto i \\ p(t) &\longmapsto p(i) \end{aligned}$$

Es gilt $\mathrm{ev}_i(t^2+1) = i^2+1 = 0$. Somit gilt $t^2+1 \in \ker \mathrm{ev}_i$ und deshalb auch $(t^2+1) \subset \ker \mathrm{ev}_i$. Mit dem Homomorphiesatz erhalten wir einen eindeutigen Ringhomomorphismus $\overline{\mathrm{ev}_i}\colon \mathbb{R}[t]/(t^2+1) \to \mathbb{C}$ mit $\overline{\mathrm{ev}_i}(\overline{b_1 t + b_0}) = b_1 i + b_0$. Dieser ist offensichtlich surjektiv.

Da sich jedes $\overline{p(t)} \in \mathbb{R}[t]/(t^2+1)$ eindeutig schreiben lässt als $\overline{p(t)} = \overline{b_1 t + b_0}$ gilt:

$$\overline{\mathrm{ev}_i}(\overline{p(t)}) = \overline{\mathrm{ev}_i}(\overline{b_1 t + b_0}) = b_1 i + b_0 = 0 \Leftrightarrow b_1 = b_0 = 0$$

Damit ist $\overline{\mathrm{ev}_i}$ injektiv und somit ist $\overline{\mathrm{ev}_i}$ ein Isomorphismus von Ringen (insbesondere von Körpern).

Definition 7.11. Ist R ein kommutativer Ring, dann heißt $a \in R$ Nullstelle von $p(t) \in R[t]$, falls gilt: $p(a) \coloneqq \mathrm{ev}_a(p(t)) = 0$ ($\varphi\colon R \to R = \mathrm{id}_R$).

Satz 7.14. *Sei R ein kommutativer Ring sowie $a \in R$. Dann gilt:*

1. *a Nullstelle von $p(t) \Leftrightarrow t - a$ teilt $p(t)$ in $R[t]$*
2. *R Integritätsbereich $\Rightarrow R[t]$ ist Integritätsbereich und $\deg(p(t)q(t)) = \deg(p(t)) + \deg(q(t))$*
3. *$\deg(p(t)) = n \geq 0$, R Integritätsbereich $\Rightarrow p(t)$ hat maximal n verschiedene Nullstellen.*

[2. November 2017]

[9. November 2017]

Beweis.

1. „$\Leftarrow$“: Gilt $t - a \mid p(t)$, so existiert ein $q(t) \in R[t]$, sodass $p(t) = q(t) \cdot (t-a)$. Dann folgt $\mathrm{ev}_a(p(t)) = \mathrm{ev}_a(q(t)) \cdot \mathrm{ev}_a(t-a) = 0$, und a ist somit eine Nullstelle von $p(t)$.

   „$\Rightarrow$“: Sei a eine Nullstelle von $p(t)$ und weiterhin

$$\begin{aligned} \varphi\colon R &\hookrightarrow R[t] \\ r &\longmapsto r \cdot 1 \\ \overset{7.12}{\Longrightarrow} \mathrm{ev}_{t-a}\colon R[t] &\longrightarrow R[t] \\ t &\longmapsto t - a \\ \mathrm{ev}_{t+a}\colon R[t] &\longrightarrow R[t] \\ t &\longmapsto t + a \end{aligned}$$

   Es gilt $\mathrm{ev}_{t-a} \circ \mathrm{ev}_{t+a} = \mathrm{id}_{R[t]} = \mathrm{ev}_{t+a} \circ \mathrm{ev}_{t-a}$ (für alle $r \in R$ gilt $r \mapsto r1$ sowie $t \mapsto t + a \mapsto (t-a) + a = t$ und umgekehrt).

   Somit folgt:

$$\begin{array}{ccc} R[t] & \xrightarrow{\mathrm{ev}_{t-a}} & R[t] \\ & \searrow^{\mathrm{ev}_0} & \downarrow{\scriptstyle \mathrm{ev}_a} \\ & & R \end{array}$$

$\mathrm{ev}_a \circ \mathrm{ev}_{t-a} = \mathrm{ev}_0$ bzw. $\mathrm{ev}_0 \circ \mathrm{ev}_{t+a} = \mathrm{ev}_a$

$\Rightarrow \mathrm{ev}_a(p(t)) = 0 \Rightarrow \mathrm{ev}_0(\mathrm{ev}_{t+a}(p(t))) = 0 \Rightarrow t$ teilt $\mathrm{ev}_{t+a}(p(t)) \Rightarrow \exists q(t) \in R[t]$ sodass $q(t) \cdot t = \mathrm{ev}_{t+a}(p(t)) \Rightarrow p(t) = \mathrm{ev}_{t-a}(ev_{t+a}(p(t))) = \mathrm{ev}_{t-a}(q(t)) \cdot \mathrm{ev}_{t-a}(t) = \mathrm{ev}_{t-a}(q(t)) \cdot (t-a) \Rightarrow t - a$ teilt $p(t)$.

2. Es seien $m, n \in \mathbb{N}_0$. Dann hat man

$$p(t)q(t) = \left(\sum_{i=0}^{m} a_i t^i\right)\left(\sum_{i=0}^{n} b_i t^i\right) = a_n b_m t^{n+m} + \ldots,$$

wobei a_n und b_n als Leitkoeffizienten nicht 0 sind, also $a_m b_n \neq 0$, da R ein Integritätsbereich ist. Es folgt $\deg(p(t)q(t)) = n + m$.

3. Wir führend eine Induktion nach dem Grad von $p(t)$.

Induktionsanfang: Für $\deg(p(t)) = 1$ ist $p(t) = b_1 t + b_0$ mit $b_0, b_1 \in R$. Falls a eine Nullstelle von $p(t)$ ist, so existiert nach Teil 1 ein $r \in R \setminus \{0\}$, sodass $r(t-a) = b_1 t + b_0$. Daraus folgt $r = b_1$ und $-ar = b_0$. Wir nehmen an, $a' \in R$ sei eine weitere Nullstelle. Dann ist $-ar = -a'r' = -a'r$, da $r = b_1 = r'$, also $r(a' + (-a)) = 0$. Da R ein Integritätsbereich ist und $r \neq 0$ ist, muss $a' = a$ gelten.

Induktionsschritt: Sei nun $\deg(p(t)) = n > 1$ sowie a eine Nullstelle von $p(t)$. Dann existiert wieder mit Teil 1 des Satzes ein $q(t) \in R[t]$ mit $(t-a)q(t) = p(t)$ und $\deg(q(t)) = n - 1$ (nach Teil 2 des Satzes). Also gilt nach der Induktionsvoraussetzung, dass $q(t)$ maximal $n-1$ Nullstellen hat.

Behauptung: b ist genau dann eine Nullstelle von $p(t)$, wenn eine b Nullstelle von $q(t)$ oder $b = a$ ist.

„$\Leftarrow$“: Ist b eine Nullstelle von $q(t)$, so erhalten wir $\mathrm{ev}_b(p(t)) = \mathrm{ev}_b(q(t)) \cdot \mathrm{ev}_b(t-a) = 0 \cdot \mathrm{ev}_b(t-a) = 0$. Ist $b = a$, so folgt ebenfalls $\mathrm{ev}_b(p(t)) = \mathrm{ev}_b(q(t)) \cdot \mathrm{ev}_b(t-a) = \mathrm{ev}_b(q(t)) \cdot 0 = 0$.

„$\Rightarrow$“: Ist b Nullstelle von $p(t)$, so folgt von R dann $0 = \mathrm{ev}_b(p(t)) = \mathrm{ev}_b(q(t)) \cdot \mathrm{ev}_b(t-a)$. Da R ein Integritätsbereich ist, hat man $\mathrm{ev}_b(q(t)) = 0$, also ist b eine Nullstelle von $q(t)$, oder $\mathrm{ev}_b(t-a) = 0$, also $b = a$.

Folglich hat $p(t)$ maximal n verschiedene Nullstellen. □

Definition 7.12. Ein Körper K heißt algebraisch abgeschlossen, falls jedes $p(t) \in K[t]$ mit $\deg(p(t)) > 0$ eine Nullstelle hat.

Bemerkung.

1. Es sei K algebraisch abgeschlossen sowie $p(t) \in K[t]$ mit $\deg(p(t)) = n > 0$. Dann existieren ein $c \in K^\times$ und $a_1, \ldots, a_n \in K$ (nicht zwangsweise verschieden), sodass $p(t) = c(t-a_1) \cdot \cdots \cdot (t-a_n)$. (Beweis: Teil 3 von Satz 7.14 induktiv anwenden)

2. Oft schreibt man $K = \overline{K}$ für K algebraisch abgeschlossen.

Definition 7.13. Sei S ein Ring und $R \subseteq S$ ein Unterring sowie $a_1, \dots, a_n \in S$ mit $a_i x = x a_i$ und $a_i a_j = a_j a_i$ für alle $x \in R$, $1 \leq i, j \leq n$. Setze

$$R[a_1, \dots, a_n] \coloneqq \bigcap_{\substack{S' \subseteq S \text{ Unterring}, \\ R \subseteq S', \\ a_1, \dots, a_n \in S'}} S'.$$

Dann heißt $R[a_1, \dots, a_n]$ der von $a_1, \dots, a_n$ erzeugte Unterring in S über R.

Bemerkung. $R[a_1, \dots, a_n]$ ist der kleinste Unterring von S, der R und $a_1, \dots, a_n$ enthält.

Beweis. $R[a_1, \dots, a_n]$ enthält R und $a_1, \dots, a_n$ per Konstruktion. Ist S' ein weiterer solcher Unterring, so ist enthält er bereits $\bigcap_{S''} S'' = R[a_1, \dots, a_n]$, wobei S'' wie oben definiert ist. □

Satz 7.15. *Sei S ein Ring und $R \subseteq S$ ein Unterring sowie $a_1, \dots, a_n \in S$ mit $a_i a_j = a_j a_i$ und $a_i x = x a_i$ für alle $x \in R$ und $1 \leq i, j \leq n$. Sei $\varphi \colon R \hookrightarrow S$ die Inklusion und $R[t_1, \dots, t_n] \coloneqq ((\dots(R[t_1])[t_2])\dots)[t_n]$. Dann ist $R[a_1, \dots, a_n]$ das Bild des Auswertungshomomorphismus*

$$\begin{aligned} \mathrm{ev} = \mathrm{ev}_{a_1, \dots, a_n} : R[t_1, \dots, t_n] &\longrightarrow S \\ p(t_1, \dots t_n) &\longmapsto p(a_1, \dots, a_n) \end{aligned}$$

wobei

$$p(t_1, \dots, t_n) = \sum_{(m_1, \dots, m_n) \in \mathbb{N}_0^n} b_{m_1, \dots, m_n} t_1^{m_1} \dots t_n^{m_n}$$

(fast alle $b_{m_1, \dots, m_n} = 0$) auf

$$p(a_1, \dots, a_n) = \sum_{(m_1, \dots, m_n) \in \mathbb{N}_0^n} b_{m_1, \dots, m_n} a_1^{m_1} \dots a_n^{m_n}$$

abgebildet wird.

Beweis. Zuerst wird Wohldefiniertheit gezeigt:

$$\begin{gathered} R[t_1, \dots, t_n] \xrightarrow{\mathrm{ev}_{a_n}} R[t_1, \dots, t_{n-1}] \xrightarrow{\mathrm{ev}_{a_{n-1}}} \dots \xrightarrow{\mathrm{ev}_{a_2}} R[t_1] \xrightarrow{\mathrm{ev}_{a_1}} S \\ \sum b_{m_1, \dots, m_n} t_1^{m_1} \dots t_n^{m_n} \longmapsto \sum b_{m_1, \dots m_n} a_n^{m_n} \dots a_1^{m_1} = \sum b_{m_1, \dots, m_n} a_1^{m_1} \dots a_n^{m_n} \end{gathered}$$

Somit ist ev als Verknüpfung von Ringhomomorphismen wieder ein wohldefinierter Ringhomomorphismus.

Nun muss noch gezeigt werden, dass $R[a_1, \dots, a_n] = \operatorname{im} \mathrm{ev}$ gilt. Für $r \in R$ gilt $\mathrm{ev}(r t_1^0 \dots t_n^0) = r a_1^0 \dots a_n^0 = r$, also folgt $R \subseteq \operatorname{im}(\mathrm{ev})$. Da nun $\mathrm{ev}(1 t_1^0 \dots t_{i-1}^0 t_1^1 t_{i+1}^0 \dots t_n^0) = 1 a_i = a_i$, erhalten wir $a_i \in \operatorname{im}(\mathrm{ev})$ und dadurch $R[a_1, \dots, a_n] \subseteq \operatorname{im}(\mathrm{ev})$.

Sei $S' \subseteq S$ ein Unterring mit $R \subseteq S'$ und $a_1, \dots, a_n \in S'$. Dann ist $p(a_1, \dots, a_n) = \sum b_{m_1, \dots, m_n} a_1^{m_1} \dots a_n^{m_n} \in S'$, da S' unter $+$ und $\cdot$ abgeschlossen ist. Man hat schließlich $R[a_1, \dots, a_n] = \operatorname{im}(\mathrm{ev})$. □

Definition 7.14. Sei S ein kommutativer Ring und $R \subseteq S$ ein Unterring. Seien $a_1, \ldots, a_n \in S$. Dann heißen $a_1, \ldots, a_n$ algebraisch unabhängig (über R), fallls ev $= \mathrm{ev}_{a_1,\ldots,a_n}$ (von Satz 7.15) injektiv ist.

Falls ev nicht injektiv ist, so heißen $a_1, \ldots, a_n$ algebraisch abhängig (über R).

Lemma 7.16. *Sei S ein kommutativer Ring und $R \subseteq S$ ein Unterring sowie $a_1, \ldots, a_n \in S$. Es gilt:*

1. *$a_1, \ldots, a_n$ sind genau dann algebraisch abhängig über R, wenn $p(t_1, \ldots, t_n) \in R[t_1, \ldots, t_n] \setminus \{0\}$ existiert sodass $p(a_1, \ldots, a_n) = 0$.*
2. *$a_1, \ldots, a_n$ sind genau dann algebraisch unabhängig über R, wenn $p(a_1, \ldots, a_n) = 0$ für ein Polynom $p(t_1, \ldots, t_n) \in R[t_1, \ldots, t_n]$ impliziert, dass $p(t_1, \ldots, t_n) = 0$.*

Spezialfall: Sei $n = 1$. Dann ist $a \in S$ algebraisch abhängig über R, falls $p(a) = 0$ für ein $p(t) \in R[t] \setminus \{0\}$ gilt.

Beispiel 12.

1. $1, i \in \mathbb{C}$ sind linear unabhängig über $\mathbb{R}$, aber algebraisch abhängig, denn mit $p(t_1, t_2) = t_1 + t_2^2$ hat man $\mathrm{ev}_{1,i}(p(t_1, t_2)) = 1 + i^2 = 0$.

   Schon $i \in \mathbb{C}$ ist algebraisch abhängig über $\mathbb{R}$, man betrachte $\mathrm{ev}_i(1 + t^2) = 1 + i^2 = 0$.
2. Sei S ein kommutativer Ring sowie $a \in S$. Dann ist a ist algebraisch abhängig über S: $\mathrm{ev}_a(t - a) = a - a = 0$.
3. Sei $S = R[t_1, \ldots, t_n]$. Dann sind $t_1, \ldots t_n$ algebraisch unabhängig über R, weil $\mathrm{ev}_{t_1,\ldots,t_n} \colon R[t_1, \ldots, t_n] \to R[t_1, \ldots, t_n] = \mathrm{id}_{R[t_1,\ldots t_n]}$ offensichtlich injektiv ist.
4. Algebraisch über $\mathbb{Q}$ unabhängige Zahlen in $\mathbb{R}$ heißen transzendente Zahlen.

[9. November 2017]

[13. November 2017]

8. Faktorielle Ringe

Ab jetzt sind alle Ringe kommutativ.

Definition 8.1. Sei R ein Integritätsbereich (also $R \neq \{0\}$ und nullteilerfrei) sowie $a \in R$, $a \neq 0$, $a \notin R^\times$. Weiterhin seien $b, c \in R$.

- a heißt irreduzibel, falls
$$a = b \cdot c \quad \Longrightarrow \quad b \in R^\times \text{ oder } c \in R^\times.$$
- a heißt prim, falls
$$a \mid b \cdot c \quad \Longrightarrow \quad a \mid b \text{ oder } a \mid c.$$

- R ist ein faktorieller Ring, falls zusätzlich für $b \in R, b \neq 0$ eine eindeutige Zerlegung „PZ“
$$b = \varepsilon p_1 p_2 \dots p_r \text{ für ein } r \in \mathbb{N}$$
mit $\varepsilon \in R^\times$ und irreduziblen $p_1, \dots, p_r \in R$ existiert. Die Eindeutigkeit besteht hierbei bis auf Einheiten und Reihenfolge der Faktoren, das heißt, falls $b = \varepsilon' p_1' \dots p_s'$ für $\varepsilon' \in R^\times$ und $p_1', \dots, p_s'$ irreduzibel, dann gilt $s = r$ und es existieren $c_1, \dots, c_r \in R^\times$ und ein $\pi \in S_r$, sodass $p_i' = c_i p_{\pi(i)}$ für alle $1 \leq i \leq s = r$ gilt.

Beispiel 1. $R = \mathbb{Z}$. Sei $a \in \mathbb{Z}$ mit $a \neq 0$ und $a \notin \{\pm 1\} = \mathbb{Z}^\times$. Dann erhalten wir

$$a \text{ prim} \quad \iff \quad a = \pm p \text{ mit } p \text{ prim} \quad \iff \quad a \text{ irreduzibel.}$$

$\mathbb{Z}$ ist faktoriell, denn jedes $b \in \mathbb{Z}, b \neq 0$ hat eine Primzahlzerlegung $b = \varepsilon p_1 \dots p_r$ mit p_i prim und $\varepsilon \in \{\pm 1\} = \mathbb{Z}^\times$. Diese ist „eindeutig“, z.B. $10 = 1 \cdot 2 \cdot 5 = (-1) \cdot (-2) \cdot 5 = (-1) \cdot 2 \cdot (-5)$ etc.

Beispiel 2. $R = \mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{5}i \mid a, b \in \mathbb{Z}\} \subset \mathbb{C}$. Das ist ein Unterring von $\mathbb{C}$, genauer der von $\sqrt{5}i$ über $\mathbb{Z}$ erzeugte Unterring in $\mathbb{C}$, also

$$\mathbb{Z}[\sqrt{-5}] = \bigcap_{\substack{S \subseteq \mathbb{C} \text{ Unterring} \\ \mathbb{Z} \subseteq S \\ \sqrt{5}i \in S}} S.$$

Dann sind 2, 3, $1 + \sqrt{5}i$, $1 - \sqrt{5}i$ irreduzibel (Übung). Insbesondere ist $1 + \sqrt{5}i \notin R^\times$, da es sonst $a, b \in \mathbb{Z}$ gäbe, sodass $(1 + \sqrt{5}i)(a + b\sqrt{5}i) = 1$ und somit $a - 5b = 1$ und $a + b = 0$ ist, was aber unlösbar ist. Außerdem: $1 + \sqrt{5}i \notin \{\varepsilon 2, \varepsilon 3 \mid \varepsilon \in R^\times\}$ (Übung).

Aber es ist $6 = 2 \cdot 3 = (1 + \sqrt{5}i)(1 - \sqrt{5}i)$, also ist R nicht faktoriell, da die Zerlegung nicht eindeutig ist.

Lemma 8.1. *Sei R ein Integritätsbereich und $a \in R$. Dann gilt:*

1. *a ist genau dann prim, wenn $(a) \neq \{0\}$ ein Primideal ist.*
2. *a ist genau dann irreduzibel, wenn $(a) \neq \{0\}$, $(a) \neq R$ und es kein $b \in R$ gibt, sodass $(a) \subsetneq (b)$ gilt, außer (b) erzeugt bereits den ganzen Ring, also $\forall b \in R : (a) \subseteq (b) \Rightarrow ((a) = (b)$ oder $(b) = R)$.*

Beweis.

1. „$\Rightarrow$“: Sei a prim. Nach Definition gilt $a \neq 0, a \notin R^\times$. Folglich gilt auch $(a) \neq \{0\}, (a) \neq R$. Sei nun $bc \in (a)$ mit $b, c \in R$. Dann teilt a bc. Da a prim ist, teilt nun also a b oder c. Es folgt $b \in (a)$ oder $c \in (a)$ und somit ist (a) ein Primideal.

   „$\Leftarrow$“: Sei $(a) \neq \{0\}$ (und somit $a \neq 0$) und sei (a) ein Primideal. Nach Definition gilt $(a) \neq R$, also ist a keine Einheit. Gelte nun a teilt bc. Dann liegt bc in (a). Da (a) ein Primideal ist, gilt $b \in (a)$ oder $c \in (a)$. Somit teilt a b oder c und ist folglich prim.

2. „⇐“: Sei $(a) \neq \{0\}, (a) \neq R$. Dann folgt sofort $a \neq 0$ und $a \notin R^\times$. Sei nun $a = bc$, also $(a) \subseteq (b)$. Nach Voraussetzung gilt dann $(a) = (b)$ oder $(b) = R$ (also $b \in R^\times$). Falls b keine Einheit ist, existiert somit ein $r \in R$, sodass $b = ar$. Durch Umformen folgt

$$\begin{aligned} & b = ar \\ \Rightarrow & b = bcr \\ \Rightarrow & b(1 - cr) = 0 \\ \Rightarrow & 1 - cr = 0, \text{ da R nullteilerfrei ist} \end{aligned}$$

In diesem Fall gilt $c \in R^\times$ und folglich ist b oder c eine Einheit, also a irreduzibel.

„⇒“: Sei a irreduzibel. Es folgt sofort $(a) \neq \{0\}$ und $(a) \neq R$. Sei nun $b \in R$ mit $(a) \subseteq (b)$. Dann gilt b teilt a und somit existiert ein $r \in R$, sodass $a = br$. Aus der Irreduzibilität von a folgt nun $b \in R^\times$ oder $r \in R^\times$. Folglich gilt $(b) = R$ oder $(a) = (b)$. □

Satz 8.2. *Sei R ein Integritätsbereich. Dann gilt für $a \in R$:*

1. *Wenn a prim ist, dann ist a auch irreduzibel.*
2. *Falls R zusätzlich ein Hauptidealring ist:*
   a) *a ist genau dann prim, wenn a irreduzibel ist.*
   b) *Sei $\{0\} \neq I \subseteq R$ ein Ideal. Dann ist I genau dann ein Primideal, wenn I ein maximales Ideal ist.*

Beweis.

1. Sei $a = bc$ mit $b, c \in R$. Da a prim ist, folgt $a \mid b$ oder $a \mid c$, es ist also $b = ar$ oder $c = ar$ für ein $r \in R$. Folglich haben wir $b = bcr$ oder $c = cbr$ und somit auch $b(1 - cr) = 0$ oder $c(1 - br) = 0$. Da R nullteilerfrei ist und $b, c \neq 0$, weil $a \neq 0$, ist c oder b eine Einheit. Schließlich ist a irreduzibel.

2. a) Die eine Richtung folgt nach 1. Sei für die Rückrichtung nun a irreduzibel. Nach Lemma 8.1 ist (a) maximal unter allen Hauptidealen in R. Da R ein Hauptidealring ist, ist (a) sogar ein maximales Ideal. Aus Korollar 7.11 folgt, dass (a) ein Primideal ist. Nun ist a prim nach Lemma 8.1, da $(a) \neq \{0\}$, weil a irreduzibel, also insbesondere $a \neq 0$ ist.

   b) „⇐“: siehe Satz 7.10

   „⇒“: Sei $\{0\} \neq I \subseteq R$ ein Primideal. Da R ein Hauptidealring ist, existiert ein $a \in R$ mit $I = (a)$, wobei a nach Lemma 8.1 prim ist. Mit Teil 1. folgt $I = (a)$ und a irreduzibel. Wieder nach Lemma 8.1 ist $I = (a)$ maximal unter allen Hauptidealen, und da R ein Hauptidealring ist, ist I tatsächlich ein maximales Ideal. □

Definition 8.2. Sei R ein Integritätsbereich. R heißt euklidischer Ring, falls eine Abbildung

$$\deg\colon R \setminus \{0\} \longrightarrow \mathbb{N}$$

existiert, sodass für alle $a, b \in R, b \neq 0$ dann $q, r \in R$ mit

$$a = qb + r \text{ und } r = 0 \text{ oder } \deg(r) < \deg(b)$$

existieren.

Satz 8.3. *Jeder euklidische Ring ist ein Hauptidealring.*

Beweis. Wie für $R = \mathbb{Z}$. □

Satz 8.4. *Jeder Hauptidealring ist faktoriell.*

Beweis. Sei R ein Hauptidealring und $0 \neq b \in R$. Es ist nun die Existenz einer eindeutigen Primfaktorzerlegung zu zeigen.

Existenz: Wir nehmen an, dass diese nicht existiert, also insbesondere b nicht irreduzibel ist. Dann existieren $b_1, c_1 \notin R^\times$ mit $b = b_1 c_1$, wobei nicht beide Faktoren eine Primfaktorzerlegung haben. O.B.d.A. habe b_1 keine Primfaktorzerlegung, insbesondere b_1 nicht irreduzibel. Folglich existieren $b_2, c_2 \notin R^\times$ mit $b_1 = b_2 c_2$ und o.B.d.A. habe b_2 keine (PZ) etc.

Wir erhalten eine Kette echter Inklusionen

$$(b_1) \subsetneq (b_2) \subsetneq (b_3) \subsetneq (b_4) \subsetneq \dots$$

für gewisse $b_i \in R$. Es gilt tatsächlich $(b_i) \subsetneq (b_{i+1})$, denn sonst wäre $b_i = b_{i+1} c_{i+1}$ für ein $c_{i+1} \in R$ und $b_{i+1} = b_i c_i'$ für ein $c_i' \in R$, also $b_i(1 - c_i' c_{i+1}) = 0$. Da R nullteilerfrei ist, folgt $c_{i+1} \in R^\times$ für alle i, was im Widerspruch zur Konstruktion steht.

Setze nun $I := \bigcup_{i=1}^{\infty} (b_i)$. Dies ist ein Ideal und somit folgt $I = (d)$ für ein $d \in R$, weil R ein Hauptidealring ist. Nach Definition von I existiert ein b_i mit $d \in (b_i)$, also $(d) \subseteq (b_i)$, weil (b_i) ein Ideal ist. Wir erhalten unmittelbar $(d) \subseteq (b_i) \subseteq I = (d)$ oder $(b_i) = (d) \subseteq (b_j) = (d)$ für alle $j > i$. Das ist nun ein Widerspruch zu $(b_i) \subsetneq (b_{i+1})$. Folglich existiert für b eine Primfaktorzerlegung.

Eindeutigkeit: Seien $b = \varepsilon p_1 \dots p_r$ und $b = \varepsilon' p_1' \dots p_s'$ zwei Zerlegungen mit $\varepsilon, \varepsilon' \in R^\times$ und irreduziblen $p_i, p_j' \in R$ für $1 \leq i \leq r$, $1 \leq j \leq s$. Betrachte p_1'. Nach Satz 8.1 2a) ist p_1' als irreduzibles Element schon prim. Da $p_1' \mid b$, folgt $p_1' \mid p_i$ für ein i $(1 \leq i \leq r)$ oder p_1' teilt ε. Letztes kann aber nicht eintreten, da sonst $p_1' \in R^\times$ ist, was im Widerspruch zur Irreduzibilität von p_1' steht.

Es sei also i so fixiert, dass $p_1' \mid p_i$. O.B.d.A. sei $i = 1$ (eventuelle Umnummerierung). Also ist $p_1 = p_1' c$ für ein $c \in R$. Da p_1 irreduzibel ist, ist $p_1' \in R^\times$ oder $c \in R^\times$. p_1' ist aber irreduzibel und damit insbesondere keine Einheit; folglich ist $c \in R^\times$.

Wir erhalten somit $\varepsilon c p_1' p_2 \dots p_r = b = \varepsilon' p_1' p_2' \dots p_s'$. Da R nullteilerfrei ist, darf man hier kürzen: $\varepsilon c p_2 \dots p_r = \varepsilon' p_2' \dots p_s'$. Wir wenden nun dieses Argument iterativ an und erhalten schließlich $r = s$ und $p_i = p'_{\pi(i)} c_i$ für $c_i \in R^\times$ und $\pi \in S_r$, was genau die gewünschte Eindeutigkeit darstellt.

Somit ist R faktoriell. □

Bemerkung. Insbesondere: In $\mathbb{Z}$ ist Primfaktorzerlegung „eindeutig“.

9. Maximale Ideale: Existenz

Satz 9.1. *Sei R ein Ring. und $R \neq \{0\}$.*

1. *R besitzt maximale Ideale (und damit auch Primideale nach Korollar 7.11).*
2. *Jedes Ideal $I \subseteq R$, $I \neq R$ ist in einem (nicht notwendigerweise eindeutigen!) maximalen Ideal enthalten.*

Beweis. Wir zeigen zunächst 2. unter der Annahme von 1.: Sei $I \neq R$ ein Ideal in R. Dann ist $R/I \neq \{0\}$ und besitzt daher nach 1. ein maximales Ideal. Nach Satz 7.9 existiert ein maximales Ideal $J \subseteq R$ mit $J \supseteq I$.

[13. November 2017]

[16. November 2017]

Es bleibt die erste Aussage zu zeigen. Hierfür sei $M \coloneqq \{I \subseteq R \mid I \text{ Ideal}, I \neq R\}$. Betrachte nun die partielle Ordnung $\leq$ auf M gegeben durch $I_1 \leq I_2$ falls $I_1 \subseteq I_2$. Sei $N \subseteq M$ eine total geordnete Teilmenge. Dann betrachte $\tilde{I} \coloneqq \bigcup_{I \in N} I$ ist ein Ideal.

Es folgt $\tilde{I} \in M$, weil $1 \notin \tilde{I}$, da $1 \notin I$ für alle $I \in N$ aus unserer Definition von $N \subseteq M$ folgt.

Somit ist N in M nach oben beschränkt. Nach dem Lemma von Zorn existiert ein maximales Element in M, woraus die Existenz eines (nicht notwendigerweise eindeutigen) maximalen Ideals in R folgt. □

Beispiel 1. $R = \mathbb{C}[t], a \in \mathbb{C}$. Dann ist

$$\begin{aligned} \mathrm{ev}_a \colon \mathbb{C}[t] &\longrightarrow \mathbb{C} \\ p(t) &\longmapsto p(a) \end{aligned}$$

ein surjektiver Ringhomomorphismus. Es gilt $p(t) \in \ker \mathrm{ev}_a$ genau dann, wenn $p(a) = 0$, also wenn a eine Nullstelle von $p(t)$ ist. Nach Satz 7.13 ist das äquivalent dazu, dass $(t-a)$ das Polynom $p(t)$ teilt; also ist $p(t)$ Element des von $(t-a)$ erzeugten Ideals. Nach dem Homomorphiesatz für Ringe erhalten wir einen Isomorphismus

$$\mathbb{C}[t]/(t-a) \longrightarrow \mathbb{C}$$

Da $\mathbb{C}$ ein Körper ist, ist $I = (t-a)$ maximales Ideal (für jedes $a \in \mathbb{C}$).

10. Einschub: Chinesischer Restsatz

Mathematik in der Praxis. Stroppel hat eine Pralinenschachtel. Wenn jemand errät, wieviele Pralinen sich darin befinden, bekommt derjenige alle Pralinen (da niemand nachprüfen kann, ob das, was Stroppel bezüglich der Anzahl der Pralinen behauptet, stimmt, wird vermutlich niemand die Pralinen bekommen). Wir wissen über die Anzahl der Pralinen: Wenn man sie auf vier Leute aufteilt, bleiben zwei übrig; wenn man sie auf sieben Personen verteilt, bleiben drei Pralinen übrig, also

$$\begin{aligned} x &\equiv 2 \pmod 4, \\ x &\equiv 3 \pmod 7. \end{aligned}$$

Eine Lösung ist zum Beispiel $x = 10$, aber laut Stroppel ist das nicht die Anzahl der Pralinen (die Pralinenschachtel sieht aber gar nicht so groß aus, als ob da noch wirklich viel mehr Pralinen darin sein könnten). Wir vermuten nun, dass genau die Zahlen der Form $10 + 28k, k \in \mathbb{Z}$ Lösungen sind.

Satz 10.1 (Chinesischer Restsatz)**.** *Sei R ein kommutativer Ring sowie $R \neq \{0\}$. Seien weiter $I_1, \dots, I_s$ Ideale in R, sodass $I_i + I_j = R$ für alle $i \neq j$ gilt. Dann existiert ein surjektiver Ringhomomorphismus*

$$\begin{aligned} \Phi\colon R &\longrightarrow R/I_1 \times \cdots \times R/I_s \\ r &\longmapsto (\overline{r}, \dots, \overline{r}) \end{aligned}$$

(wobei $\overline{r}$ jeweils die Nebenklasse von r bezüglich dem passenden Ideal I_i ist). Dabei gilt $\ker \Phi = I_1 \cap \cdots \cap I_s$*. Insbesondere erhalten wir einen Isomorphismus von Ringen:*

$$R/(I_1 \cap \cdots \cap I_s) \longrightarrow R/I_1 \times \cdots \times R/I_s$$

Beweis. Es lässt sich leicht nachrechnen, dass Φ tatsächlich ein Ringhomomorphismus ist. Es bleibt die Surjektivität von Φ zu zeigen. Nach Voraussetzung existieren für $1 \leq i, j \leq s$ Elemente $a_{ij} \in I_i, a_{ji} \in I_j$ mit $a_{ij} + a_{ji} = 1$. Wir definieren nun

$$b_i := \prod_{\substack{j \neq i \\ 1 \leq j \leq s}} (1 - a_{ij}) = \prod_{\substack{j \neq i \\ 1 \leq j \leq s}} a_{ji}$$

Es gilt

$$\overline{b_i} = \begin{cases} \overline{0} \text{ in } R/I_j & \text{für } i \neq j, \\ \overline{1} \text{ in } R/I_i & \text{für } i = j. \end{cases} \tag{*}$$

Sei nun $(\overline{r_1}, \dots, \overline{r_s}) \in R/I_1 \times \cdots \times R/I_s$ beliebig ($r_i \in R$). Wir setzen

$$x := \sum_{i=1}^{s} b_i r_i \in R.$$

Da Φ ein Ringhomomorphismus ist, folgt dann mit (*)

$$\Phi(x) = \sum_{i=1}^{s} \Phi(b_i r_i) = \sum_{i=1}^{s} \Phi(b_i)\Phi(r_i) = \left(\sum_{i=1}^{s} \overline{b_i}\overline{r_i}, \dots, \sum_{i=1}^{s} \overline{b_i}\overline{r_i} \right) = (\overline{r_1}, \dots, \overline{r_s}).$$

Folglich ist x Urbild von $(\overline{r_1}, \dots, \overline{r_s})$. Damit ist Φ ist surjektiv.

Schließlich ist $r \in \ker \Phi$ genau dann, wenn $(\overline{r}, \dots, \overline{r}) = (\overline{0}, \dots, \overline{0}) \in R/I_1 \times \cdots \times R/I_s$, also wenn $\overline{r} = \overline{0} \in R/I_k$ für alle $1 \leq k \leq s$. Das ist aber äquivalent dazu, dass r im Schnitt $I_1 \cap \cdots \cap I_s$ liegt, also $\ker \Phi = I_1 \cap \cdots \cap I_s$. □

11. Lokalisierung

Definition 11.1. Sei R ein kommutativer Ring und $R \neq \{0\}$. Eine Teilmenge $S \subseteq R$ heißt multiplikativ abgeschlossen, falls $1 \in S$ und $s_1, s_2 \in S \Rightarrow s_1 s_2 \in S$ gelten. Dann nennen wir $S^{-1}R$ die Lokalisierung von R an S. Dabei ist $S^{-1}R$ ein kommutativer Ring, wobei die Elemente die Äquivalenzklassen in $R \times S$ bezüglich $\sim$ definiert durch

$$(r, s) \sim (r', s') \quad \Longleftrightarrow \quad \exists a \in S \colon a \cdot (r \cdot s' - r' \cdot s) = 0_R$$

(siehe Übungsblatt 5) sind. Wir bezeichnen mit $\frac{r}{s}$ die Äquivalenzklasse von $(r, s) \in R \times S$. Wir nennen $S^{-1}R$ auch den Ring der Brüche für R bezüglich S.

Bemerkung.

1. Falls $0_R \in S$ ist, so ist $S^{-1}R$ bereits der Nullring, denn für $s, s' \in S$ und $r, r' \in R$ gibt es ein $a \in S$ (nämlich z.B. $a = 0$) mit $a(rs' - r's) = 0$.

2. Falls R ein Integritätsbereich ist, ist auch $S^{-1}R$ ein Integritätsbereich für alle S mit $0 \notin S$ (selber nachrechnen!).

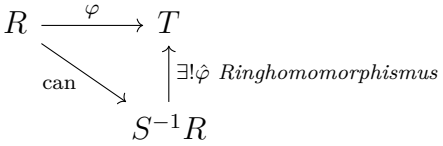
Satz 11.1 (Universelle Eigenschaft der Lokalisierung)**.** *Sei R ein kommutativer Ring, $R \neq \{0\}$, und $S \subseteq R$ multiplikativ abgeschlossen.*

1. *Die Abbildung*

$$\begin{array}{rccc} \mathrm{can} \colon & R & \longrightarrow & S^{-1}R \\ & r & \longmapsto & \dfrac{r}{1} \end{array}$$

   ist ein Ringhomomorphismus, wobei $\mathrm{can}(S) \subseteq (S^{-1}R)^\times$.

2. *Sei $\varphi \colon R \to T$ ein Ringhomomorphismus, sodass $\varphi(S) \subseteq T^\times$, dann existiert ein eindeutiger Ringhomomorphismus $\hat{\varphi} \colon S^{-1}R \to T$, sodass $\hat{\varphi} \circ \mathrm{can} = \varphi$, also sodass das nachfolgende Diagramm kommutiert.*



Beweis.

1. Durch einfaches Nachrechnen stellt man fest, dass can ein Ringhomomorphismus ist. Weiterhin sei $s \in S$. Dann ist $\mathrm{can}(s) = \frac{s}{1}$ und $\frac{s}{1} \cdot \frac{1}{s} = 1$, also hat $\frac{s}{1}$ ein Inverses bezüglich der Multiplikation, ist also eine Einheit. Damit folgt die erste Aussage.

2. Existenz: Wir definieren $\hat{\varphi}(\frac{r}{s}) = \varphi(r)\varphi(s)^{-1}$, wobei das Inverse bezüglich $\cdot$ in $S^{-1}R$ nach Voraussetzung existiert. Wieder durch Nachrechnen erhält man, dass $\hat{\varphi}$ ein Ringhomomorphismus ist. Es gilt

$$\hat{\varphi} \circ \mathrm{can}(r) = \hat{\varphi}(\frac{r}{1}) = \varphi(r)\varphi(1)^{-1} = \varphi(r) \cdot 1^{-1} = \varphi(r)$$

   Damit folgt die Existenz von $\hat{\varphi}$.

   Eindeutigkeit: Wir erhalten

$$\begin{aligned}\hat{\varphi}\left(\frac{r}{s}\right) =& \hat{\varphi}\left(\frac{r}{1} \cdot \frac{1}{s}\right)\\ =& \hat{\varphi}\left(\frac{r}{1}\right) \cdot \hat{\varphi}\left(\frac{1}{s}\right)\\ =& \hat{\varphi}\left(\frac{r}{1}\right) \hat{\varphi}\left(\left(\frac{s}{1}\right)^{-1}\right)\\ =& \hat{\varphi}\left(\frac{r}{1}\right) \hat{\varphi}\left(\frac{s}{1}\right)^{-1}\\ =& \varphi(r)\varphi(s)^{-1}\end{aligned}$$

   weil $\hat{\varphi} \circ \mathrm{can} = \varphi$, also $\hat{\varphi}(\frac{r}{s}) = \varphi(r)\varphi(s)^{-1}$ gilt. Damit ist $\hat{\varphi}$ eindeutig. □

Definition 11.2. Falls R ein Integritätsbereich ist und $R \neq \{0\}$, so ist $S = R \setminus \{0\}$ multiplikativ abgeschlossen und $S^{-1}R =: \mathrm{Quot}(R)$ ist nach dem Übungsblatt ein Körper. Wir nennen diesen den Quotientenkörper zu R.

Bemerkung. Wir weisen auf die Unterscheidung zwischen R/I, einem Faktorring, und $S^{-1}R$, einem Quotientenring bzw. Quotientenkörper, hin.

Beispiel 1.

1. Es ist
$$\mathrm{Quot}(\mathbb{R}[t]) = \left\{ \frac{f(t)}{g(t)} \;\middle|\; f(t), g(t) \in \mathbb{R}[t], g(t) \neq 0 \right\}$$
   der Körper der rationalen Funktionen über $\mathbb{R}$ in der Variable t.

2. Was ist z.B. $\mathrm{Quot}(\mathbb{Z}[t])$? Können wir diesen „gut“ beschreiben? (Stroppel kündigt einen Überkill an...)

   Es sei R ein Integritätsbereich, wir betrachten die Abbildung

$$\begin{array}{rccccccc}\varphi\colon R & \xrightarrow{\mathrm{can}} & \mathrm{Quot}(R) & \longrightarrow & (\mathrm{Quot}(R))[t] & \longrightarrow & \mathrm{Quot}((\mathrm{Quot}(R))[t])\\ r & \longmapsto & \frac{r}{1} & \longmapsto & \text{konstantes Polynom } \frac{r}{1} & & \end{array}$$

wobei wir beachten, dass mit R' auch $R'[t]$ ein Integritätsbereich ist. Sei nun $T := \mathrm{Quot}((\mathrm{Quot}(R))[t])$.

Nach der universellen Eigenschaft des Polynomrings existiert genau ein Ringhomomorphismus

$$\begin{aligned} f = \mathrm{ev}_{\tilde{t}} \colon R[t] &\longrightarrow T \\ \sum_{i=0}^{\infty} b_i t^i &\longmapsto \sum_{i=0}^{\infty} \varphi(b_i)\tilde{t}^i \end{aligned}$$

wobei

$$\tilde{t} = \frac{1_{\mathrm{Quot}(R)} \cdot t}{1} \in T$$

Für $p(t) \neq 0$ ist klar, dass $f(p(t))$ nicht 0, also eine Einheit ist, da T ein Körper ist. Nach Satz 11.1 existiert genau ein Ringhomomorphismus $\hat{f} \colon \mathrm{Quot}(R[t]) \to T$ mit $\hat{f}\left(\frac{g_1}{g_2}\right) = f(g_1)(f(g_2))^{-1}$. Man kann zeigen, dass $\hat{f}$ ein Ringisomorphismus ist, indem man die inversen Abbildungen angibt.

Also erhalten wir $\mathrm{Quot}(R[t]) \xrightarrow{\sim} \mathrm{Quot}((\mathrm{Quot}(R))[t]) = T$, einen Isomorphismus von Ringen. Im Beispiel hier setzen wir $R = \mathbb{Z}$ und es ergibt sich

$$\begin{aligned} \mathrm{Quot}(\mathbb{Z}[t]) &\xrightarrow{\sim} \mathrm{Quot}((\mathrm{Quot}(\mathbb{Z}))[t]) \\ &= \mathrm{Quot}(\mathbb{Q}[t]) \\ &= \text{rationale Funktionen über } \mathbb{Q} \text{ in einer Variablen} \end{aligned}$$

Wir definieren $K(t_1, \ldots, t_n) \coloneqq \mathrm{Quot}(K[t_1, \ldots, t_n])$ für einen Körper K.

[13. November 2017]

[20. November 2017]

Bemerkung. Sei R ein kommutativer Ring und $S \subseteq R$ multiplikativ abgeschlossen. Falls S keine Nullteiler besitzt, dann ist

$$\begin{aligned} \mathrm{can} \colon R &\longrightarrow S^{-1}R \\ r &\longmapsto \frac{r}{1} \end{aligned}$$

injektiv. Denn sei $\mathrm{can}(r) = \mathrm{can}(r')$ mit $r, r' \in R$ Dann folgt $\frac{r}{1} = \frac{r'}{1}$, es existiert also ein $s \in S$ mit $s(r1 - r'1) = 0$. Da S keine Nullteiler enthält, ist $r1 - r'1 = 0$, und wir erhalten $r' = r$. Insbesondere können wir R als Unterring von $S^{-1}R$ vermöge can auffassen.

12. Satz von Gauß

Ziel dieses Kapitels:

Satz 12.1 (Satz von Gauß)**.** *Der Polynomring eines faktoriellen Ringes ist faktoriell.*

Genauer: *Sei R ein faktorieller Ring. Dann ist $R[t]$ faktoriell und die irreduziblen Elemente sind bis auf Einheiten in R genau die*

(a) irreduziblen Elemente in $R \subseteq R[t]$ und die

(b) Elemente $p(t) \in R[t]$, die irreduzibel in $\mathrm{Quot}(R)[t]$ und primitiv (siehe Definition 12.1) sind.

Korollar 12.2. *Sei K ein Körper. Dann ist $K[t_1, \ldots, t_n]$ faktoriell. Ebenso ist $\mathbb{Z}[t_1, \ldots, t_n]$ faktoriell (aber kein Hauptidealring, vgl. Übungungsblatt 5).*

Beweis. K und $\mathbb{Z}$ sind beide Hauptidealringe, weshalb K und $\mathbb{Z}$ nach Satz 8.4 also faktoriell sind. Laut Satz von Gauss sind damit $K[t_1]$ und $\mathbb{Z}[t_1]$ faktoriell. Durch iterative Anwendung folgt die Aussage. □

Beispiel 1. $p(t) = 2t$ ist irreduzibel in $\mathbb{Q}[t] = \mathrm{Quot}(\mathbb{Z})[t]$ (da für $p(t) = bc$ in $\mathbb{Q}[t]$ schon $\deg(b) = 0$ oder $\deg(c) = 0$ gilt und damit b oder c eine Einheit in $\mathbb{Q}$ ist).

Aber: $p(t)$ ist nicht irreduzibel in $\mathbb{Z}[t]$, da $p(t) = 2 \cdot t$ und $2, t \notin \mathbb{Z}[t]^\times$. (Einfaches Argument über den Grad der Polynome)

Definition 12.1. Sei R ein faktorieller Ring. Dann heißt $p(t) = \sum_{i=0}^{n} a_i t^i$ mit $n = \deg(p(t))$ primitiv, falls kein $r \in R \setminus R^\times$ existiert, welche alle a_i mit $1 \leq i \leq n$ teilt.

Beispiel 2. $2t^2 + 4t^3 \in \mathbb{Z}[t]$ ist nicht primitiv (man wähle $r = 2$), dafür aber in $\mathbb{Q}[t]$.

Lemma 12.3 (Lemma von Gauß)**.** *Sei R ein faktorieller Ring sowie $P, Q \in R[t]$ primitiv. Dann folgt, dass $PQ \in R[t]$ primitiv ist.*

Beweis. Wir nehmen an, dass $PQ \in R[t]$ nicht primitiv ist. Dann existiert ein $r \in R \setminus R^\times$ mit $r \mid PQ$. Sei ohne Beschränkung der Allgemeinheit r prim. Betrachte $R/(r)$. Da r prim ist, ist (r) ein Primideal. Folglich ist $R/(r)$ ein Integritätsbereich, also insbesondere nullteilerfrei.

Betrachte nun $\overline{PQ} \in R/(r)[t]$ (Polynome mit Koeffizienten modulo (r)). Dann gilt $\overline{PQ} = \overline{0} \in R/(r)[t]$, da r das Polynom PQ teilt. Da $\overline{PQ} = \overline{P}\,\overline{Q}$ ist, folgt damit $\overline{P}\,\overline{Q} = \overline{0}$. Da $R/(r)$ nullteilerfrei ist, ist $\overline{P} = 0$ oder $\overline{Q} = 0$ und damit P nicht primitiv oder Q nicht primitiv. Das ist ein Widerspruch zur Annahme. □

Lemma 12.4. *Sei R ein faktorieller Ring, $K = \mathrm{Quot}(R)$ und $f \in R[t]$ primitiv. Wenn f irreduzibel in $K[t]$ ist, ist f auch irreduzibel in $R[t]$.*

Beweis. Sei $f = bc$ in $R[t]$. Es ist zu zeigen, dass b oder c eine Einheit in $R[t]$ ist. Es gilt $f = bc$ auch in $K[t]$. Nach Voraussetzung ist f irreduzibel in $K[t]$. Also ist b oder $c \in K[t]^\times = K^\times$. Ohne Beschränkung der Allgemeinheit gelte $b \in K^\times$, also $b \neq 0$ (da K ein Körper ist) und da nach Voraussetzung $b \in R[t]$ ist, folgt $b \in R \setminus \{0\}$. Da R faktoriell ist, ist $b = \varepsilon p_1 \ldots p_r$, wobei $\varepsilon \in R^\times$ und die $p_i \in R$ irreduzibel für alle $1 \leq i \leq r$ mit einem geeigneten $r \in \mathbb{N}_0$ sind.

Aus der Tatsache, dass f primitiv ist, folgt, dass b primitiv ist und somit $b = \varepsilon$ (weil sonst die Primfaktoren Teiler von b wären). Damit ist b eine Einheit in R und $f \in R[t]$ ist irreduzibel. □

Beweis des Satzes von Gauß.

Elemente der Form (a) und (b) sind irreduzibel. Für (b) ist dies nach Lemma 12.4 klar. Für (a): Sei $r \in R$ irreduzibel und $r = bc$ in $R[t]$. Es bleibt b oder $c \in R[t]^\times$ zu zeigen. Da R nullteilerfrei ist, gilt $\deg(b) = 0 = \deg(c)$, also $b, c \in R$. Weil $r \in R$ irreduzibel ist, folgt $b \in R^\times$ oder $c \in R^\times$.

Existenz einer Primfaktorzerlegung. Sei $K = \mathrm{Quot}(R)$. Da K ein Körper ist, folgt mit Übungsblatt 5, dass $K[t]$ ein Hauptidealring ist, welcher nach Satz 8.4 faktoriell ist. Sei $0 \neq f \in R[t] \subseteq K[t]$, so existiert eine Primfaktorzerlegung mit $f = \varepsilon p_1 \dots p_r$ in $K[t]$ mit $\varepsilon \in K[t]^\times = K^\times$ und irreduziblen $p_1, \dots, p_r \in K[t]$.

Wir wählen für $1 \leq i \leq r$ Elemente $c_i \in K$, sodass $p_i = c_i \tilde{p}_i$ mit primitiven $\tilde{p}_i \in R[t]$ ist („Hauptnenner“). Ist $c := c_1 \dots c_r \varepsilon$, so gilt $f = c\tilde{p}_1 \dots \tilde{p}_r$, wobei $\tilde{p}_1 \dots \tilde{p}_r$ nach dem Lemma von Gauss primitiv ist. Daraus folgt $c \in R$.

Da R faktoriell ist, gilt $c = \eta q_1 \dots q_s$ mit $\eta \in R^\times$ und irreduziblen $q_1, \dots, q_2 \in R$. Also ist $f = \eta q_1 \dots q_s \tilde{p}_1 \dots \tilde{p}_r$, wobei $q_1, \dots q_s$ Faktoren von Typ (a) und $\tilde{p}_1, \dots, \tilde{p}_r$ Faktoren von Typ (b) sind. Folglich existiert eine Primfaktorzerlegung

Typ (a) und Typ (b) sind genau die irreduziblen Elemente in $R[t]$ (bis auf Einheiten). Sei $p \in R[t]$ irreduzibel. Dann existiert ein $\varepsilon \in R[t]^\times = R^\times$ und irreduzible $p_1, \dots, p_r \in R[t]$ vom Typ (a) oder (b), sodass $p = \varepsilon p_1 \dots p_r$, da die Primfaktorzerlegung existiert. Da p irreduzibel ist, gilt $p = p_i$ für ein i bis auf Einheiten.

Eindeutigkeit der Primfaktorzerlegung (bis auf Einheiten). Seien $p = \eta q_1 \dots q_s \tilde{p}_1 \dots \tilde{p}_r$ und $p = \eta' q'_1 \dots q'_{s'} \tilde{p}'_1 \dots \tilde{p}'_{r'}$ zwei Primfaktorzerlegungen wie oben. Weil $K[t]$ faktoriell ist, gilt dann $\eta q_1 \dots q_s, \eta' q'_1 \dots q'_{s'} \in K[t]^\times$ und somit $r = r'$, und es existiert ein $\gamma_i \in K[t]^\times = K^\times$ für jedes i mit $1 \leq i \leq r$ und $\pi \in S_r$, sodass $\tilde{p}'_{\pi(i)} = \gamma_i \tilde{p}_i$. Da $\tilde{p}_i$ primitiv und $\tilde{p}'_i \in R[t]$ ist, gilt $\gamma_i \in R$ für alle i. Also existiert ein $\gamma = \gamma_1 \dots \gamma_r$, sodass $\eta\gamma q_1 \dots q_s = \eta' q'_1 \dots q'_{s'}$ ist.

Dabei sind alle Terme in R, und da R faktoriell ist, gilt $s = s'$ und die Zerlegung ist „eindeutig“. Folglich ist die Zerlegung insgesamt „eindeutig“. □

Satz 12.5 (Eisensteinsches Irreduzibilitätskriterium)**.** *Sei $f = \sum_{i=1}^n a_i t^i \in \mathbb{Z}[t]$ primitiv sowie $\deg(f) = n > 0$. Es sei $p \in \mathbb{Z}$ eine Primzahl, für die Folgendes gilt:*

$$p \nmid a_n \qquad p \mid a_i \text{ für } 0 \leq i \leq n-1 \qquad p^2 \nmid a_0$$

Existiert ein solches p, dann ist f irreduzibel in $\mathbb{Z}[t]$ und somit auch in $\mathbb{Q}[t]$.

Beweis. Sei $f = gh$ mit $g, h \notin \mathbb{Z}[t]^\times$, also $\deg(g) > 0$, $\deg(h) > 0$, da f primitiv ist. Sei $g = \sum_{i=0}^m b_i t^i$, $h = \sum_{i=0}^s c_i t^i$ mit $m, s > 0$, $m + s = n$. Dann gilt $a_n = b_m c_s$, also $p \nmid b_m, p \nmid c_s$, sowie $a_0 = b_0 c_0$, also $p \nmid b_0$ oder $p \nmid c_0$. Ohne Beschränkung der Allgemeinheit gelte $p \mid b_0$ und $p \nmid c_0$. Sei t maximal mit $p \mid b_j$ für alle $0 \leq j \leq t$. Es gilt $0 \leq t < m$.

Nun gilt $a_{l+1} = b_0 c_{l+1} + b_1 c_l + b_2 c_{l-1} + \dots + b_{l+1} c_0$. Dabei werden alle bis auf den letzten Summanden von p geteilt und $b_{l+1} c_0$ wird nicht von p geteilt. Damit teilt p nicht

a_{l+1}. Nach Voraussetzung muss also $l+1=n$ gelten. Folglich $m=n$ und damit $s=0$. Das ist ein Widerspruch. Damit gilt das Eisensteinsche Irreduzibilitätskriterium. □

[20. November 2017]
[23. November 2017]

13. Kreisteilungspolynome

Anwendung 13.1. *Sei p prim. Dann ist $\Phi_p(t) \coloneqq t^{p-1}+\cdots+t+1$ irreduzibel in $\mathbb{Z}[t]$. Wir nennen $\Phi_p(t)$ das p-te Kreisteilungspolynom.*

Beweis. Wir betrachten

$$\begin{aligned} f = \mathrm{ev}_{t+1} : \mathbb{Z}[t] &\longrightarrow \mathbb{Z}[t] \\ p(t) &\longmapsto p(t+1), \end{aligned}$$

was ein Ringhomomorphismus mit der inversen Abbildung ev_{t-1} ist. Jeder Ringhomomorphismus φ bildet Einheiten auf Einheiten ab. Falls φ ein Ringisomorphismus ist, gilt, dass für $\varphi : R \to R'$ ein $x \in R$ genau dann irreduzibel ist, wenn $\varphi(x) \in R$ irreduzibel ist. *Begründung:* Sei $x \in R$ irreduzibel und $\varphi(x) = b \cdot c$. Dann ist $\varphi^{-1}(\varphi(x)) = \varphi^{-1}(b)\varphi^{-1}(c)$, da φ^{-1} existiert. Also gilt $x = \varphi^{-1}(b)\varphi^{-1}(c)$ und damit ist $\varphi^{-1}(b)$ oder $\varphi^{-1}(c)$ eine Einheit. Deshalb ist bereits b oder c eine Einheit und somit folgt die Behauptung.

Es reicht nun zu zeigen, dass $f(\Phi_p(t))$ irreduzibel in $\mathbb{Z}[t]$ ist. Es gilt, dass $\Phi_p(t)\cdot(t-1) = t^p-1$.

$$\begin{aligned} &\Rightarrow f(\Phi_p(t)) \cdot f(t-1) = f(t^p-1) \\ &\Rightarrow f(\Phi_p(t)) \cdot t = (t+1)^p - 1 = t^p + \binom{p}{1} t^{p-1} + \cdots + \binom{p}{p-1} t + \binom{p}{p} 1 - 1 \\ &\Rightarrow f(\Phi_p(t)) = t^{p-1} + \binom{p}{1} t^{p-2} + \cdots + \binom{p}{p-1} t^0 = a_{p-1}t^{p-1} + a_{p-2}t^{p-2} + \cdots + a_0 t^0 \end{aligned}$$

Nun gilt $p \nmid a_{p-1}$ und $p \mid a_i$ für $0 \le i \le p-2$ und $p^2 \nmid a_0$. Somit sind die Kriterien für das Eisensteinsche Irreduzibilitätskriterium erfüllt. Folglich ist $f(\Phi_p(t)) \in \mathbb{Z}[t]$ irreduzibel. Damit ist auch $\Phi_p(t)$ irreduzibel. □

Anschauliche Interpretation von $\Phi_p(t)$. Wir betrachten das Polynom $t^n - 1 \in \mathbb{C}[t]$ mit $n \in \mathbb{N}$. Die Nullstellen sind dann genau die komplexen Zahlen $z \in \mathbb{C}$ mit $z^n = 1$, also die n-ten Einheitswurzeln.

Wir erhalten also „gleichverteilte“ Punkte auf dem Einheitskreis mit $(0,1) = \zeta_0$. Wir nennen ζ primitive n-te Einheitswurzel, falls $\zeta^n = 1$ und $\zeta^m \neq 1$ für alle $m > n$ ($m \in \mathbb{N}$) gilt. Insbesondere ist dann $n = \mathrm{ord}(\zeta)$ bezüglich der Multiplikation.

Definition 13.1. Für $d \in \mathbb{N}$ definieren wir

$$\Phi_d(t) = \prod_{\substack{z \text{ primitive } d\text{-te} \\ \text{Einheitswurzel} \neq 1}} (t - z)$$

als das d-te Kreisteilungspolynom.

Bemerkung. $\Phi_d(t) = \Phi_p(t)$ wie oben, falls d eine Primzahl ist.

Wir wissen, dass $\Phi_p(t) \in \mathbb{Z}[t]$ irreduzibel ist, falls p eine Primzahl und primitiv ist. Nach dem Satz von Gauss ist deshalb auch $\Phi_p(t) \in \mathbb{Q}[t] = \mathrm{Quot}(\mathbb{Z})[t]$ irreduzibel. Deshalb folgt nach Lemma 8.1, dass das von $\Phi_p(t)$ erzeuge Ideal $I := (\Phi_p(t))$ maximal unter den Hauptidealen in $\mathbb{Q}[t]$ ist. Da $\mathbb{Q}[t]$ ein Hauptidealring ist (siehe Übungsblatt 5), ist I auch ein maximales Ideal. Deshalb ist $\mathbb{Q}[t]/I =: K_p$ ein Körper, auch der p-te Kreisteilungskörper genannt.

Lemma 13.2. *Sei K ein Körper und $R \neq \{0\}$ ein kommutativer Ring. Sei $\varphi : K \to R$ ein Ringhomomorphismus. Dann ist φ injektiv.*

Beweis. Wir wissen, dass $\varphi(1) = 1 \neq 0$. Sei $\ker \varphi \neq \{0\}$. Dann existiert ein $a \in K$, welches im Kern liegt, sodass $1 = a^{-1} \cdot a$, was auch im Kern liegt, da $\ker \varphi$ ein Ideal ist. Dann wäre aber $\varphi(1) = 0$, was ein Widerspruch ist. Insbesondere können wir K vermöge φ als Teilmenge von R auffassen. □

Deshalb können wir $\mathbb{Q}$ als Teilmenge von K_p vermöge der (injektiven) Einbettung

$$\mathbb{Q} \hookrightarrow \mathbb{Q}[t] \xrightarrow{\text{can}} \mathbb{Q}[t]/(\Phi_p(t))$$

auffassen. K_p ist dadurch ein $\mathbb{Q}$-Vektorraum (nachrechnen!).

Lemma 13.3. *Sei p prim. Dann ist K_p ein $(p-1)$-dimensionaler $\mathbb{Q}$-Vektorraum.*

Beweis. Wir wollen zeigen, dass

$$B = \left\{\overline{1}, \overline{t}, \overline{t}^2, \ldots, \overline{t}^{p-2}\right\}$$

eine Basis ist.

Erzeugendensystem. Es reicht zu zeigen, dass $\overline{t}^k \in \mathrm{Span}_{\mathbb{Q}}(B)$ für $k \in \mathbb{N}_0$, damit B ein Erzeugendensystem ist.

1. Für $0 \leq k \leq p-2$ ist das klar.
2. Sei $k = p - 1$.

$$\begin{aligned} \overline{t}^{p-1} &= \overline{t}^{p-1} - \underbrace{\left(\overline{t}^{p-1} + \cdots + \overline{t} + \overline{1}\right)}_{\overline{0} \in K_p} \\ &= -\overline{t}^{p-2} + \cdots - \overline{t} - \overline{1} \in \mathrm{Span}_{\mathbb{Q}}(B) \end{aligned}$$

3. Sei $k > p-1$.

$$\begin{aligned}\overline{t}^k &= \overline{t} \cdot \overline{t}^{k-1} \in \overline{t} \cdot \mathrm{Span}_{\mathbb{Q}}(B) \\ &\subseteq \mathrm{Span}_{\mathbb{Q}} \left\{\overline{t}, \overline{t}^2, \cdots, \overline{t}^{p-1}\right\} \\ &\subseteq \mathrm{Span}_{\mathbb{Q}}(B)\end{aligned}$$

Somit ist B ein Erzeugendensystem.

Lineare Unabhängigkeit. Sei $\sum_{i=0}^{p-2} a_i \overline{t}^i = \overline{0}$ in K_p mit $a_i \in \mathbb{O}$. Wir betrachten $Q(X) \coloneqq \sum_{i=0}^{p-2} a_i X^i \in \mathbb{Q}[X]$. Es ist klar, dass $Q(t) \in \mathbb{Q}[t]$ und $Q(t) \in K_p$. Wir wissen, dass

$$\overline{0} = \sum_{i=0}^{p-2} a_i \overline{t}^i = \overline{\sum_{i=0}^{p-2} a_i t^i} = \overline{Q(t)}$$

Dann liegt $Q(t)$ in $I = \Phi_p(t)$ und folglich gilt $\Phi_p(t) \mid Q(t)$. Es folgt also, dass $\deg(Q(t)) \geq p-1$ oder $Q(t) = 0$, wobei ersteres ein Widerspruch zur Definition ist. Folglich gilt $Q(t) = 0$, womit alle $a_i = 0$ und B ist damit linear unabhängig. □

Wir betrachten

$$G \coloneqq \left\{\varphi : K_p \to K_p \,\middle|\, \begin{smallmatrix}\varphi \text{ ist Ringisomorphimus} \\ \text{und } \mathbb{Q}\text{-linear, } \varphi|_{\mathbb{Q}} = \mathrm{id}_{\mathbb{Q}}\end{smallmatrix}\right\}.$$

G ist eine Gruppe bezüglich der Komposition von Abbildungen. Man nennt G die Galoisgruppe $\mathrm{Gal}(K_p /\!\!/ \mathbb{Q})$ von K_p über $\mathbb{Q}$. Es gilt, dass $\varphi(\overline{1}) = \overline{1}$. Falls $\varphi(\overline{t}) = z$, dann gilt $\varphi\left(\overline{t}^k\right) = z^k$, weil φ ein Ringhomomorphismus ist. Wegen Lemma 13.3 bestimmt also $\varphi(\overline{t})$ die Abbildung φ bereits eindeutig, da φ $\mathbb{Q}$-linear ist. Wir interessieren uns also nur für die Möglichkeiten für z.

Lemma 13.4. *Sei $\varphi \in G$ sowie $a_i \in \mathbb{Q}$ für alle (endlich viele) i. Sei weiterhin*

$$P(X) = \sum_{i \geq 0} a_i X^i \in K_p[X].$$

Falls y eine Nullstelle von $P(X)$ in K_p ist, dann ist auch $\varphi(y)$ mit $\varphi \in G$ eine Nullstelle von $P(X)$.

Beweis. Sei y eine Nullstelle von $P(X)$. Dann ist $\sum_{i \geq 0} a_i y^i = 0$ in K_p. Folglich gilt

$$0 = \varphi(0) = \varphi\left(\sum_{i \geq 0} a_i y^i\right) = \sum_{i \geq 0} \varphi(a_i)\varphi(y^i) = \sum_{i \geq 0} a_i \varphi(y)^i$$

Somit ist $\varphi(y)$ eine Nullstelle. □

Nun ist $\overline{t}$ eine Nullstelle von $X^p - 1 \in K_p[X]$, weil $X^p - 1 = \Phi_p(X) \cdot (X-1)$ und $\Phi_p(\overline{t}) = 0$ in K_p gilt. Damit ist $\varphi(\overline{t})$ eine Nullstelle von $X^p - 1$ falls $\varphi \in G$.

Andererseits ist $\overline{t}^k$ für $0 \leq k \leq p-1$ eine Nullstelle von $X^p - 1$, weil

$$\left(\overline{t}^k\right)^p = \left(\overline{t}^p\right)^k = \overline{1} = 1 \in K_p$$

gilt. Die $\overline{t}^k$ für $0 \leq k \leq p-2$ sind paarweise verschieden, da sie linear unabhängig sind.

Somit definiert die Zuordnung $\overline{t} \mapsto \overline{t}^k$ für $0 \leq k \leq p-2$ dann $p-1$ paarweise verschiedene Elemente in G. Nach Lemma 13.4 gibt es aber höchstens p Nullstellen, also $|G| \leq p$.

Also hat G genau die Elemente gegeben durch

$$\varphi(\overline{t}) = \overline{t}^k \quad \text{für } 1 \leq k \leq p-2,$$

weil $\varphi(\overline{t}) = \overline{t}^0 = 1$ und $\varphi(\overline{1}) = \overline{1} = 1$ unmöglich sind.

Zusammenfassend ist G endlich und permutiert die Nullstellen von $X^p - 1$. Wir werden zeigen:

$$\mathrm{Gal}(K_p /\!\!/ \mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^\times$$

III. Körpertheorie

14. Körpererweiterungen

Definition 14.1. Es seien K und K' Körper. Dann heißt $\varphi : K \to K'$ Körperhomomorphismus bzw. Körperisomorphismus, falls φ ein Ringhomomorphismus bzw. ein Ringisomorphismus ist.

Definition 14.2. Es sei K ein Körper. Dann heißt $L \subseteq K$ Unterkörper, falls L ein Unterring ist und für alle Elemente $x \in L$ das Inverse x^{-1} bezüglich x in L liegt. Äquivalent dazu ist, dass L ein Körper mit den von K eingeschränkten Verknüpfungen ist.

Bemerkung. Beliebige Schnitte von Unterkörpern sind Unterkörper.

Definition 14.3. Sei K ein Körper sowie $N \subseteq K$ eine Teilmenge von K. Dann ist

$$\langle N \rangle_{\text{Körper}} := \bigcap_{\substack{L \subseteq K \text{ Unterkörper} \\ N \subseteq L}} L$$

der von N erzeugte Unterkörper. Insbesondere heißt

$$\langle \emptyset \rangle_{\text{Körper}} = \bigcap_{L \subseteq K \text{ Unterkörper}} L$$

der Primkörper von K.

[23. November 2017]

[27. November 2017]

Bemerkung. Der Primkörper eines Körpers ist selbst ein Körper und zwar der kleinste Unterkörper von K. Es ist $0, 1 \in \langle \emptyset \rangle$ und damit auch $1 + \cdots + 1 \in \langle \emptyset \rangle$ als die n-fache Addition der 1 ($n \in \mathbb{N}$).

Satz 14.1. *Sei K ein Körper. Dann ist der Primkörper von K isomorph (als Körper) zu*

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

Beweis. Betrachte $\varphi\colon \mathbb{Z} \to K$ mit

$$\varphi(n) = \begin{cases} n \cdot 1 & \text{falls } n \in \mathbb{N}, \\ 0 & \text{falls } n = 0, \\ -(-n \cdot 1) & \text{falls } -n \in \mathbb{N}, \end{cases}$$

wobei klar ist, dass φ ein Ringhomomorphismus ist und das Bild von φ im Primkörper von K liegt.

Fall 1: $\operatorname{char} K = p > 0$. Dann liegt $p \cdot 1 = 0$ in K, es gilt also $\varphi(pm) = 0$ für alle $m \in \mathbb{Z}$, also folgt $p\mathbb{Z} \subseteq \ker \varphi$. Nun existiert nach dem Homomorphiesatz ein Ringhomomorphismus $\overline{\varphi}\colon \mathbb{Z}/p\mathbb{Z} \to K$ mit $\overline{\varphi} \circ \mathrm{can} = \varphi$. Da p prim ist, ist $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ ein Körper. Nach Lemma 13.2 ist $\overline{\varphi}$ folglich injektiv und $\operatorname{im} \overline{\varphi}$ ist im Primkörper von K enthalten, wobei $\operatorname{im} \overline{\varphi} \cong \mathbb{F}_p$ nach dem Homomorphiesatz. Weil der Primkörper der kleinste Unterkörper von K ist und $\operatorname{im} \overline{\varphi}$ ein Körper (isomorph zu $\mathbb{F}_p$) ist, ist $\operatorname{im} \overline{\varphi}$ der Primkörper von K.

Fall 2: $\operatorname{char} K = 0$. Dann ist φ injektiv, denn aus $\varphi(n) = \varphi(m)$ folgt $(n-m)1 = 0$ in K, also gilt $n = m$ oder $\operatorname{char} K > 0$, wobei letzteres aber nicht der Fall ist. Also ist $\varphi(n) \neq 0$ für alle $n \neq 0$, da φ ein Gruppenhomomorphismus ist. Damit gilt $\varphi(n) \in K^\times$ für alle $n \in \mathbb{Z} \setminus \{0\}$. Nach der universellen Eigenschaft der Lokalisierung existiert ein Ringhomomorphismus $\hat{\varphi}\colon \mathbb{Q} = \operatorname{Quot}(\mathbb{Z}) \to K, \frac{a}{b} \mapsto \varphi(a)(\varphi(b))^{-1}$. Mit Lemma 13.2 folgt dann, dass $\hat{\varphi}$ injektiv ist, und weiter gilt nach dem Homomorphiesatz $\mathbb{Q}/\ker \hat{\varphi} \cong \operatorname{im} \hat{\varphi}$, also $\mathbb{Q} \cong \operatorname{im} \hat{\varphi}$ (Isomorphie von Ringen bzw. Körpern). Wir wissen, dass $\operatorname{im} \varphi$ im Primkörper von K enthalten ist. Nach Definition von $\hat{\varphi}$ liegt auch $\operatorname{im} \hat{\varphi}$ im Primkörper von K, weil der Primkörper ein Körper ist. Damit haben wir nun einen Unterkörper $\operatorname{im} \hat{\varphi}$ als Teilmenge des Primkörpers von K, also ist $\operatorname{im} \hat{\varphi}$ der Primkörper, weil dieser minimal ist. Also ist $\mathbb{Q}$ isomorph zum Primkörper von K. □

Definition 14.4. Eine Körpererweiterung $L \mathbin{/\!\!/} K$ ist ein Paar L, K von Körpern, wobei $K \subseteq L$ ein Unterkörper von L ist. Genauer: L ist eine Körpererweiterung von K.

Beispiel 1.

1. $\mathbb{C} \mathbin{/\!\!/} \mathbb{R}$ ist eine Körpererweiterung.
2. Sei $L \mathbin{/\!\!/} K$ eine Körpererweiterung und seien $\alpha_1, \ldots, \alpha_n \in L$. Sei $M \coloneqq K \cup \{\alpha_1, \ldots, \alpha_n\}$ Dann sind $K \subseteq \langle M \rangle_{\text{Körper}} \subseteq L$ jeweils Körpererweiterungen. Wir bezeichnen $\langle M \rangle_{\text{Körper}} = K(\alpha_1, \ldots, \alpha_n)$ den von K und $\alpha_1, \ldots, \alpha_n$ erzeugten Unterkörper von L.

Beachte: $K \subseteq K[\alpha_1, \ldots, \alpha_n] \subseteq K(\alpha_1, \ldots, \alpha_n) \subseteq L$; wobei die erste Inklusion eine Inklusion von Ringen ist und die zweite im Allgemeinen tatsächlich echt ist. Die letzte Inklusion ist eine Inklusion von Körpern.

Beispiel 2.

1. $\mathbb{R} \subseteq \mathbb{R}[i] = \{a + bi \mid a, b \in \mathbb{R}\} = \mathbb{R}(i) = \mathbb{C}$
2. $\mathbb{R} \subsetneq \mathbb{R}[t] \subsetneq \mathbb{R}(t) \subsetneq \mathbb{C}(t)$

Definition 14.5. Eine Körpererweiterung $L /\!\!/ K$ heißt endlich erzeugt, falls $\alpha_1, \ldots, \alpha_n \in L$ existieren, sodass $L = K(\alpha_1, \ldots, \alpha_n)$. $L /\!\!/ K$ heißt einfach (oder auch primitiv), falls ein $\alpha \in L$ mit $L = K(\alpha)$ existiert.

Definition 14.6. Sei $L /\!\!/ K$ eine Körpererweiterung. Dann ist L ein K-Vektorraum (in offensichtlicher Weise; siehe Abschnitt 13). Wir nennen $\dim_K L = [L : K]$ den Grad der Körpererweiterung $L /\!\!/ K$.

Beispiel 3. $\mathbb{C} /\!\!/ \mathbb{R}$: $[\mathbb{C} : \mathbb{R}] = 2$; $\mathbb{R}(t) /\!\!/ \mathbb{R}$: $[\mathbb{R}(t) : \mathbb{R}] = \infty$.

Bemerkung. Falls L ein endlicher Körper sowie $L /\!\!/ K$ eine Körpererweiterung ist, so gilt $|L| = |K|^{[L:K]}$.

Satz 14.2. *Sei $L /\!\!/ K$ eine Körpererweiterung und V ein L-Vektorraum. Dann ist V durch Einschränkung der Verknüpfungen auch ein K-Vektorraum. Es gilt* $\dim_K V = \dim_L V \cdot [L : K]$.

Korollar 14.3 (Gradformel)**.** *Seien $L_1 /\!\!/ L_2$ und $L_2 /\!\!/ L_3$ Körpererweiterungen. Dann gilt*

$$[L_1 : L_3] = [L_1 : L_2] \cdot [L_2 : L_3]$$

Beweis. Folgt direkt aus Satz 14.2. □

Beweis von Satz 14.2. Sei $\{v_i \mid i \in I\}$ eine Basis von V als L-Vektorraum und $\{w_j \mid j \in J\}$ eine Basis von L als K-Vektorraum. Wir zeigen nun, dass $\{z_{(i,j)} = w_j v_i \mid i \in I, j \in J\}$ eine Basis von V als K-Vektorraum ist. Damit folgt dann der Satz.

Erzeugendensystem. Sei $v \in V$, so existiert eine Darstellung $v = \sum_{i \in I} a_i v_i$ mit $a_i \in L$, wobei nur endliche viele $a_i \neq 0$ sind, und für festes $i \in I$ gilt außerdem

$$a_i = \sum_{j \in J} b_{ij} w_j \text{ mit } b_{ij} \in K$$

wobei wieder nur endlich viele $b_{ij} \neq 0$ sind. Nun gilt aber $v = \sum_{i \in I} \sum_{j \in J} b_{ij} w_j v_i$, und wir sind fertig.

Lineare Unabhängigkeit. Sei $\sum_{(i,j) \in I'} c_{ij} z_{(i,j)} = 0$ mit $c_{ij} \in K$ und endlichem $I' \subseteq I \times J$. Es ist zu zeigen, dass $c_{ij} = 0$ für alle $(i, j) \in I'$ gilt.

Wir setzen $c_{ij} = 0$ für alle $(i,j) \in (I \times J) \setminus I'$. Nun folgt

$$0 = \sum_{(i,j)\in I'} c_{ij} z_{(i,j)} = \sum_{i\in I} \left(\sum_{j\in J} (c_{ij} w_j) \right) v_i,$$

also $c_{ij} w_j \in L$, weil $K \subseteq L$ ein Unterkörper ist. Da $\{v_i \mid i \in I\}$ eine Basis von V als L-Vektorraum ist, folgt $\sum_{j\in J} c_{ij} w_j = 0$ für alle $i \in I$. Da weiterhin $\{w_j \mid j \in J\}$ linear unabhängig über K ist, gilt $c_{ij} = 0$ für alle $i \in I$ und $j \in J$. □

15. Algebraische Körpererweiterung

Sei $L \mathbin{/\!/} K$ eine Körpererweiterung sowie $a \in L$. Die Inklusion $K \to L, \lambda \mapsto \lambda$ ist ein Ringhomomorphismus. Nach der universellen Eigenschaft des Polynomrings existiert genau ein Ringhomomorphismus

$$\begin{aligned} \mathrm{ev}_a \colon K[t] &\longrightarrow L \\ p(t) &\longmapsto p(a). \end{aligned}$$

Wir nennen a transzendent über K, falls ev_a injektiv ist, und algebraisch anderenfalls. Betrachte nun diese beiden Fälle.

Fall 1: a ist transzendent. Dann ist $\mathrm{ev}_a \colon K[t] \to L$ injektiv und nach Satz 7.15 gilt $\operatorname{im} \mathrm{ev}_a = K[a] \subseteq L$. Also existiert ein Isomorphismus von Ringen $K[t] \to K[a]$ nach dem Homomorphiesatz. Nach Definition ist $K[a] \subseteq K(a)$ und somit gilt

$$K(a) \supseteq \{ f g^{-1} \mid f, g \in K[a], g \neq 0 \} =: X.$$

Da $K(a)$ der kleinste Unterkörper von L ist, der K und a enthält und X offensichtlich ein Körper ist, folgt Gleichheit.

Folglich erhalten wir einen Isomorphismus von Ringen (bzw. Körpern) von $K(a) \cong K(t) = \mathrm{Quot}(K[t])$. Insbesondere sind $K(t)$, also auch $K(a)$ unendlichdimensionale als K-Vektorräume, also $[K(a) : K] = \infty$.

Fall 2: a ist algebraisch über K. Nach Definition ist ev_a nicht injektiv. Also gilt, dass $\ker(\mathrm{ev}_a) \neq \{0\}$ ein Ideal in $K[t]$ ist. Da $K[t]$ ein Hauptidealring ist, existiert ein $p(t) \in K[t]$ mit $\ker(\mathrm{ev}_a) = (p(t))$. Sei ohne Beschränkung der Allgemeinheit $p(t)$ normiert (d.h. der Leitkoeffizient ist 1).

Wir wissen, dass $p(a) = \mathrm{ev}_a(p(t)) = 0$, also dass a eine Nullstelle von $p(t)$ ist. Wähle nun ein normiertes Polynom minimalen Grades in $K[t]$, genannt $m_a(t)$, sodass $m_a(a) = 0$, also sodass eine Nullstelle ist. Wir nennen m_a das Minimalpolynom zu a (Existenz und Eindeutigkeit zeigt man wie für das Minimalpolynom in LA II). Ebenfalls wie in LA II zeigt man, dass $m_a(t)$ jedes Polynom $p(t) \in K[t]$ mit $p(a) = 0$ teilt. Damit folgt, dass $\ker \mathrm{ev}_a = (m_a(t))$ ist.

Vermöge des Homomorphiesatz erhalten wir schließlich einen Ringhomomorphismus $\overline{\mathrm{ev}_a} \colon K[t]/(m_a(t)) \to \operatorname{im}(\mathrm{ev}_a) \subset L$.

[27. November 2017]

[30. November 2017]

Dabei ist $\operatorname{im}(\operatorname{ev}_a) \subseteq L$ und L ein Körper und $\operatorname{im}(\operatorname{ev}_a)$ ein Ring. Folglich sind $\operatorname{im}\operatorname{ev}_a$ und $K[t]/(m_a(t))$ Integritätsbereiche. Damit ist $(m_a(t))$ ein Primideal und $m_a(t)$ ist prim. Da $K[t]$ ein Hauptidealring ist, ist $m_a(t)$ irreduzibel und $(m_a(t))$ maximal unter allen Hauptidealen; folglich ist $(m_a(t))$ maximal und $K[t]/(m_a(t))$ ein Körper.

Da $\overline{\operatorname{ev}_a}\colon K[t]/(m_a(t)) \to \operatorname{im}\operatorname{ev}_a = K[a] \subseteq L$ ein Ringhomomorphismus und auf einem Körper definiert ist, ist $\overline{\operatorname{ev}_a}$ injektiv und $K[a]$ somit ein Körper. Also gilt $K[a] \subseteq K(a) \subseteq L$. Da $K(a)$ der kleinste Körper ist, der K und a enthält, folgt $K[a] = K(a)$.

Behauptung: $[K(a) : K] = d \coloneqq \deg(m_a(t))$. Genauer: $1, a, a^2, \dots, a^{d-1}$ ist eine Basis von $K(a)$ als K-Vektorraum.

Beweis.

Erzeugendensystem. Sei $k \geq 0$. Dann gilt $t^{d+k} = t^k m_a(t) + Q$ in $K[t]$, wobei Q eine Linearkombination von Polynomen mit Grad kleiner als $d + k$ ist. Also gilt in $K[t]/(m_a(t))$.

$$\overline{t^{d+k}} = \overline{t^k m_a(t)} + \overline{Q} = \overline{Q}.$$

Damit folgt $\overline{t^{d+k}} \in \langle\{1, \bar{t}, \dots, \overline{t^{d-1}}\}\rangle$. Folglich erzeugt $B \coloneqq \{1, \bar{t}, \dots, \overline{t^{d-1}}\}$ dann $K[t]/(m_a(t))$ als K-Vektorraum. Wende nun die Evaluationsabbildung an: $\overline{\operatorname{ev}_a}(B)$ erzeugt $\operatorname{im}\overline{\operatorname{ev}_a} = K(a)$ als K-Vektorraum, da $\overline{\operatorname{ev}_a}$ insbesondere ein K-Vektorraum-Isomorphismus ist. Da $\overline{\operatorname{ev}_a}(B) = \{1, a, a^2, \dots, a^{d-1}\}$ gilt, folgt die Aussage.

Lineare Unabhängigkeit. Sei $\sum_{i=0}^{d-1} c_i a^i = 0$ (in $K(a)$) mit $c_i \in K$. Wir nehmen an, dass ein i mit $c_i \neq 0$ existiert. Wähle m maximal mit $c_m \neq 0$. Dann ist $\sum_{i=0}^{m} c_i a^i = 0$. Sei ohne Beschränkung der Allgemeinheit $c_m = 1$. Dann wissen wir

$$0 = \sum_{i=0}^{m} c_i a^i = \overline{\operatorname{ev}_a}\left(\sum_{i=0}^{m} c_i \bar{t}^i\right) \Longrightarrow \operatorname{ev}_a\left(\sum_{i=0}^{m} c_i t^i\right) = 0.$$

Folglich hat $\sum_{i=0}^{m} c_i t^i \in K[t]$ als Nullstelle a und den Grad $m < d$ im Widerspruch zu Definition von $m_a(t)$, weil $m_a(t)$ das normierte Polynom kleinsten Grades mit a als Nullstelle ist. □

Beispiel 1. Betrachte $\mathbb{C} /\!\!/ \mathbb{R}$ und $i \in \mathbb{C}$. Dann ist $t^2 + 1 \in \mathbb{R}[t]$ das Minimalpolynom $m_i(t)$ zu i. Es gilt folglich $[\mathbb{R}(i) : \mathbb{R}] = 2$.

Satz 15.1. *Sei $L /\!\!/ K$ eine Körpererweiterung und $a \in L$. Dann sind äquivalent:*

1. *a ist algebraisch über K.*
2. *$K[a] = K(a) \subseteq L$*
3. *$\dim_K K(a) = d = \deg(m_a(t))$.*

Im letzten Fall nennen wir $d = [K(a) : K]$ den Grad von a über K.

Beweis. siehe oben □

Definition 15.1. Eine Körpererweiterung $L /\!\!/ K$ heißt algebraisch, falls jedes $a \in L$ algebraisch über K ist. Weiter heißt $L /\!\!/ K$ endlich, wenn L als K-Vektorraum endliche Dimension hat, also der Grad $[L : K]$ der Körpererweiterung endlich ist.

Satz 15.2.

1. *Jede endliche Körpererweiterung ist algebraisch.*
2. *Falls $L /\!\!/ K$ algebraisch und endlich erzeugt ist, ist $L /\!\!/ K$ endlich.*
3. *Seien $L_1 /\!\!/ L_2$ und $L_2 /\!\!/ L_3$ beide algebraisch. Dann ist auch $L_1 /\!\!/ L_3$ algebraisch (Transitivität).*

Beweis.

1. Sei $a \in L$. Dann existiert ein $m \in \mathbb{N}$, sodass $1, a, a^2, \ldots, a^m$ linear abhängig über K ist, da nach Voraussetzung $\dim_K L < \infty$ gilt. Folglich existieren $c_i \in K$ $(0 \leq i \leq m)$, die nicht alle 0 sind, mit $\sum_{i=0}^{m} c_i a^i = 0$. Also ist $\mathrm{ev}_a \colon K[t] \longrightarrow L$ nicht injektiv und a somit algebraisch über K.

2. Sei L algebraisch und endlich erzeugt über K. Dann existieren Elemente $a_1, \ldots, a_n \in L$ mit $L = K(a_1, \ldots, a_n)$. Betrachte

$$K \subseteq K(a_1) \subseteq K(a_1)(a_2) = K(a_1, a_2) \subseteq \cdots \subseteq K(a_1, \ldots, a_n) = L.$$

   Nach der Gradformel gilt

$$[L : K] = [K(a_1, \ldots, a_n) : K] = \prod_{i=1}^{n} [K(a_1, \ldots, a_i) : K(a_1, \ldots, a_{i-1})]$$

   Nach Voraussetzung ist a_i algebraisch über K, also insbesondere algebraisch über $K(a_1, \ldots, a_{i-1})$. Somit gilt $[K(a_1, \ldots, a_i) : K(a_1, \ldots, a_{i-1})] < \infty$ nach Satz 15.1. Schließlich folgt $[L : K] < \infty$.

3. Ist $a \in L_1$, so existiert ein $p(t) \in L_2[t]$ mit $p(t) \neq 0$ und $p(a) = 0$, da $L_1 /\!\!/ L_2$ algebraisch ist. Sei $p(t) = \sum_{i=0}^{n} b_i t^i$. Betrachte den Unterkörper $K = L_3(b_0, b_1, \ldots, b_n)$ von L_2. Dann ist a offensichtlich algebraisch über K, also folgt $[K(a) : K] \leq \deg(p(t)) < \infty$ nach 2; $K(a) /\!\!/ K$ ist somit endlich. Andererseits ist $L_2 /\!\!/ L_3$ algebraisch, also ist erst recht $K /\!\!/ L_3$ algebraisch.

   Nach Konstruktion ist $K /\!\!/ L_3$ endlich erzeugt; mit 2 folgt, dass $K /\!\!/ L_3$ endlich ist. Mit der Gradformel erhalten wir $[K(a) : L_3] = [K(a) : K][K : L_3]$. Somit ist $[K(a) : L_3] < \infty$, also ist a algebraisch über L_3 nach 1. Somit ist $L_1 /\!\!/ L_3$ algebraisch. □

Lemma 15.3. *Seien $L /\!\!/ K$ eine Körpererweiterung sowie $a, b \in L$ algebraisch über K. Dann sind $a+b$, $a \cdot b$, $a-b$ und ab^{-1} (falls $b \neq 0$) auch algebraisch über K.*

Beweis. Betrachte $K(a,b) = K(a)(b)$. Dann $[K(a,b) : K] = [K(a)(b) : K(a)][K(a) : K]$, wobei beide Faktoren endlich sind (der zweite ist endlich, weil a algebraisch über K ist, der erste ist endlich, weil b algebraisch über K, also insbesondere über $K(a)$ ist). Folglich ist $K(a,b) /\!\!/ K$ endlich und damit nach Satz 15.1 algebraisch. Aber $K(a,b)$ enthält $a+b$, $a-b$, ab und ab^{-1} (falls $b \neq 0$) und somit sind diese Elemente algebraisch über K. □

Bemerkung. Insbesondere bilden die algebraischen Elemente über K (in L) selbst einen Körper.

Beispiel 2.

1. Sei p eine Primzahl und $n \in \mathbb{N} \setminus \{0\}$. Dann ist $f(t) = t^n - p \in \mathbb{Q}[t]$ irreduzibel (nach dem Eisensteinschen Irreduzibilitätskriterium irreduzibel in $\mathbb{Z}[t]$ und primitiv, also irreduzibel in $\mathbb{Q}[t]$ nach dem Satz von Gauss). Sei nun $a = \sqrt[n]{p} \in \mathbb{C}$ eine Nullstelle von $f(t)$.

   Behauptung: $[\mathbb{Q}(\sqrt[n]{p}) : \mathbb{Q}] = n$. Denn nach Definition des Minimalpolynoms $m_a(t)$ gilt $m_a(t) \mid f(t)$, also $f(t) = m_a(t)q(t)$ für ein $q(t) \in \mathbb{Q}[t]$. Da $f(t)$ irreduzibel ist, folgt daraus $m_a(t)$ oder $q(t) \in \mathbb{Q}[t]^\times = \mathbb{Q}^\times$. Aber $m_a(t)$ kann keine Einheit sein; also $f(t) = m_a(t) \cdot \varepsilon$ mit $\varepsilon \in \mathbb{Q}^\times$. Da $f(t)$ aber normiert ist, folgt $\varepsilon = 1$. Mit Satz 15.1 folgt die Behauptung.

2. Betrachte $\mathbb{C} /\!\!/ \mathbb{Q}$. Sei $\mathbb{Q}^{\text{alg}} = \{a \in \mathbb{C} \mid a \text{ algebraisch über } \mathbb{Q}\}$. Nach Lemma 15.3 ist $\mathbb{Q} \subseteq \mathbb{Q}^{\text{alg}} \subseteq \mathbb{C}$ eine Körpererweiterung, nämliche der größte Unterkörper von $\mathbb{C}$, der algebraisch über $\mathbb{Q}$ ist.

   Aber $\mathbb{Q}^{\text{alg}}$ ist nicht endlich über $\mathbb{Q}$. Angenommen, $\mathbb{Q}^{\text{alg}} /\!\!/ \mathbb{Q}$ wäre endlich, also $[\mathbb{Q}^{\text{alg}} : \mathbb{Q}] = m < \infty$. Wähle nun $n > m$. Nach dem ersten Beispiel ist $\sqrt[n]{p} \in \mathbb{Q}^{\text{alg}}$ (mit p wie oben) und $[\mathbb{Q}(\sqrt[n]{p}) : \mathbb{Q}] = n > m$. Aber dann folgt $\mathbb{Q}(\sqrt[n]{p}) \subseteq \mathbb{Q}^{\text{alg}}$ und damit $[\mathbb{Q}^{\text{alg}} : \mathbb{Q}] \geq n$.

Wir haben nun folgende Frage: Mit einem Körper K und $p(t) \in K[t]$, existiert eine Körpererweiterung $L /\!\!/ K$, sodass $p(t)$ eine Nullstelle in L hat?

Satz 15.4. *Sei K ein Körper und $f(t) \in K[t]$ irreduzibel. Dann existiert eine algebraische Körpererweiterung $L /\!\!/ K$ mit $[L : K] = d = \deg(f(t))$, sodass $f(t)$ eine Nullstelle in L hat.*

Beweis. Da $f(t)$ irreduzibel ist, ist $(f(t))$ ein maximales Ideal in $K[t]$ und $K[t]/(f(t))$ somit ein Körper. Betrachte den Ringhomomorphismus

$$\begin{array}{rcl} \varphi\colon K & \longrightarrow & K[t] \longrightarrow K[t]/(p(t)) =: L \\ \lambda & \longmapsto & \text{konstantes Polynom } \lambda \end{array}$$

welcher injektiv ist, da K ein Körper ist; wir können K also als Unterkörper von L auffassen. Es gilt $L = K(\bar{t})$ mit $\bar{t} = \text{can}(t)$. Setzt man $a := \bar{t}$, so folgt $f(a) = f(\bar{t}) =$

$\overline{f(t)} = \overline{0} \in L$. Es ist $a \in L$ also eine Nullstelle von $f(t)$. Da $f(t)$ irreduzibel ist, ist $f(t) = m_a(t)\varepsilon$ für ein geeignetes $\varepsilon \in K^\times$ (siehe oben). Also gilt $[L : K] = [K(a) : K] = \deg(m_a(t)) = \deg(f(t)) = d$. □

[27. November 2017]

[4. Dezember 2017]

Bemerkung. Sei $f \in K[t]$ nicht notwendig irreduzibel. Dann können wir Satz 15.4 auf irreduzible Faktoren von f, etwa $g \in K[t]$, anwenden. Wir schreiben $f = g \cdot h$ mit $h \in K[t]$. Dann existiert eine Körpererweiterung $L \mathbin{/\!\!/} K$, sodass g in L eine Nullstelle hat, und damit auch f. Weiterhin gilt $[L : K] = \deg(g) \leq \deg(f)$.

Beispiel 3. Sei $K = \mathbb{R}$, sei $f = t^2 - 1 \in \mathbb{R}[t]$. Dann ist f nicht irreduzibel, da $f = (t-1)(t+1) = gh$ mit $g = t - 1$ und $h = t + 1 \in \mathbb{R}[t]$ gilt. Sei also $L = K = \mathbb{R}$, und wir erhalten $[L : K] = 1 = \deg(g) < 2 = \deg(f)$. Im Gegensatz dazu sei $f = t^2 + 1$ (irreduzibel in $\mathbb{R}[t]$). Mit $L = \mathbb{C}$ erhält man $[L : K] = [\mathbb{C} : \mathbb{R}] = 2 = \deg(f)$.

Satz 15.5. *Ein Körper K heißt algebraisch abgeschlossen, falls eine der folgenden äquivalenten Aussagen gilt:*

1. *Jedes Polynom $f \in K[t] \setminus K$ hat eine Nullstelle in K.*
2. *Jedes Polynom $f \in K[t] \setminus K$ ist Produkt von Polynomen von Grad 1.*
3. *Die normierten irreduziblen Polynome in $K[t]$ sind genau die Elemente der Form $t - a$ mit $a \in K$.*
4. *Falls $L \mathbin{/\!\!/} K$ eine algebraische Körpererweiterung ist, dann gilt schon $L = K$.*

Beispiel 4.

- $\mathbb{R}$ ist nicht algebraisch abgeschlossen, weil zum Beispiel $t^2 + 1$ keine Nullstelle in $\mathbb{R}$ hat.
- $\mathbb{C}$ ist algebraisch abgeschlossen (Fundamentalsatz der Algebra).

Beweis von Satz 15.5.

„1 ⇒ 2“: Sei $f \in K[t] \setminus K$. Nach Annahme existiert eine Nullstelle $a \in K$. Wir zeigen Aussage 2 mit vollständiger Induktion.

- Der Induktionsanfang $\deg(f) = 1$ ist klar.
- $\deg(f) \geq 2$: Wir nehmen an, dass die Behauptung für alle Polynome kleineren Grades stimmt. Da eine a Nullstelle von f ist, teilt $t - a$ das Polynom f nach Satz 7.14. Folglich gilt $f = (t - a)g$ für ein $g \in K[t]$. Es gilt $\deg(g) < \deg(f)$, da K ein Integritätsbereich ist. Somit ist g und damit auch f ein Produkt von Linearfaktoren.

„2 ⇒ 3“: Offensichtlich ist $t - a \in K[t]$ normiert und irreduzibel (aus Gradgründen). Sei $f \in K[t]$ normiert und irreduzibel.

- Falls $\deg(f) \in \{0, -\infty\}$, so folgt $f = 0$ oder $f \in K^\times = K[t]^\times$; damit ist f aber nicht irreduzibel, ein Widerspruch.
- Wenn $\deg(f) = 1$, ist $f = t - a$ für ein $a \in K$, weil f normiert ist.
- Sei $\deg(f) \geq 2$. Nach 2 gilt dann $f = (t - a)g$ für ein $a \in K$ und $g \in K[t]$, wobei g auch normiert ist. Da $(t - a)$ und g aber aus Gradgründen keine Einheiten sind, steht dies im Widerspruch dazu, dass f irreduzibel ist.

„3 ⇒ 4“: Sei $L \mathbin{/\!/} K$ eine algebraische Körpererweiterung und $b \in L$. Dann ist b algebraisch über K, es existiert also ein $f \in K[t] \setminus K$ mit $f(b) = 0$. Folglich existiert ein Minimalpolynom $m_b(t) \in K[t]$ mit $m_b(b) = 0$. Nach der Definition des Normalpolynoms ist $m_b(t)$ normiert und irreduzibel. Mit 3 folgt, dass $m_b(t) = t - a$ für ein $a \in K$. Da b eine Nullstelle von $m_b(t)$ ist, erhalten wir $b = a$ und damit $b \in K$. Somit ist bereits $L = K$.

„4 ⇒ 1“: Sei $f \in K[t] \setminus K$. Nach Satz 15.4 existiert eine algebraische Körpererweiterung $L \mathbin{/\!/} K$, sodass f in L eine Nullstelle hat. Aber nach Voraussetzung ist $L = K$. □

16. Algebraischer Abschluss

Satz 16.1. *Sei K ein Körper. Dann existiert ein algebraisch abgeschlossener Körper L mit $K \subseteq L$.*

Zur Erinnerung: Für einen kommutativen Ring R und eine Teilmenge $N \subseteq R$ bezeichnet (N) das von N erzeugte Ideal, also das kleinste Ideal in R, das N enthält. Es gilt

$$(N) = \left\{ \sum_{i=1}^{m} r_i n_i \;\middle|\; m \in \mathbb{N}, n_i \in N, r_i \in R \; \forall i \right\}.$$

Beweis von Satz 16.1.

1. *Schritt:* Wir „bauen“ eine Körpererweiterung $L_1 \mathbin{/\!/} K$, sodass jedes $f \in K[t]$ mit $\deg(f) \geq 1$ eine Nullstelle in L_1 hat. Sei

$$J := K[t] \setminus K = \{\text{Polynome vom Grad} \geq 1\}$$

Betrachte $R = K\left[X_f \mid f \in J\right]$ (siehe Übungsblatt 9 für eine saubere Definition). Das ist ein Polynomring über K in unendlich vielen Variablen.

Wir definieren $I := (f(X_f) \mid f \in J) \subseteq R$ vermöge der universellen Eigenschaft von $K[t]$. Es ist klar, dass I ein Ideal ist; wir behaupten, dass I sogar ein echtes Ideal ist. Der Beweis hierfür folgt weiter unten.

Nach Satz 9.1 existiert ein maximales Ideal $m \subseteq R$ mit $R \supseteq m \supseteq I$. Damit ist $R/m =: L_1$ ein Körper. Offenbar gilt $K \subseteq R$ und sogar $K \subseteq R/m$ (durch die Abbildung $K \to R \to R/m$). Somit haben wir eine Körpererweiterung $L_1 \mathbin{/\!/} K$. Sei

nun $f \in J = K[t] \setminus K$ mit $f = \sum_{i=0}^{\infty} b_i t^i$ und fast allen $b_i = 0$. Es ist zu zeigen, dass f eine Nullstelle in L_1 hat.

Wir wissen $f(\mathrm{can}(X_f)) = \sum_{i=0}^{\infty} b_i \overline{X_f}^i$, wobei $b_i \in K$ ist. Also gilt

$$f(\mathrm{can}(X_f)) = \sum_{i=0}^{\infty} \overline{b_i} {X_f}^i = \overline{\sum_{i=0}^{\infty} b_i X_f^i} = \mathrm{can}(f(X_f)),$$

wobei $f(X_f) \in I \subseteq m$, also $f(\mathrm{can}(X_f)) = 0$. Also ist $\mathrm{can}(X_f) \in L_1$ eine Nullstelle von $f(t)$.

2. Schritt: Betrachte den „Turm“ von Körpererweiterungen $K \coloneqq L_0 \subseteq L_1 \subseteq L_2 \subseteq \ldots$, sodass $L_{i+1} /\!\!/ L_i$ eine Körpererweiterung ist und jedes $f \in L_i[t] \setminus L_i$ eine Nullstelle in L_{i+1} hat (existiert nach Schritt 1). Setze

$$L := \bigcup_{i \geq 0} L_i,$$

was natürlich ein Körper ist. Es ist nun zu zeigen, dass es für jedes $g \in L[t] \setminus L$ eine Nullstelle in L gibt.

Sei dafür $g = \sum_{i=0}^{\infty} a_i t^i$ mit nur endlich vielen $a_i \neq 0$. Folglich gibt es ein $n_0 \in \mathbb{N}$ mit $a_i \in L_{n_0}$ für alle i. Das heißt aber, dass wir g als Polynom in $L_{n_0}[t]$ auffassen können. Dadurch hat $g(t)$ eine Nullstelle in $L_{n_0+1} \subseteq L$.

Somit gibt es einen Körper L mit $K \subseteq L$.

Beweis von $I \neq R$: Sei $I = R$, also liegt $1 \in I$. Somit existieren gewisse $g_i \in R$ und $f_i \in J$ mit $1 = \sum_{i=1}^{n} g_i f_i(X_{f_i})$. Nach wiederholter Anwendung von Satz 15.4 existiert eine Körpererweiterung $L' /\!\!/ K$, wobei $f_1, \ldots, f_n$ Nullstellen in L' haben, sagen wir $a_1, \ldots, a_n$. Nach der universellen Eigenschaft für Polynomringe existiert ein Ringhomomorphismus

$$\mathrm{ev} \colon R \longrightarrow L'[X_f \mid f \in J]$$

mit

$$\mathrm{ev}(X_f) = \begin{cases} a_i & \text{falls } f = f_i \text{ für ein } i \\ X_f & \text{sonst} \end{cases}$$

und $\mathrm{ev}(\lambda) = \lambda \in K \subseteq L'$ für $\lambda \in K$. Dann gilt $\mathrm{ev}(f_i(X_{f_i})) = f_i(a_i) = 0$, weil a_i eine Nullstelle von f_i ist. Also gilt für $1 \in R$

$$1 = \mathrm{ev}(1) = \mathrm{ev}\left(\sum_{i=0}^{m} g_i f_i(X_{f_i})\right) = \sum_{i=0}^{m} \mathrm{ev}(g_i)\,\mathrm{ev}(f_i(X_{f_i})) = 0$$

Folglich gilt $1 = 0$ in $L'[X_f \mid f \in J]$, was ein Widerspruch ist, also ist $1 \notin I$. □

[4. Dezember 2017]

[7. Dezember 2017]

Satz 16.2. *Sei K ein Körper. Dann existiert eine algebraische Körpererweiterung $L /\!\!/ K$, wobei L algebraisch abgeschlossen ist.*

Beweis. Nach obigem Satz existiert ein Körper L', sodass $K \subseteq L'$ ein Unterkörper und L' algebraisch abgeschlossen ist. Betrachte

$$K^{\text{alg}} = \{a \in L' \mid a \text{ algebraisch über } K\},$$

was nach Lemma 15.3 ein Körper ist.

Nun ist $K \subseteq K^{\text{alg}}$, denn für $b \in K$ ist b eine Nullstelle von $f = t - b \in K[t]$. Also sind $K \subseteq K^{\text{alg}} \subseteq L'$ jeweils Körpererweiterungen. Außerdem ist $K^{\text{alg}} /\!\!/ K$ algebraisch, was nach Definition klar ist, da jedes Element $a \in K^{\text{alg}}$ algebraisch über K ist.

Wir zeigen schließlich, dass K^{alg} algebraisch abgeschlossen ist. Sei nämlich $f \in K^{\text{alg}}[t] \setminus K^{\text{alg}}$. Es ist zu zeigen, dass f eine Nullstelle in K^{alg} hat. Wir wissen dabei, dass $K^{\text{alg}} \subseteq L'$ und L' algebraisch abgeschlossen ist. Folglich hat f eine Nullstelle $a \in L'$, also ist a algebraisch über K^{alg}. Mit Satz 15.1 folgt, dass $K^{\text{alg}}(a) /\!\!/ K^{\text{alg}}$ eine algebraische Körpererweiterung ist. Aus der Transitivität von algebraischen Körpererweiterungen (Satz 15.2) und der Algebraizität von $K^{\text{alg}} /\!\!/ K$ folgt, dass $K^{\text{alg}}(a) /\!\!/ K$ eine algebraische Körpererweiterung ist. Folglich ist jedes Element in $K^{\text{alg}}(a)$ algebraisch über K; insbesondere ist a algebraisch über K, also $a \in K^{\text{alg}}$. Setze nun $L \coloneqq K^{\text{alg}}$. □

Definition 16.1. Wir nennen den vermöge Satz 16.2 existierenden Körper L algebraischen Abschluss von K und bezeichnen ihn oft mit $\overline{K}$.

Wie sieht es nun mit der Eindeutigkeit von $\overline{K}$ aus (bis auf Isomorphie)?

Definition 16.2. Sei K ein Körper sowie $L_1 /\!\!/ K$ und $L_2 /\!\!/ K$ Körpererweiterungen. Eine Abbildung $\varphi\colon L_1 \to L_2$ heißt K-Homomorphismus, falls φ ein Ring- und damit ein Körperhomomorphismus und $\varphi|_K = \mathrm{id}_K$ ist. φ heißt K-Isomorphismus, falls zusätzlich φ bijektiv ist. Falls $L_1 = L_2$ und $\varphi\colon L_1 \to L_2 = L_1$ ein K-Isomorphismus ist, dann nennen wir φ auch K-Automorphismus.

Beispiel 1. $L_1 = L_2$, $\varphi = \mathrm{id}_{L_1}$ ist ein K-Automorphismus.

Definition 16.3. Die Menge

$$\mathrm{Aut}(L /\!\!/ K) \coloneqq \{\varphi\colon L \to L \mid \varphi \ K\text{-Automorphismus}\}$$

ist eine Gruppe bezüglich der Komposition von Abbildungen (für jede Körpererweiterung $L /\!\!/ K$). Wir nennen sie die Automorphismengruppe von $L /\!\!/ K$.

Beispiel 2. Für $\mathbb{C} /\!\!/ \mathbb{R}$ gilt $\mathrm{Aut}(\mathbb{C} /\!\!/ \mathbb{R}) = \{\mathrm{id}_{\mathbb{C}}, z \mapsto \overline{z}\}$.

Beweis.

„$\supseteq$“: Klar.

„$\subseteq$“: Sei $\varphi \in \mathrm{Aut}(\mathbb{C} /\!\!/ \mathbb{R})$. Dann ist $\varphi(a+bi) = \varphi(a)+\varphi(b)\varphi(i) = a+b\varphi(i)$, wobei $a, b \in \mathbb{R}$. Also ist φ durch durch $\varphi(i)$ bereits eindeutig bestimmt. Es gilt $-1 = \varphi(-1) = \varphi(i^2) = \varphi(i)^2$. Daraus folgt, dass $\varphi(i)$ eine Quadratwurzel von -1 sein muss, also $\varphi(i) = i$ (also $\varphi = \mathrm{id}_{\mathbb{C}}$) oder $\varphi(i) = -i$ (also ist φ die komplexe Konjugation). □

Unser Ziel ist nun:

Satz 16.3 (Eindeutigkeit des algebraischen Abschlusses)**.** *Sei K ein Körper sowie $L_1 /\!\!/ K$ und $L_2 /\!\!/ K$ Körpererweiterungen, sodass L_1, L_2 algebraische Abschlüsse von K sind. Dann existiert ein K-Isomorphismus $\varphi\colon L_1 \to L_2$.*

Bemerkung. Sei $\varphi\colon L_1 \to L_2$ ein K-Homomorphismus und $[L_1 : K] = [L_2 : K] < \infty$. Dann ist φ ein K-Isomorphismus, da φ ein Ringhomomorphismus und L_i ein Körper ist. Somit ist φ injektiv. Außerdem ist $\varphi(x+y) = \varphi(x)+\varphi(y)$ und $\varphi(\lambda x) = \varphi(\lambda)\varphi(x) = \lambda\varphi(x)$ für $\lambda \in K$ sowie $x, y \in L_i$. Also ist φ eine K-lineare Abbildung. Folglich ist φ eine K-lineare injektive Abbildung zwischen endlichdimensionalen K-Vektorräumen der gleichen Dimension, also ist φ bijektiv und damit ein K-Isomorphismus.

Übersicht. Sei $L /\!\!/ K$ eine Körpererweiterung. Dann gilt folgendes bezüglich der Teilmengen von $\{\varphi\colon L \to L\}$:

$$
\begin{array}{ccccc}
\left\{\varphi \middle| \begin{smallmatrix}\varphi \text{ Ringhomo-}\\ \text{morphismus}\end{smallmatrix}\right\} & & & & \{\varphi \mid \varphi \ K\text{-linear}\} \\
\| & & & & \cup| \\
\left\{\varphi \middle| \begin{smallmatrix}\varphi \text{ Körperhomo-}\\ \text{morphismus}\end{smallmatrix}\right\} & \supset & \left\{\varphi \middle| \begin{smallmatrix}\varphi \text{ Körperiso-}\\ \text{morphismus}\end{smallmatrix}\right\} & & \left\{\varphi \middle| \begin{smallmatrix}\varphi \ K\text{-linear}\\ \text{und injektiv}\end{smallmatrix}\right\} \\
\cup| & & \cup| & \subsetneq & \\
\left\{\varphi \middle| \begin{smallmatrix}\varphi \ K\text{-Homo-}\\ \text{morphismus}\end{smallmatrix}\right\} & \supset & \mathrm{Aut}(L /\!\!/ K) & &
\end{array}
$$

Lemma 16.4. *Es sei $\varphi\colon L_1 \to L_2$ ein K-Homomorphismus, und es sei $f \in K[t]$. Dann ist $a \in L_1$ genau dann eine Nullstelle von f, wenn $\varphi(a) \in L_2$ eine Nullstelle von f ist.*

Beweis. Sei $f = \sum_{i=0}^{\infty} b_i t^i \in K[t]$ und a eine Nullstelle von $f(t)$, also $\sum_{i=0}^{\infty} b_i a^i = 0$. Das ist genau dann der Fall, wenn $\varphi(\sum_{i=0}^{\infty} b_i a^i) = \varphi(0) = 0$, da φ als Ringhomomorphismus zwischen Körpern injektiv ist. Hierzu ist $\sum_{i=0}^{\infty} \varphi(b_i)\varphi(a)^i = 0$ äquivalent, weil φ ein Ringhomomorphismus ist, was wiederum genau dann eintritt, wenn $\sum_{i=0}^{\infty} b_i \varphi(a)^i = 0$, da φ ein K-Homomorphismus ist, also ist $\varphi(a)$ eine Nullstelle von f. □

Lemma 16.5. *Sei $\varphi\colon L_1 \to L_2$ ein K-Homomorphismus. Wenn $a \in L_1$ algebraisch über K ist, ist $\varphi(a)$ algebraisch über K und für die Minimalpolynome gilt $m_a(t) = m_{\varphi(a)}(t) \in K[t]$.*

Beweis. Sei $a \in L_1$ algebraisch über K, es existiert also ein $f \in K[t] \setminus K$ mit $f(a) = 0$. a ist folglich eine Nullstelle von $f \in K[t]$. Nach Lemma 16.4 ist $\varphi(a)$ eine Nullstelle von f. Daher ist $\varphi(a)$ algebraisch über K und Teil 1 des Lemmas folgt.

Sei $m_a(t) \in K[t]$ das Minimalpolynom von a; $m_a(t)$ ist also normiert und von minimalem Grad, sodass a Nullstelle ist. Nach Lemma 16.4 ist $\varphi(a)$ eine Nullstelle von $m_a(t) \in K[t]$. Folglich ist $m_{\varphi(a)}$ Teiler von $m_a(t)$. Da analog auch $m_a(t)$ ein Teiler von $m_{\varphi(a)}$ ist, gilt $m_a(t) = m_{\varphi(a)}(t)$. □

Bemerkung. Beachte: φ bildet algebraische $a \in L_1$ auf Nullstellen von $m_a(t)$ ab!

Lemma 16.6. *Sei K ein Körper sowie $L /\!\!/ K$ und $L' /\!\!/ K$ algebraische Körpererweiterungen und $a \in L$, $a' \in L'$ mit $m_a(t) = m_{a'}(t) \in K[t]$. Dann existiert ein eindeutiger K-Isomorphismus $\varphi\colon K(a) \to K(a')$, sodass $\varphi(a) = a'$.*

Beweis. Betrachte den Ringhomomorphismus

$$\begin{aligned} \mathrm{ev}_a\colon K[t] &\longrightarrow L \\ p &\longmapsto p(a). \end{aligned}$$

Dann gilt $m_a(t) \mapsto m_a(a) = 0$, also $m_a(t) \in \ker(\mathrm{ev}_a)$, woraus $(m_a(t)) \subseteq \ker(\mathrm{ev}_a)$ folgt. Nach dem Homomorphiesatz existiert genau ein Ringhomomorphismus

$$\overline{\mathrm{ev}_a}\colon K[t]/(m_a(t)) \to L,$$

sodass $\overline{\mathrm{ev}_a} \circ \mathrm{can} = \mathrm{ev}_a$.

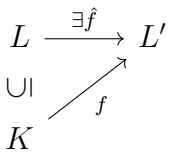
Es ist klar, dass $\operatorname{im} \mathrm{ev}_a \subseteq K(a)$. Dann gilt auch $\operatorname{im} \overline{\mathrm{ev}_a} \subseteq K(a)$, und wir können $\overline{\mathrm{ev}_a}\colon K[t]/(m_a(t)) \to K(a)$ betrachten. Wir wissen (siehe Vergleich transzendent vs. algebraisch), dass $(m_a(t))$ ein maximales Ideal ist. Also ist $K[t]/(m_a(t))$ ein Körper. Damit ist $\overline{\mathrm{ev}_a}$ injektiv und $\operatorname{im} \overline{\mathrm{ev}_a} \subseteq K(a)$. Außerdem ist $\operatorname{im} \overline{\mathrm{ev}_a}$ ein Körper, weil es das Bild eines Körpers unter einem Ringhomomorphismus ist, und $\operatorname{im} \overline{\mathrm{ev}_a}$ enthält offensichtlich K und a. Somit gilt $\operatorname{im}(\overline{\mathrm{ev}_a}) = K(a)$. Also ist $\varphi_1 = \overline{\mathrm{ev}_a}\colon K[t]/(m_a(t)) \to K(a)$ ein Isomorphismus von Körpern. Nach Konstruktion gilt $\varphi_1(\bar{t}) = a$ und $\varphi_1|_K = \mathrm{id}_K$.

Analog haben wir einen Isomorphismus von Körpern $\varphi_2 : K[t]/(m_{a'}(t)) \to K(a')$ mit $\varphi_2(\bar{t}) = a'$ und $\varphi_2|_K = \mathrm{id}_K$. Dabei ist $(m'_a(t)) = (m_a(t))$ (nach Voraussetzung). Nun ist $\varphi = \varphi_1 \circ \varphi_1^{-1}\colon K(a) \to K(a')$ ein Isomorphismus von Körpern und $\varphi(a) = \varphi_2(\bar{t}) = \varphi(a')$ und $\varphi|_K = \mathrm{id}_K$. Folglich erhalten wir einen K-Isomorphismus $\varphi\colon K(a) \to K(a')$ mit $\varphi(a) = a'$

φ ist eindeutig, da $\varphi|_K = \mathrm{id}_K$ und $\varphi(a) = a'$; dadurch ist φ eindeutig bestimmt. □

Satz 16.7 (Fortsetzungssatz)**.**

1. *Sei $L /\!\!/ K$ eine algebraische Körpererweiterung sowie L' ein algebraisch abgeschlossener Körper und $f\colon K \to L'$ ein Ringhomomorphismus. Dann existiert ein Ringhomomorphismus $\hat{f}\colon L \to L'$, sodass $\hat{f}|_K = f$, also sodass das Diagramm*



kommutiert.

2. *Seien K, K' Körper und $f\colon K \to K'$ ein Ringisomorphismus. Seien weiterhin $\overline{K}$ und $\overline{K'}$ algebraische Abschlüsse von K beziehungsweise K'. Dann existiert ein Isomorphismus von Körpern $\hat{f}\colon \overline{K} \to \overline{K'}$ mit $\hat{f}|_K = f$.*

[7. Dezember 2017]

[11. Dezember 2017]

Beweis.

1. Betrachte
$$Z = \left\{ (M, g_M) \,\middle|\, \begin{smallmatrix} K \subseteq M \subseteq L \text{ Zwischenkörper,} \\ g_M\colon M \to L' \text{ Ringhomo-} \\ \text{morphismus, } g_M|_K = f \end{smallmatrix} \right\}.$$
Nun gilt:
   - Z ist nicht leer, da $(K, f) \in Z$.
   - Wir definieren auf Z durch $(M, g_M) \leq (M', g_{M'}) :\Leftrightarrow M \subseteq M', g_{M'}|_M = g_M$ eine partielle Ordnung. Das Nachprüfen dieser Eigenschaft bleibt dem Leser überlassen.
   - Sei $U \subseteq Z$ eine total geordnete Teilmenge. Dann hat U eine obere Schranke (S, g_S) in Z bezüglich obiger Ordnung. Dafür sei $U = \{(U_i, g_i) \mid i \in I\} \subseteq Z$. Dann setze $S \coloneqq \bigcup_{i\in I} U_i$ und $g_S\colon S \to L'$ definiert durch $g_s(u_i) = g_i(u_i)$, falls $u_i \in U_i$. Nun gilt:

     S ist ein Körper. Da U total geordnet ist, existiert für $x, y \in S$ ein $i \in I$ mit $x, y \in U_i$, da etwa für $x \in U_m, y \in U_j$ schon $U_m \leq U_j$ oder $U_j \leq U_m$ gilt. Da alle U_k Körper sind, ist auch S ein Körper.

     g_S ist wohldefiniert. Sei $u \in S$ mit $u \in U_i \cap U_j$. Da U total geordnet ist, gilt $U_i \subseteq U_j$ oder $U_j \subseteq U_i$, und dann nach Definition der Ordnung sogar $g_i(u) = g_j(u)$, weil $(U_i, g_i) \leq (U_j, g_j)$ oder $(U_j, g_j) \leq (U_i, g_i)$ und $u \in U_i \cap U_j$ ist.

     g_S ist ein Ringhomomorphismus. Analog zu den obigen Beweisen ist dies sofort klar, da U total geordnet ist und alle g_i Ringhomomorphismen sind.

     Somit liegt $(S, g_S) \in Z$ (beachte $g_i|_K = f$ für alle $i \in I$ nach Definition, also auch $g_S|_K = f$). Offensichtlich ist (S, g_S) eine obere Schranke für U.
   - Mit dem Lemma von Zorn folgt die Existenz eines maximalen Elementes $(M_{\max}, g_{\max}) \in Z$.
   - *Behauptung:* $M_{\max} = L$. Daraus folgt direkt 1 mit dem Ringhomomorphismus $\hat{f} = g_{\max}\colon M_{\max} = L \to L'$, für den $\hat{f}|_K = g_{\max}|_K = f$ gilt, weil $(M_{\max}, g_{\max}) \in Z$ liegt.

Beweis der Behauptung. Da $(M_{\max}, g_{\max}) \in Z$, gilt $M_{\max} \subseteq L$. Sei also $a \in L$, aber $a \notin M_{\max}$. Wir wollen nun einen Widerspruch herleiten. Da $L \mathbin{/\!\!/} K$ algebraisch ist, ist erst recht $L \mathbin{/\!\!/} M_{\max}$ algebraisch, da $K \subseteq M_{\max}$. Folglich existiert das Minimalpolynom $m_a(t) \in M_{\max}[t] \setminus M_{\max}$ von a. Sei $m_a = \sum_{i=0}^{\infty} b_i t^i$. Sei $m'_a(t) = \sum_{i=0}^{\infty} g_{\max}(b_i) t^i \in L'[t] \setminus L'$. Da L' nach Voraussetzung algebraisch abgeschlossen ist, existiert eine Nullstelle a' von $m'_a(t)$ in L'. Betrachte nun den Ringhomomorphismus

$$\begin{aligned} \mathrm{ev}_{a'} \colon M_{\max}[t] &\longrightarrow L' \\ \sum_{j=0}^{\infty} c_i t^i &\longmapsto \sum_{i=0}^{\infty} g_{\max}(c_i)(a')^i. \end{aligned}$$

Nach Konstruktion gilt hier:

- $(m_a(t)) \subseteq \ker \mathrm{ev}_{a'}$.
- Es gilt $\mathrm{ev}_{a'}|_K = g_{\max}|_K = f$ nach der Definition von Z. Nach dem Homomorphiesatz erhalten wir einen Ringhomomorphismus

  $$\overline{\mathrm{ev}_{a'}} \colon M_{\max}[t]/(m_a(t)) \to L' \ ,$$

  sodass $\overline{\mathrm{ev}_{a'}} \circ \mathrm{can} = \mathrm{ev}_{a'}$. Da a algebraisch ist, ist andererseits

  $$\beta : M_{\max}(a) \xrightarrow{\sim} M_{\max}[t]/(m_a(t))$$

  ein Isomorphismus von Körpern und damit

  $$M_{\max} \subsetneq M_{\max}(a) \cong M_{\max}[t]/(m_a(t))$$

  Wir erhalten also einen Körper $M_{\max}(a) \subseteq L$ mit $M_{\max} \subsetneq M_{\max}(a)$.

  Also ist $(M_{\max}, \mathrm{ev}_{a'} \circ \beta) \in Z$, da $\mathrm{ev}_{a'} \circ \beta \colon M_{\max}(a) \to L'$ offensichtlich ein Ringhomomorphismus mit $(\mathrm{ev}_{a'} \circ \beta)|_K = \mathrm{ev}_{a'}|_K = f$ nach Konstruktion ist. Das ist ein Widerspruch zur Maximalität von $(M_{\max}, g_{\max})$. Damit folgt die Behauptung und insgesamt Teil 1 des Satzes. □

2. Betrachte $L := \overline{K}$ und $f \colon K \xrightarrow{\varphi} K' \subseteq \overline{K'} =: L'$. Da $L \mathbin{/\!\!/} K$ algebraisch (nach Definition des algebraischen Abschlusses) und $L' = \overline{K'}$ algebraisch abgeschlossen ist, können wir Teil 1 des Satzes anwenden und erhalten einen Ringhomomorphismus

   $$\hat{\varphi} \colon L = \overline{K} \longrightarrow \overline{K'} = L'$$

   mit $\hat{\varphi}|_K = \varphi$. Da $\hat{\varphi}$ ein Ringhomomorphismus und $\overline{K}$ ein Körper ist, ist $\hat{\varphi}$ injektiv. Es bleibt die Surjektivität von $\hat{\varphi}$ zu zeigen. Dabei wissen wir:

   - $\mathrm{im}\, \hat{\varphi} \subseteq L'$ ist ein Unterkörper, weil $\overline{K}$ ein Körper ist.
   - $K' = \mathrm{im}\, \varphi = f(K) = \hat{\varphi}(K) \subseteq \mathrm{im}\, \hat{\varphi}$, also $K' \subseteq \mathrm{im}\, \hat{\varphi} \subseteq \overline{K'} = L'$.

- Da $\overline{K}$ algebraisch abeschlossen ist, ist auch $\operatorname{im}\hat{\varphi}$ algebraisch abgeschlossen, da für $\sum_{i=0}^{\infty} c_i t^i \in \operatorname{im}\hat{\varphi}[t] \setminus \operatorname{im}\hat{\varphi}$ dann $a_i \in \overline{K}$ mit $c_i = \hat{\varphi}(a_i)$ existieren, wobei $\sum_{i=0}^{\infty} a_i t^i \in \overline{K}[t] \setminus \overline{K}$ eine Nullstelle x in $\overline{K}$ hat, da $\overline{K}$ algebraisch abgeschlossen ist, weshalb $\hat{\varphi}(x)$ eine Nullstelle von $\sum_{i=0}^{\infty} c_i t^i$ ist.
- Die Körpererweiterung $\operatorname{im}\hat{\varphi} \mathbin{/\!\!/} K'$ ist algebraisch, da $\operatorname{im}\hat{\varphi} \subseteq \overline{K'}$ und $\overline{K'} \mathbin{/\!\!/} K'$ algebraisch per Definition ist, und somit insbesondere auch $\operatorname{im}\hat{\varphi} \mathbin{/\!\!/} K'$ algebraisch ist.

Also ist $K' \subseteq \operatorname{im}\hat{\varphi} \subseteq \overline{K'}$; da $\operatorname{im}\hat{\varphi}$ algebraisch abgeschlossen ist, folgt mit Satz 15.5 $\operatorname{im}\hat{\varphi} = \overline{K'}$. Folglich haben wir einen Isomorphismus von Körpern

$$\hat{\varphi}\colon \overline{K} \xrightarrow{\sim} \overline{K'},$$

wobei $\hat{\varphi}|_K = f|_K = \varphi$. Also folgt Teil 2. □

Damit folgt der Eindeutigkeitssatz 16.3.

Wie sehen nun zum Beispiel $\overline{\mathbb{Q}}$ oder $\overline{\mathbb{F}_2}$ aus?

Bemerkung. Wir wissen: $\mathbb{Q} \subsetneq \overline{\mathbb{Q}}$, da beispielsweise $t^2 - 2 \in \mathbb{Q}[t]$ keine Nullstelle in $\mathbb{Q}$ hat. Wir können $\mathbb{Q}^{\text{alg}} = \{z \in \mathbb{C} \mid z \text{ algebraisch über } \mathbb{Q}\} \subseteq \mathbb{C}$ als algebraischen Abschluss nehmen, da $\mathbb{C}$ algebraisch abgeschlossen ist. „Man“ weiß, dass $\mathbb{Q}^{\text{alg}} \subsetneq \mathbb{C}$, weil es transzendente Zahlen gibt, z.B. $\pi \in \mathbb{C} \setminus \mathbb{Q}^{\text{alg}}$. Aus der Konstruktion des algebraischen Abschlusses kann man folgern, dass $\mathbb{Q}^{\text{alg}}$ abzählbar ist.

Für $\overline{\mathbb{F}_2}$ ist die Lage besser. Wir brauchen aber ein besseres Verständnis endlicher Körper.

17. Endliche Körper

Ziel: Gegeben eine Primzahl p und $r \in \mathbb{N} = \mathbb{Z}_{>0}$. Dann existiert ein Körper $\mathbb{F}$ mit $|\mathbb{F}| = p^r$. Genauer gilt der folgende Satz.

Satz 17.1 (Klassifikationssatz endlicher Körper)**.** *Es gibt eine Bijektion*

$$\begin{array}{rccc} \Phi\colon & \left\{\mathbb{F} \,\middle|\, \substack{\mathbb{F} \text{ endlicher Körper} \\ \text{(bis auf Körperisomorphie)}}\right\} & \xleftrightarrow{1:1} & \{p^r \mid p \text{ Primzahl}, r \in \mathbb{N}\} \\ & \mathbb{F} & \longmapsto & |\mathbb{F}| \end{array}$$

Wir nennen dann den (bis auf Isomorphie eindeutigen) Körper mit p^r Elementen $\mathbb{F}_{p^r}$.

Bemerkung.

- Falls $r = 1$ ist, kennen wir $\mathbb{F}_p = (\mathbb{Z}/p\mathbb{Z}, +, \cdot)$ aus der linearen Algebra.
- Achtung: $\mathbb{F}_4 \ncong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, da letzterer Nullteiler hat.

Beispiel 1. Betrachte $p(t) = t^2 + t + 1 \in \mathbb{F}_2[t]$. p ist irreduzibel, da p keine Nullstellen hat. Folglich ist $K = \mathbb{F}_2[t]/(p(t))$ ein Körper, weil $(p(t))$ ein maximales Ideal ist. Als $\mathbb{F}_2$-Vektorraum hat K die Basis $\overline{1}, \overline{t}$. Also hat K 4 Elemente $a\overline{1} + b\overline{t}$ mit $a, b \in \mathbb{F}_2$; $K = \{0, \overline{1}, \overline{t}, \overline{1+t}\}$, wobei wir $x \coloneqq \overline{t}$ und $y \coloneqq \overline{1+t}$ setzen.

Wir betrachten nun die Additions- und Multiplikationstafeln von K.

$+$	$\overline{0}$	$\overline{1}$	x	y
$\overline{0}$	$\overline{0}$	$\overline{1}$	x	y
$\overline{1}$	$\overline{1}$	$\overline{0}$	y	x
x	x	y	$\overline{0}$	$\overline{1}$
y	y	x	$\overline{1}$	$\overline{0}$

$\cdot$	$\overline{0}$	$\overline{1}$	x	y
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	x	y
x	$\overline{0}$	x	y	$\overline{1}$
y	$\overline{0}$	y	$\overline{1}$	x

Beobachtungen:

- $\operatorname{char} K = 2$, weil $1 + 1 = 0$ und $\mathbb{F}_2 \subseteq K$ der Primkörper ist.
- Alle Elemente in $K^\times$ sind Nullstellen von $t^3 - 1$; alle Elemente in K sind Nullstellen von $t^4 - t$.
- $K^\times = K \setminus \{0\}$ ist eine Gruppe bezüglich $\cdot$ sowie ismorph zu $\mathbb{Z}/3\mathbb{Z}$ und somit insbesondere zyklisch.

[11. Dezember 2017]

[14. Dezember 2017]

Lemma 17.2. *Sei $\mathbb{F}$ ein endlicher Körper. Dann ist $|\mathbb{F}| = p^r$ für eine Primzahl p und $r \in \mathbb{N}$ und es gilt $\operatorname{char} \mathbb{F} = p$.*

Beweis. $\mathbb{F}$ hat den Primkörper $\mathbb{F}_p$ (weil sonst $\mathbb{Q} \cong$ Primkörper $\subseteq \mathbb{F}$, was ein Widerspruch zur Endlichkeit von $\mathbb{F}$ wäre) für eine eindeutig bestimmte Primzahl p. Insbesondere ist $\mathbb{F}_p \subseteq \mathbb{F}$ ein Unterkörper. Damit ist $\mathbb{F}$ ein $\mathbb{F}_p$-Vektorraum und es gilt $\mathbb{F} \cong (\mathbb{F}_p)^n$ für ein $n \in \mathbb{N}$ (Isomorphismus als $\mathbb{F}_p$-Vektorraum). Folglich ist $|\mathbb{F}| = p^n$; wir setzen also $r = n = \dim_{\mathbb{F}_p} \mathbb{F}$. □

Also ist Φ aus Satz 17.1 eine wohldefinierte Abbildung.

Satz 17.3. *Sei K Körper sowie $H < (K^\times, \cdot)$ eine endliche Untergruppe. Dann ist H zyklisch.*

Beweis.

1. Behauptung: Sei G eine endliche abelsche Gruppe. Dann existiert ein Isomorphismus von Gruppen $G \cong G_{p_1} \times \cdots \times G_{p_n}$, wobei die G_{p_i} die p_i-Sylowuntergruppen von G sind (genauer: $G_{p_1}, \ldots, G_{p_n}$ sind genau die Sylowuntergruppen von G). Insbesondere gilt dann
$$H \cong G_{p_1} \times \cdots \times G_{p_n} \tag{*}$$
mit G_{p_i} als p_i-Sylowuntergruppe von H für $1 \leq i \leq n$.
2. Behauptung: Alle G_{p_i} $(1 \leq i \leq n)$ in (*) für $1 \leq i \leq n$ sind zyklisch.
3. Behauptung: Die Gruppe $G_{p_1} \times \cdots \times G_{p_n}$ wie in (*) ist zyklisch.

Damit ist H zyklisch.

Beweis 1. Behauptung: Sei $|G| = p_1^{c_1} \dots p_n^{c_n}$ mit paarweise verschiedenen Primzahlen p_i. Nach den Sylowsätzen existiert eine p_i-Sylowuntergruppe G_{p_i} von G. Diese ist eindeutig, da jede andere p_i-Sylowuntergruppe zu dieser konjugiert ist, woraus sogar Gleichheit folgt, da G abelsch ist. Es ist nach dem Satz von Lagrange klar, dass $G_{p_i} \cap G_{p_j} = \{e\}$ für $i \neq j$ gilt. Betrachte

$$\begin{aligned} f \colon G_{p_1} \times \dots \times G_{p_n} &\longrightarrow G \\ (g_1, \dots, g_n) &\longmapsto g_1 \dots g_n. \end{aligned}$$

Im Folgenden seien $(g_1, \dots, g_n), (g_1', \dots, g_n')$ immer in $G_{p_1} \times \dots \times G_{p_n}$.

- f ist ein Gruppenhomomorphismus, da

$$\begin{aligned} f((g_1, \dots, g_n)(g_1', \dots, g_n')) &= f((g_1 g_1', \dots, g_n g_n')) = g_1 g_1' g_2 g_2' \dots g_n g_n' \\ &= g_1 g_2 \dots g_n g_1' \dots g_n' = f((g_1, \dots, g_n)) f((g_1', \dots, g_n')) \end{aligned}$$

  gilt.

- f ist injektiv. Zum Beweis sei $f((g_1, \dots, g_n)) = f((g_1', \dots, g_n'))$. Dann ist $g_1 \dots g_n = g_1' \dots g_n'$. Umformen ergibt

$$g_2 \dots g_n (g_2' \dots g_n')^{-1} = g_1^{-1} g_1' \ ,$$

  wobei $g_2 \dots g_n (g_2' \dots g_n')^{-1} = g_2 (g_2')^{-1} \dots g_n (g_n')^{-1} \in f(\{e\} \times G_{p_2} \times \dots \times G_{p_n})$ und $g_1^{-1} g_1' \in f(G_{p_1})$.

  Sei $\tilde{G} = \{e\} \times G_{p_2} \times \dots \times G_{p_n}$. Nach dem Homomorphiesatz gilt $f(\tilde{G}) \cong \tilde{G} / \ker f|_{\tilde{G}}$. Damit folgt

$$|f(\tilde{G})| = \frac{|\{e\} \times G_{p_2} \times \dots \times G_{p_n}|}{|\ker f|_{\tilde{G}}|}$$

  nach dem Satz von Lagrange. $|f(\tilde{G})|$ teilt somit $p_2^{c_2} \dots p_n^{c_n}$. Analog zeigt man, dass $|f(G_{p_1})|$ dann $p_1^{c_1}$ teilt.

  $\operatorname{ord}(g_2 \dots g_n (g_2' \dots g_n')^{-1})$ teilt also $p_2^{c_2} \dots p_n^{c_n}$ und $\operatorname{ord}(g_1^{-1} g_1')$ teilt $p_1^{c_1}$. Da die p_i paarweise verschieden sind, gilt $\operatorname{ord}(g_1^{-1} g_1') \mid \operatorname{ggT}(p_1^{c_1}, p_2^{c_2} \dots p_n^{c_n}) = 1$, also $g_1^{-1} g_1' = e$ und schließlich $g_1' = g_1$. Völlig analog folgt $g_i = g_i'$ für alle $1 \leq i \leq n$.

- f ist surjektiv, da f injektiv ist und $|G_{p_1} \times \dots \times G_{p_n}| = p_1^{c_1} \dots p_n^{c_n} = |G| < \infty$ gilt.

Damit ist f ein bijektiver Ringhomomorphismus und die 1. Behauptung folgt.

Beweis 2. Behauptung: Wir nehmen an, G_{p_i} wäre nicht zyklisch für ein $i = 1, \dots, n$. Wir setzen $p = p_i$ und $c = c_i$ (c_i wie oben). Es gilt $|G_p| = p^c$ und nach Annahme $\operatorname{ord}(g) < p^c$ für alle $g \in G_p$. Da $\operatorname{ord}(g)$ die Ordnung der Gruppe $|G_p|$ teilt, folgt $ord(g) \leq p^{c-1}$ und sogar $\operatorname{ord}(g) = p^m$ für ein $m \leq c - 1$ für alle $g \in G_p$, wobei m von g abhängig ist.

Also ist $g^{p^m} = 1$ und g ist eine Nullstelle des Polynoms $t^{p^m} - 1$, und somit auch von $t^{p^{c-1}} - 1$. Damit ist g eine Nullstelle von $t^{p^{c-1}} - 1$ für alle $g \in G_p$. Aber $t^{p^{c-1}} - 1$ hat höchstens p^{c-1} verschiedene Nullstellen, was im Widerspruch dazu steht, dass $|G_p| = p^c > p^{c-1}$ ist. Also ist G_{p_i} zyklisch für alle $1 \leq i \leq n$.

Beweis 3. Behauptung: Es ist zu zeigen, dass $G_{p_1} \times \cdots \times G_{p_n}$ wie in (*) zyklisch ist. Nach der 2. Behauptung wissen wir $G_{p_i} \cong \mathbb{Z}/p_i^{c_i}\mathbb{Z}$ mit der Klassifikation zyklischer Gruppen. Es ist also $H \cong \mathbb{Z}/p_1^{c_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_n^{c_n}\mathbb{Z}$ als Isomorphismus von Gruppen. Da die p_i paarweise verschiedene Primzahlen sind, existieren $a, b \in \mathbb{Z}$ so, dass $1 = ap_i^{c_i} + bp_j^{c_j}$ (Euklidischer Algorithmus). Damit ist $1 \in p_i^{c_i}\mathbb{Z} + p_j^{c_j}\mathbb{Z}$ und wir können den Chinesischen Restsatz anwenden. Dadurch erhalten wir einen Isomorphismus von Ringen

$$\mathbb{Z}/p_1^{c_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_n^{c_n}\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/m\mathbb{Z}$$

mit $m = p_1^{c_1} \dots p_n^{c_n}$. Dies ist insbesondere ein Isomorphismus von Gruppen. Da $\mathbb{Z}/m\mathbb{Z}$ zyklisch ist, folgt schließlich, dass H zyklisch ist. □

Bemerkung. Insbesondere gilt: Für endliche Körper $\mathbb{F}$ ist $(\mathbb{F}^\times, \cdot)$ eine zyklische Gruppe.

Lemma 17.4. *Sei $\mathbb{F}$ ein endlicher Körper mit $|\mathbb{F}| = n = p^r$, wobei p eine Primzahl und $r \in \mathbb{N}$ ist. Dann existiert ein Isomorphismus von Körpern $\mathbb{F} \cong \mathbb{F}_p[t]/(p(t))$, wobei $p(t) \in \mathbb{F}_p[t]$ mit $\deg(p(t)) = r$ und $p(t) \mid t^n - t \in F_p[t]$ sowie irreduzibel ist. Umgekehrt existiert ein solcher Isomorphismus, wenn $p(t)$ soebige Eigenschaften erfüllt.*

Beweis. $(\mathbb{F}^\times, \cdot)$ ist eine endliche ablesche Gruppe, also nach Satz 17.3 zyklisch mit der Ordnung $n-1$. Folglich existiert ein $a \in \mathbb{F}^\times$ mit $\mathbb{F}^\times = \langle a \rangle$. Insbesondere ist $\operatorname{ord}(a) = n-1$, also $a^{n-1} = 1 \in \mathbb{F}^\times \subseteq \mathbb{F}$. Es gilt sogar $x^{n-1} = 1$ für alle $x \in \langle a \rangle = \mathbb{F}^\times$. Damit ist jedes $x \in \mathbb{F}$ Nullstelle von $t^n - t \in \mathbb{F}_p[t]$. Da es höchstens n verschiedene Nullstellen gibt und $|\mathbb{F}| = n$, folgt

$$\mathbb{F} = \{\text{Nullstellen von } t^n - t \in \mathbb{F}_p[t]\}$$

und somit zerfällt $t^n - t$ über $\mathbb{F}$ vollständig in Linearfaktoren. Sei $p(t)$ wie im Lemma definiert und o.B.d.A. $p(t)$ normiert. Da $x \in \mathbb{F}^\times$ eine Nullstelle von $t^n - t$ ist und $p(t)$ das Polynom $t^n - t$ teilt, ist $p(t) = m_x(t)$ das Minimalpolynom für ein $x \in \mathbb{F}^\times$, weil $p(t)$ irreduzibel ist. Betrachte nun den Ringhomomorphismus

$$\begin{aligned} \operatorname{ev}_x \colon \mathbb{F}_p[t] &\longrightarrow \mathbb{F} \\ \sum_{i=0}^{\infty} b_i t^i &\longmapsto \sum_{i=0}^{\infty} b_i x^i \end{aligned}$$

Dieser induziert, weil $p(x) = 0$ ist, nach dem Homomorphiesatz einen Ringhomomorphismus

$$\overline{\operatorname{ev}_x} \colon \mathbb{F}_p[t]/(m_x(t)) \to \mathbb{F}.$$

Wir wissen, dass $K \coloneqq \mathbb{F}_p[t]/(p(t))$ ein Körper ist, weil $p(t)$ irreduzibel ist. Folglich ist $\overline{\operatorname{ev}_x} \colon K \to \mathbb{F}$ injektiv.

Wir behaupten, dass $\overline{\mathrm{ev}_x}$ surjektiv ist. Wir wissen $\dim_{\mathbb{F}_p} K = \deg(p(t)) = r$, da $\{1, \bar{t}, \ldots, \overline{t^{\deg(p(t))-1}}\}$ eine Basis ist. Also gilt $|K| = p^r = n = |\mathbb{F}|$. Damit ist $\overline{\mathrm{ev}_x}$ eine injektive Abbildung zwischen endlichen Mengen derselben Kardinalität, also bijektiv.

Folglich existiert ein $\mathbb{F}_p[t]/(p(t)) \xrightarrow{\cong} \mathbb{F}$ Körperisomorphismus für alle $p(t)$ wie im Lemma.

Es bleibt noch zu zeigen, dass ein solches $p(t)$ auch tatsächlich immer existiert; siehe dazu den Nachtrag zu Beginn der nächsten Vorlesung. □

Bemerkung. Wir betrachten das Φ aus Satz 17.1. Lemma 17.4 besagt insbesondere, dass zwei endliche Körper derselben Kardinalität isomorph sind; Φ ist also injektiv. Es bleibt zu zeigen, dass Φ surjektiv ist.

Beachte: Sei $\mathbb{F}$ wie im Lemma 17.4 definiert. Dann gilt:

1. $f(t) = t^n - t \in \mathbb{F}_p[t]$ zerfällt in Linearfaktoren über $\mathbb{F}$.
2. $\mathbb{F} = \mathbb{F}_p(a_1, \ldots, a_n)$, wobei $a_1, \ldots, a_n$ die Nullstellen von $f(t)$ sind.

18. Zerfällungskörper

Definition 18.1. Sei K ein Körper und $f(t) \in K[t]$ mit $\deg(f(t)) \geq 1$. Sei $L \mathbin{/\!\!/} K$ eine Körpererweiterung. Dann heißt L (ein) Zerfällungskörper von $f(t)$ über K, falls

1. $f(t)$ in Linearfaktoren über L zerfällt, es existiert also eine Darstellung

$$f(t) = c \prod_{i=1}^{n} (t - a_i) \tag{*}$$

   mit $a_1, \ldots, a_n \in L$ und $c \in K$, und
2. $L = K(a_1, \ldots, a_n) \subseteq L$ mit $a_1, \ldots, a_n$ wie in (*) gilt.

Beispiel 1. Sei $f(t) = t^2 + 1 \in \mathbb{R}[t]$. Dann ist $\mathbb{C}$ ein Zerfällungskörper über $\mathbb{R}$, da $f(t) = (t - i)(t + i)$, also gilt 1., und $\mathbb{R}(i, -i) = \mathbb{C}$, also gilt 2.

Existenz von Zerfällungskörpern. Sei $f(t) \in K[t]$. Betrachte den algebraischen Abschluss $\overline{K}$ von K. Dann existieren $a_1, \ldots, a_n \in \overline{K}$ und $c \in K$ mit $f(t) = c \prod_{i=1}^{n} (t - a_i)$. Setze $L := K(a_1, \ldots, a_n)$. Dies ist dann ein Zerfällungskörper von $f(t) \in K[t]$, der in $\overline{K}$ enthaltene Zerfällungskörper.

[14. Dezember 2017]

[18. Dezember 2017]

Wir wollen später noch zeigen:

Satz 18.1. *Sei p eine Primzahl und $r \in \mathbb{N}$. Dann existiert ein Körper $\mathbb{F}$ mit $|\mathbb{F}| = p^r$.*

Zunächst noch ein Nachtrag zu Lemma 17.4. Beim dortigen Beweis bleibt noch zu zeigen, dass ein solches $p(t)$ existiert.

Beweis. Wir wissen:

- $\mathbb{F}_p \subseteq \mathbb{F}$ ist der Primkörper.
- $\mathbb{F}^\times$ ist zyklisch; es existiert also ein $a \in \mathbb{F}^\times$ mit $\mathbb{F}^\times = \langle a \rangle$.
- Für alle Einheiten $x \in \mathbb{F}^\times$ gilt $x^n - x = 0$.

Insbesondere teilt $m_a(t) \in \mathbb{F}_p[t]$ dann $t^n - t \in \mathbb{F}_p[t]$ und es gilt $\mathbb{F}_p(a) = \mathbb{F}$. Betrachte den Ringhomomorphismus

$$\begin{aligned} \mathrm{ev}_a \colon \mathbb{F}_p[t] &\longrightarrow \mathbb{F} \\ \sum_{i=0}^{\infty} b_i t^i &\longmapsto \sum_{i=0}^{\infty} b_i a^i. \end{aligned}$$

Klar ist, dass $\operatorname{im} \mathrm{ev}_a = \mathbb{F}_p(a) = \mathbb{F}$ gilt; ev_a ist also surjektiv. Nach dem Homomorphiesatz existiert ein Ringhomomorphismus

$$\overline{\mathrm{ev}_a} \colon K := \mathbb{F}_p[t]/(m_a(t)) \longrightarrow \mathbb{F}$$

mit $\mathrm{ev}_a = \overline{\mathrm{ev}_a} \circ \mathrm{can}$. $\overline{\mathrm{ev}_a}$ ist surjektiv und auch injektiv, da K ein Körper ist. Somit ist $\overline{\mathrm{ev}_a}$ ist ein Isomorphismus von Körpern.

Insbesondere ist $\deg(m_a(t)) = \dim_{\mathbb{F}_p} K = \dim_{\mathbb{F}_p} \mathbb{F} = r$. Klar ist, dass $m_a(t)$ irreduzibel ist und $t^m - t$ teilt. Folglich ist $m_a(t)$ ein gesuchtes Polynom. □

Definition 18.2. Sei K ein Körper sowie $f \in K[t]$ mit $f = \sum_{i=0}^{n} a_i t^i$. Die formale Ableitung von $f(t)$ ist $f'(t) = \sum_{i=1}^{n} i a_i t^{i-1} \in K[t]$.

Beispiel 2.

$$f(t) = 2t^3 + 2t^2 + 1 \in \mathbb{F}_3[t] \quad \Longrightarrow \quad f'(t) = 6t^2 + 4t = t \in \mathbb{F}_3[t]$$

Übungsblatt: Die formale Ableitung erfüllt die Produktregel $(fg)' = f'g + fg'$.

Satz 18.2. *Sei $L /\!\!/ K$ eine Körpererweiterung sowie $f, g \in K[t]$ und $g \neq 0$. Dann:*

1. *Gilt $f = hg + r$ in $L[t]$ mit $\deg(r) < \deg(h)$, dann gilt auch $f = hg + r$ in $K[t]$.*
2. *Falls g das Polynom f in $L[t]$ teilt, dann teilt es es auch in $K[t]$.*
3. *Die normierten größten gemeinsamen Teiler in $L[t]$ und $K[t]$ sind gleich.*

Beweis. Da $K[t]$ euklidisch ist, existieren $h', r' \in K[t]$ mit $f = h'g + r'$, wobei $\deg(r') < \deg(g)$. Da $L[t]$ ebenfalls euklidisch ist, existieren eindeutige $h, r \in L[t]$ mit $f = hg + r$ und $\deg(r) < \deg(g)$. Aus der Eindeutigkeit folgen $h = h'$ und $r = r'$. Also gilt die 1. Aussage. Die 2. Aussage folgt aus der ersten mit $r = 0$. Die letzte Aussage bleibt dem aufmerksamen Leser als Übung überlassen. □

Satz 18.3. *Sei K ein Körper sowie $p \in K[t]$ mit $p \neq 0$. Sei L ein Zerfällungskörper von p über K. Dann sind folgende Aussagen äquivalent:*

1. *p hat eine eine mehrfache Nullstelle in L, es existiert also ein $a \in L$ mir $(t-a)^2 \mid p$ in $L[t]$.*
2. *p und p' haben einen gemeinsamen Teiler $h(t) \in L[t] \setminus L$.*
3. *p und p' haben eine gemeinsame Nullstelle.*

Beweis.

„1 $\Rightarrow$ 2“: Sei $a \in L$ eine mehrfache Nullstelle von p. Dann ist $p = (t-a)^2Q(t) = (t^2-2at+a^2)Q(t)$ für ein $Q(t) \in L[t]$. Nach der Produktregel ist $p' = 2(t-a)Q(t)+(t-a)^2Q'(t)$. Damit teilt $(t-a)$ sowohl p als auch p'.

„2 $\Rightarrow$ 3“: p und p' haben einen gemeinsamen Teiler $h(t) \in L[t] \setminus L$. Da L ein Zerfällungskörper von p ist, existiert ein $a \in L$, welches eine Nullstelle von $h(t)$ ist. Insbesondere ist a eine gemeinsame Nullstelle von p und p'.

„3 $\Rightarrow$ 1“: Sei a eine gemeinsame Nullstelle von p und p'. Also ist $p = (t-a)Q(t)$ mit $Q(t) \in L[t]$. Es folgt $p' = Q(t) + (t-a)Q'(t)$. Da $(t-a)$ das Polynom p' teilt, muss also $(t-a)$ auch $Q(t)$ teilen und somit gilt $(t-a)^2 \mid p$. Folglich ist a eine mehrfache Nullstelle von p.

□

Korollar 18.4. *Sei K ein Körper und $p \in K[t] \setminus K$ irreduzibel. Dann sind äquivalent:*

1. *p hat eine mehrfache Nullstelle im Zerfällungskörper.*
2. *$p' = 0$ (Nullpolynom).*
3. *Es existiert ein $Q \in K[t]$ mit $p = Q(t^p)$ mit $0 < p = \operatorname{char} K$.*

Beweis.

„2 $\Rightarrow$ 3“: Sei $p = a_nt^n + \cdots + a_1t + a_0$ mit $a_n \neq 0$, $n \geq 1$. Mit der Voraussetzung $p' = 0$ folgt $ja_j = 0$ für alle $1 \leq j \leq n$. Da K aber nullteilerfrei ist, gilt $n = 0$ in K. Folglich existiert eine Primzahl q mit $q = \operatorname{char} K$ und dann $n = qk$ für ein $k \in \mathbb{N}$. Also ist $ja_j = 0$, falls $a_j = 0$ oder j Vielfaches von p. Das heißt, $p = a_0 + a_pt^p + a_{2p}t^{2p} + \cdots + a_{pk}t^{pk}$. Damit ist $p = Q(t^p)$, wobei $Q(t) = a_0 + a_pt + a_{2p}t^2 + \ldots a_{pk}t^k$.

„3 $\Rightarrow$ 1“: Sei a eine Nullstelle von $Q(t)$ in einem Zerfällungskörper L von $Q(t)$. Dann ist $Q(t) = (t-a)h(t)$ für ein $h(t) \in L[t]$; es gilt also $p = (t^p - a)h(t^p)$. Sei b eine Nullstelle von $t^p - a$, also eine p-te Wurzel von a, in einem algebraischen Abschluss von K.

Nach der binomischen Formel „für Dumme“ erhalten wir $p(t) = (t^p - b^p)h(t^p) = (t-b)^pn(t^p)$. Da $p \geq 2$ ist, hat $p(t)$ die mehrfache Nullstelle b in einem algebraischen Abschluss von K, also auch in dem zugehörigen Zerfällungskörper.

„1 ⇒ 2“: Sei a eine mehrfache Nullstelle von p. Nach Satz 18.3 ist a eine gemeinsame Nullstelle von p und p' bzw. p und p' haben einen gemeinsamen Teiler $h(t) \in L[t] \setminus L$. Es gilt $h(t) \neq 0$, da sonst schon $p(t) = 0$ im Widerspruch zur Irreduzibilität von p ist. Da p irreduzibel ist und $\deg(h(t)) \leq \deg(p') < \deg(p)$ im Fall von $p' \neq 0$, ist damit $h(t)$ eine Einheit im Widerspruch zu $h(t) \notin L$. Also ist $p' = 0$. □

Definition 18.3. Sei K ein Körper, $\operatorname{char} K = p$. Dann ist $\mathrm{Fr}\colon K \to K, a \mapsto a^p$ ein Ringhomomorphismus, der Frobeniushomomorphismus. (Denn $\mathrm{Fr}(xy) = (xy)^p = x^p y^p = \mathrm{Fr}(x)\,\mathrm{Fr}(y)$ und $\mathrm{Fr}(x+y) = (x+y)^p = x^p + y^p = \mathrm{Fr}(x) + \mathrm{Fr}(y)$ für alle $x, y \in K$.)

Beweis von Satz 18.1. Sei $p(t) = t^n - t \in \mathbb{F}_p[t]$. Sei L ein Zerfällungskörper von $p(t)$ über $\mathbb{F}_p$. Dann ist $\mathbb{F}_p \subseteq L$ der Primkörper, also $\operatorname{char} L = p$. Betrachte $\mathrm{Fr}^r := \mathrm{Fr} \circ \cdots \circ \mathrm{Fr}\colon L \to L$ als den r-ten Frobeniushomomorphismus. Sei weiterhin

$$L^{\mathrm{Fr}^r} := \{x \in L \mid Fr^r(x) = x\} = \{x \in L \mid x^{p^r} = x\} = \{x \in L \mid x^n - x = 0\} \subseteq L.$$

Man rechnet leicht nach, dass $L^{\mathrm{Fr}^r} \subseteq L$ ein Unterkörper von L ist. Da L ein Zerfällungskörper von $p(t) = t^n - t$ ist und andererseits alle Nullstellen von $t^n - t$ schon in L^{Fr^r} liegen, gilt $L^{\mathrm{Fr}^r} = L$. Daher ist $|L| \leq n$, weil $t^n - t$ höchstens n verschiedene Nullstellen hat. Nun reicht es zu zeigen, dass $|L| = n$.

Wir behaupten, dass $t^n - t$ genau n verschiedene Nullstellen hat; damit ist dann $\mathbb{F} := L$ der gesuchte Körper. Angenommen, es gibt weniger als n verschiedene Nullstellen; dann existiert eine mehrfache Nullstelle a in L, da L ein Zerfällungskörper ist. Dann gilt aber $p'(a) = 0$. Andererseits ist $p'(t) = nt^{n-1} - 1 = -1$, da $n = p^r$ und wir mit Charakteristik p rechnen. Folglich ist p' nie 0 und wir erhalten einen Widerspruch. Also hat $t^n - t$ genau n verschiedene Nullstellen. □

Damit ist der Klassifikationssatz endlicher Körper gezeigt.

Korollar 18.5. *Der Zerfällungskörper von $p(t) = t^n - t \in \mathbb{F}_p[t]$ (mit p, n wie in Satz 18.1) ist eindeutig bis auf Isomorphie.*

Beweis. $\Phi(p^r) := \mathbb{F}$ ist (ein) Zerfällungskörper von $t^n - t$ und ist eindeutig bis auf Isomorphie von Körpern. □

Allgemeiner lässt sich der folgende Satz formulieren:

Satz 18.6. *Seien K und K' Körper und $\varphi\colon K \to K'$ ein Ringhomomorphismus. Sei $f(t) \in K[t] \setminus K$ und L bzw. L' Zerfällungskörper von $f(t)$ über K bzw. von $\varphi_*(f) \in K'[t] \setminus K'$, wobei*

$$\begin{aligned} \varphi_*\colon K[t] &\longrightarrow K'[t] \\ \sum b_i t^i &\longmapsto \sum \varphi(b_i) t^i. \end{aligned}$$

Falls φ ein Isomorphismus ist, dann existiert ein Ringisomorphismus $\hat{\varphi}\colon L \to L'$ mit $\hat{\varphi}|_K = \varphi$.

Beweis. Wähle den bis auf Isomorphie eindeutigen algebraischen Abschluss $\overline{K}$ bzw. $\overline{K'}$ von K bzw. K' so, dass $K \subseteq L \subseteq \overline{K}$ und $K' \subseteq L' \subseteq \overline{K'}$. Der Fortsetzungssatz sagt uns nun, dass ein Homomorphismus $\hat{\varphi}\colon \overline{K} \to \overline{K'}$ mit $\hat{\varphi}|_K = \varphi$ existiert. Falls φ ein Isomorphismus ist, dann ist auch $\hat{\varphi}$ Isomorphismus von Körpern.

Andererseits existieren $a_1, \dots, a_n \in \overline{K}$ und $c \in K$ mit $f(t) = c\prod_{i=1}^{n}(t - a_i)$ und damit $\hat{\varphi}(f(t)) = \varphi(c)\prod_{i=1}^{n}(t - \hat{\varphi}(a_i))$. Also ist $\hat{\varphi}(a_i)$ für $1 \leq i \leq n$ eine Nullstelle von $\hat{\varphi}(f(t)) = \varphi_*(f)(t)$. Damit ist $L = K(a_1, \dots, a_n)$, da er ein Zerfällungskörper von K ist, und wird unter $\hat{\varphi}$ auf $L' = K'(\hat{\varphi}(a_1), \dots, \hat{\varphi}(a_n))$ abgebildet. $\hat{\varphi}$ ist offensichtlich surjektiv. Da $\hat{\varphi}$ automatisch injektiv ist, ist $\hat{\varphi}$ ein Isomorphismus von Körpern. □

Satz 18.7 (Eindeutigkeit des Zerfällungskörpers)**.** *Sei K ein Körper und L, L' Zerfällungskörper von K. Dann existiert ein K-Isomorphismus $\hat{\varphi}\colon L \to L'$.*

Beweis. Wende Satz 18.6 auf $K' = K$ und $\varphi = \mathrm{id}_K$ an. □

Folgender Satz ist als Ausblick auf die im nächsten Kapitel erzielt werdenden Ergebnisse gedacht, da die Galoisgruppe noch nicht offiziell eingeführt wurde.

Satz 18.8. *Sei $\mathbb{F}$ ein endlicher Körper sowie $|\mathbb{F}| = p^r = n$. Dann gilt:*

- $\mathrm{Gal}(\mathbb{F} /\!\!/ \mathbb{F}_p) = \{\varphi\colon \mathbb{F} \to \mathbb{F} \mid \varphi \text{ Ringisomorphismus}\}$.
- $\mathrm{Gal}(\mathbb{F} /\!\!/ \mathbb{F}_p) \cong (\mathbb{Z}/r\mathbb{Z}, +)$ *als Gruppe, erzeugt von* Fr. *Wir werden zeigen, dass daraus folgt, dass eine Bijektion (Galoiskorrespondenz) existiert:*

$$\begin{array}{ccc} \{\text{Untergruppen von } \mathrm{Gal}(\mathbb{F} /\!\!/ \mathbb{F}_p)\} & \overset{1:1}{\longleftrightarrow} & \{\text{Unterkörper von } \mathbb{F}\} \\ U & \longmapsto & \mathbb{F}^U = \{x \in \mathbb{F} \mid \varphi(x) = x \ \forall \varphi \in U\} \end{array}$$

[18. Dezember 2017]

[8. Januar 2018]

IV. Galoistheorie

Ziel: Für eine „gute“ Körpererweiterung $L /\!\!/ K$ gibt es eine 1:1-Korrespondenz zwischen den Untergruppen der Galoisgruppe $\mathrm{Gal}(L /\!\!/ K)$ und Zwischenkörpern $K \subseteq M \subseteq L$.

19. Normale und separable Körpererweiterungen

Satz 19.1 (Spezialfall der Galoiskorrespondenz)**.** *Sei $\mathbb{F}$ ein endlicher Körper mit $|\mathbb{F}| = n = p^r$ (p prim). Dann definiere*

$$G := \mathrm{Gal}(\mathbb{F} /\!\!/ \mathbb{F}_p) := \{\varphi\colon \mathbb{F} \to \mathbb{F} \text{ Körperisomorphismus}, \varphi|_{\mathbb{F}_p} = \mathrm{id}_{\mathbb{F}_p}\}.$$

Dann existiert eine Bijektion von Mengen

$$\begin{array}{rcl} \Phi\colon \{\textit{Untergruppen von } G = \mathrm{Gal}(\mathbb{F}/\mathbb{F}_p)\} & \overset{1:1}{\longleftrightarrow} & \{\textit{Zwischenkörper } \mathbb{F}_p \subseteq M \subseteq \mathbb{F}\} \\ H & \longmapsto & \mathbb{F}^H, \end{array}$$

wobei $\mathbb{F}^H := \{x \in \mathbb{F} \mid \forall \varphi \in H : \varphi(x) = x\}$ *den Fixkörper bezüglich* H *bezeichnet.*

Bemerkung.

1. $\mathbb{F}^H$ ist ein Körper, denn für $x, y \in \mathbb{F}^H$ gilt für alle $\varphi \in H : \varphi(x \pm y) = \varphi(x) \pm \varphi(y) = x \pm y$, $\varphi(xy) = \varphi(x)\varphi(y) = xy$, $\varphi(x^{-1}) = \varphi(x)^{-1} = x^{-1}$. Also ist Φ wohldefiniert.

2. Aus $\varphi \in H$ folgt bereits, dass φ ein Ringhomomorphismus ist, da $\varphi(1) = 1$ und $\varphi|_{\mathbb{F}_p} = \mathrm{id}_{\mathbb{F}_p}$ automatisch gelten (wir müssen es also eigentlich gar nicht fordern).

   Also $G = \{\varphi\colon \mathbb{F} \to \mathbb{F}$ Körperhomomorphismus$\}$ in diesem Fall. Insbesondere ist $\mathrm{Fr}\colon \mathbb{F} \to \mathbb{F}, x \mapsto x^p$ in G.

Vorbereitung zum Beweis von Satz 19.1:

Lemma 19.2. *Sei* $\mathbb{F}$ *ein endlicher Körper mit* $|\mathbb{F}| = n = p^r$ *(*p *prim). Dann ist* $G = \mathrm{Gal}(\mathbb{F}/\mathbb{F}_p)$ *zyklisch der Ordnung* r*.*

Beweis. Wir wissen (nach der Konstruktion endlicher Körper) $\mathbb{F} = \mathbb{F}_p(a)$ für ein $a \in \mathbb{F}$. Nach Bemerkung 2 ist $\varphi \in G$ festgelegt durch $\varphi(a)$. Sei $m_a(t) \in \mathbb{F}_p[t]$ das Minimalpolynom von a.

1. Behauptung: $m_a(t) = (t-a)(t-a^p)\dots(t-a^{p^{r-1}})$. *Beweis:* später. Dabei sind die Koeffizienten von $m_a(t)$ in $\mathbb{F}_p$, also $m_a(\varphi(a)) = \varphi(m_a(a)) = 0$, denn $\varphi|_{\mathbb{F}_p} = \mathrm{id}_{\mathbb{F}_p}$, also ist $\varphi(a)$ eine Nullstelle von $m_a(t)$. Folglich existiert ein s mit $0 \le s \le r-1$ mit $\varphi(a) = a^{p^s}$. Damit ist $\varphi = \mathrm{Fr}^s$ (weil eindeutig bestimmt auf a) und $G = \langle \mathrm{Fr} \rangle = \{\mathrm{id}, \mathrm{Fr}, \mathrm{Fr}^2, \dots\}$.

2. Behauptung: $\mathrm{Fr}^r = \mathrm{id}_{\mathbb{F}}$ sowie $\mathrm{Fr}^j \neq \mathrm{Fr}^i$ für $1 \le i < j \le r$. *Beweis:* Ist $\mathrm{Fr}^j = \mathrm{Fr}^i$, so folgt $\mathrm{Fr}^{j-i} = \mathrm{id}_{\mathbb{F}}$, also $\mathrm{Fr}^m = \mathrm{id}_{\mathbb{F}}$ für ein $m < r$. Deshalb gilt nun $x^{p^m} = x$ und weiter $x^{p^m} - x = 0$ für alle $x \in \mathbb{F}$. Damit muss $p^m \ge |\mathbb{F}| = p^r$ oder $p^m = 1$ sein, also $m \ge r$ oder $m = 0$ im Widerspruch zu $m < r$ und $i \neq j$. Außerdem hatten wir $\mathbb{F}$ als Nullstellen von $f(t) = t^n - t$ konstruiert. Also gilt für $x \in \mathbb{F}$ immer $x^{p^r} - x = 0$ $(p^r = n)$, also $\mathrm{Fr}^r = \mathrm{id}_{\mathbb{F}}$.

Damit erhalten wir insgesamt $G = \{\mathrm{Fr}, \mathrm{Fr}^2, \dots, \mathrm{Fr}^r = \mathrm{id}_{\mathbb{F}}\}$. Wie behauptet ist G folglich zyklisch (erzeugt von Fr) der Ordnung r. □

Beweis von Satz 19.1. Sei $H < G$. Da G zyklisch ist, ist H zyklisch der Ordnung k, wobei k ein Teiler von r ist, also $r = km$. Damit folgt $H = \{\mathrm{Fr}^m, \mathrm{Fr}^{2m}, \dots, \mathrm{Fr}^{km} = \mathrm{id}\}$. Weiter gilt $\Phi(H) = \mathbb{F}^H = \{x \in \mathbb{F} \mid \forall \varphi \in H : \varphi(x) = x\} = \{x \in \mathbb{F} \mid \mathrm{Fr}^m(x) = x\} = \{x \in \mathbb{F} \mid x^{p^m} - x = 0\}$. Nun betrachte $f \in \mathbb{F}_p[t], f = t^{p^m} - t$.

Injektivität: f hat p^m verschiedene Nullstellen in $\mathbb{F}$, da $f' = p^m t^{p^m-1} - 1 = -1$ keine Nullstellen hat. Damit ist $|\mathbb{F}^H| = p^m$ (da m ein Teiler von r ist, liegen alle Nullstellen in $\mathbb{F}$ nach Konstruktion von $\mathbb{F}$). Folglich ist Φ injektiv.

Surjektivität: Sei $K \subseteq \mathbb{F}$ ein Unterkörper. Dann gilt automatisch $\mathbb{F}_p \subseteq K$, und K ist ein $\mathbb{F}_p$-Vektorraum. Somit gilt $|K| = p^m$ für ein $m \leq r$. Da $\mathbb{F}$ auch ein K-Vektorraum ist, muss m ein Teiler von r sein. Nach der Konstruktion endlicher Körper gilt $x^{p^m} - x = 0$ für alle $x \in K$ und K besteht genau aus diesen Nullstellen. Es folgt, dass $K = \mathbb{F}^{\mathrm{Fr}^m} = \{x \in \mathbb{F} \mid \mathrm{Fr}^m(x) = x\}$. Damit ist $K = \Phi(H)$ für $H = \langle \mathrm{Fr}^m \rangle$. □

Satz 19.3. *Sei $\mathbb{F}$ ein endlicher Körper mit $\operatorname{char}\mathbb{F} = p$. Sei $1 \neq a \in \mathbb{F}$ und r minimal, sodass $a^{p^r} = a$. Dann gilt:*

1. *$1, a, a^2, \ldots, a^{p^{r-1}}$ sind paarweise verschieden.*
2. *$m_a(t) = (t-a)(t-a^p)\ldots(t-a^{p^{r-1}}) =: f(t) \in \mathbb{F}_p[t]$ Minimalpolynom von a über $\mathbb{F}_p$. (Damit folgt dann die 2. Behauptung aus dem Beweis von Lemma 19.2)*

Beweis.

1. Folgt aus Punkt 2, weil r minimal gewählt wurde.
2. Es gilt $m_a(t^p) = m_a(t)^p$ nach der binomischen Formel „für Dumme“. Falls nun z eine Nullstelle von $m_a(t)$ ist, so gilt das Gleiche für z^p. Somit ist Menge der Nullstellen von $m_a(t)$ sind stabil unter Frobeniusabbbildung Fr. Also teilt $Q_z = (t-z)(t-z^p)\ldots(t-z^{p^{r-1}})$ dann $m_a(t)$ für jede Nullstelle z von $m_a(t)$, insbesondere für $z = a$. Deshalb ist $Q_{z=a} = f(t) = m_a(t)$, weil $m_a(t)$ minimal mit Nullstelle a und Leitkoeffizient 1, falls $q \in \mathbb{F}_p[t]$ ist.

   Noch zu zeigen: $Q(t) \in \mathbb{F}_p[t]$. Wir wissen

   $$Q(t^p) = Q(t)^p. \tag{*}$$

   Falls $Q(t) = \sum_{i\geq 0} b_i t^i \in \mathbb{F}[t]$, dann gilt $Q(t)^p = \sum_{i\geq 0} b_i^p (t^i)^p = \sum_{i\geq 0} \mathrm{Fr}(b_i)(t^i)^p$. Somit mit (*): $b_i = \mathrm{Fr}(b_i)$ für alle i. Nach Konstruktion endlicher Körper ist dadurch $b_i \in \mathbb{F}_p$ für alle $i \geq 0$, womit wir schließlich $Q(t) \in \mathbb{F}_p[t]$ erhalten. □

Wir rufen uns an dieser Stelle die Definition einer einfachen Körpererweiterungen ins Gedächtnis (siehe Definition 14.5).

Definition 19.1. $L \mathbin{/\!\!/} K$ heißt einfach, falls ein $a \in L$ existiert, sodass $L \cong K(a)$ gilt.

Satz 19.4. *Sei $K(a) \mathbin{/\!\!/} K$ eine einfache, algebraische Körpererweiterung und $M \mathbin{/\!\!/} K$ eine beliebige Körpererweiterung. Dann*

$$\begin{array}{ccc} \{K\text{-Homomorphismen } \varphi\colon K(a) \to M\} & \overset{1:1}{\longleftrightarrow} & \{\text{Nullstellen von } m_a(t) \in K[t] \text{ in } M\} \\ \varphi & \longmapsto & \varphi(a) \end{array}$$

Es existiert also zu jeder Nullstelle $z \in M$ von $m_a(t)$ genau ein K-Homomorphismus $\varphi\colon K(a) \to M$ mit $\varphi(a) = z$.

Beweis.

Wohldefiniertheit: Sei $\varphi\colon K(a) \to M$ ein K-Homomorphismus, $\varphi(a) = z$. Dann folgt $m_a(z) = m_a(\varphi(a)) = \varphi(m_a(a)) = 0$.

Injektivität: φ ist eindeutig bestimmt durch $\varphi(a)$, weil φ ein Körperhomomorphismus mit $\varphi|_K = \mathrm{id}_K$ ist.

Surjektivität: Sei $z \in M$ eine Nullstelle von $m_a(t)$. Betrachte den Ringhomomorphismus

$$\begin{aligned} \mathrm{ev}_z\colon K[t] &\longrightarrow M \\ f(t) &\longmapsto f(z). \end{aligned}$$

Da z eine Nullstelle von $m_a(t)$ ist, induziert ev_z einen Ringhomomorphismus

$$\overline{\mathrm{ev}_z}\colon K[t]/(m_a(t)) \longrightarrow M,$$

wobei $\beta\colon K[t]/(m_a(t)) \xrightarrow{\sim} K(a) \subseteq K$, $K(a) /\!\!/ K$ algebraisch und $\overline{\mathrm{ev}_z}$ ein Körperhomomorphismus mit $\overline{\mathrm{ev}_z} \circ \beta|_K = \mathrm{id}_K$ nach Konstruktion ist. Man setze nun $\varphi \coloneqq \overline{\mathrm{ev}_z} \circ \beta$ und $\varphi(a) = \overline{\mathrm{ev}_z} \circ \beta(a) = \overline{\mathrm{ev}_z}(\overline{t}) = z$. □

Korollar 19.5. *Sei K Körper sowie $f \in K[t]$. Dann ist der Zerfällungskörper von f eindeutig bis auf K-Isomorphismus.*

Beweis. Übung. □

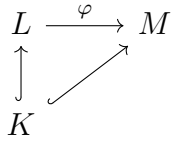
Definition 19.2. Eine Körpererweiterung $L /\!\!/ K$ heißt normal, falls sie algebraisch ist und falls irreduzible $f \in K[t]$ in Linearfaktoren über L zerfallen, wenn f eine Nullstelle in L hat.

Beispiel 1.

1. $\mathbb{Q}(\sqrt{2}) /\!\!/ \mathbb{Q}$ normal (Übung)
2. $\mathbb{Q}(\sqrt[3]{2}) /\!\!/ \mathbb{Q}$ ist nicht normal, denn betrachte $f = t^3 - 2$. Es gilt $\mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{R}$ und f hat Nullstellen $\sqrt[3]{2} \in \mathbb{Q}(\sqrt[3]{2})$ und $\sqrt[3]{2}\xi, \sqrt[3]{2}\xi^2 \notin \mathbb{R}$, mit $\xi = e^{\frac{2\pi i}{3}}$.

Satz 19.6 (Charakterisierung von Normalität)**.** *Sei $L /\!\!/ K$ eine endliche Körpererweiterung. Dann sind äquivalent:*

1. *$L /\!\!/ K$ ist normal.*
2. *L ist Zerfällungskörper eines Polynoms $f \in K[t]$.*
3. *Sei $M /\!\!/ K$ eine Körpererweiterungen . Dann haben alle Körperhomomorphismen $\varphi\colon L \to M$, die die Inklusion $K \hookrightarrow M$ fortsetzen, dasselbe Bild; das folgende Diagramm kommutiert also.*



[8. Januar 2018]

[11. Januar 2018]

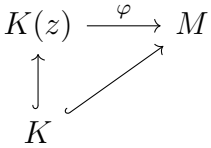
Beweis.

1 ⇒ 2: Sei $L = K(a_1, \dots, a_n)$ für gewisse $a_1, \dots, a_n \in L$. Wir betrachten das Minimalpolynom $m_{a_i}(t) \in K[t]$ von a_i. Sei $f(t) := m_{a_1}(t) \dots m_{a_n}(t) \in K[t]$. Jedes m_{a_i} hat eine Nullstelle in L, nämlich z.B. a_i. Da $L /\!\!/ K$ normal ist, sind alle Nullstellen von $m_{a_i}(t)$ in L für $1 \leq i \leq n$, weil $m_{a_i}(t)$ irreduzibel. Damit sind alle Nullstellen von $f(t)$ in L und somit ist L Zerfällungskorper von $f(t)$.

2 ⇒ 3: Ist L Zerfällungskörper von $f(t) \in K[t]$, so gilt $L = K(a_1, \dots, a_n)$ mit den a_i als Nullstellen von $f(t)$. Seien $\varphi_j \colon L \to M$ zwei K-Homomorphismen mit $j = 1, 2$ wie in 3. Es ist $\operatorname{im} \varphi_1 = \operatorname{im} \varphi_2$ zu zeigen.

Es ist $\varphi_j(a_i)$ eine Nullstelle von $f(t)$. Da die Nullstelle eindeutig ist, gilt nach Satz 19.4 $\{\varphi_1(a_i) \mid 1 \leq i \leq n\} = \{\varphi_2(a_i) \mid 1 \leq i \leq n\}$. Da dadurch φ_1 und φ_2 durch $\varphi|_K = \mathrm{id}$ und $\varphi(a_i)$ für $1 \leq i \leq n$ bereits eindeutig bestimmt sind, folgt $\operatorname{im} \varphi_1 = \operatorname{im} \varphi_2$.

3 ⇒ 1: Sei $f(t) \in K[t]$ irreduzibel. Sei $z \in L$ eine Nullstelle von $f(t)$. Für die Normalität von $L /\!\!/ K$ ist zu zeigen, dass alle Nullstellen von $f(t)$ in L liegen. Nach Voraussetzung gilt $L = K(b_1, \dots, b_n)$ für gewisse $b_i \in L$. Sei $M /\!\!/ L$ eine Körpererweiterung, sodass $m_{b_1}(t), \dots, m_{b_n}(t) \in K[t]$ (die Minimalpolynome der b_i) über M vollständig zerfallen. Sei z' eine weitere Nullstelle von $f(t)$. Betrachte



wobei $K \hookrightarrow K(z)$ und $K \hookrightarrow M$ Inklusionen sind und φ ein K-Homomorphismus mit $\varphi(z) = z'$ ist, welcher nach Satz 19.4 existiert.

Deshalb existiert ein $\hat{\varphi} \colon L \to M$ mit $\hat{\varphi}|_{K(z)} = \varphi$, weil $L /\!\!/ K$ endlich, also algebraisch ist und damit auch $L /\!\!/ K(z)$ algebraisch ist. Offensichtlich gilt $\hat{\varphi}(z) = z'$. Nun liegt jede Nullstelle von $f(t)$ im Bild von $\hat{\varphi}$. Nach Voraussetzung liegt jede Nullstelle von $f(t)$ dann schon im Bild jedes K-Homomorphismus $L \to M$; insbesondere also in L; man nehme etwa id_L mit $\operatorname{im} \mathrm{id}_L = L$. □

Bemerkung. Man kann statt $L /\!\!/ K$ endlich auch nur $L /\!\!/ K$ algebraisch fordern und 2 ersetzen durch: „L ist Zerfällungskörper über K (d.h. alle $f(t) \in K[t]$ zerfallen über L).“.

Letzterer existiert und ist gegeben durch den Zwischenkörper $K \subseteq M \subseteq \overline{K}$, welcher von allen Nullstellen der Polynome in $K[t]$ erzeugt ist. Wie vorher für Zerfällungskörper von Polynomen kann man zeigen, dass obiger Zerfällungskörper eindeutig bis auf K-Isomorphie ist.

Zum Beweis dieser alternativen Formulierung des Satzes siehe Übungsblatt 12.

Satz 19.7. *Sei $L \mathbin{/\!\!/} K$ eine endliche Körpererweiterung. Dann existiert eine endliche Körpererweiterung $M \mathbin{/\!\!/} L$, sodass $M \mathbin{/\!\!/} K$ normal ist.*

Korollar 19.8. *Sei $L \mathbin{/\!\!/} K$ eine Körpererweiterung und $K \subseteq M \subseteq L$ ein Zwischenkörper mit $M \mathbin{/\!\!/} K$ normal (und endlich, wobei man das nach obiger Bemerkung auch weglassen kann). Sei $\varphi\colon M \to L$ ein K-Homomorphismus. Dann ist $\varphi(M) = M$.*

Beweis. Betrachte die K-Homomorphismen $M \xrightarrow{\varphi} L$ und $M \xrightarrow{\mathrm{id}} M \subseteq L$. Da $M \mathbin{/\!\!/} K$ normal ist, gilt nach Satz 19.6 $\operatorname{im}\varphi = \operatorname{im}(\mathrm{id}_M) = M$. □

Beweis von Satz 19.7. Da $L \mathbin{/\!\!/} K$ endlich ist, gilt $L = K(a_1, \dots, a_n)$ für gewisse $a_1, \dots, a_n \in L$. Sei $f(t) = m_{a_1}(t) \dots m_{a_n}(t) \in K[t]$ mit $m_{a_i}(t)$ als Minimalpolynom von a_i für $1 \leq i \leq n$. Sei M Zerfällungskörper von $f(t)$ über L, also auch Zerfällungskörper von $f(t)$ über K. Nach Satz 19.6 ist $M \mathbin{/\!\!/} K$ normal.Es bleibt zu zeigen, dass $M \mathbin{/\!\!/} K$ endlich ist. Wir behaupten, dass $[M : K] \leq \deg(f(t))$. Damit folgt der Satz; die Behauptung folgt aus Lemma 19.9. □

Lemma 19.9. *Sei K ein Körper, $f(t) \in K[t]$, und L Zerfällungskörper von $f(t)$. Dann gilt $[L : K] \leq (\deg(f(t)))!$.*

Beweis. Sei $L = K(b_1, \dots, b_n)$, wobei b_i die (verschiedenen) Nullstellen von $f(t)$ sind. Sei weiterhin m_{b_i} das Minimalpolynom von b_i für $1 \leq i \leq n$. Insbesondere teilt $m_{b_i}(t)$ das $f(t)$, also gilt $[K(b_i) : K] = \deg m_{b_i}(t) \leq \deg f(t)$. Es gilt $[L : K] = [L : K(b_1)][K(b_1) : K]$. Da $L = K(b_1)(b_2, \dots, b_n)$ Zerfällungskörper von $f(t)/(t - b_1)$ ist, folgt induktiv $[L : K(b_1)][K(b_1) : K] \leq (\deg(f(t)/(t - b_1))! \cdot \deg(f(t)) = (\deg(f(t)))!$ □

Bemerkung. Sei $L \mathbin{/\!\!/} K$ eine normale Körpererweiterung und $K \subseteq M \subseteq L$ ein Zwischenkörper. Dann ist L eine normale Hülle von $M \mathbin{/\!\!/} K$, falls es keinen Zwischenkörper $M \subseteq N \subseteq L$ mit $N \mathbin{/\!\!/} K$ normal gibt. L ist also der kleinste Körper, der M enthält und normal über K ist. Man kann zeigen, dass die normale Hülle eindeutig bis auf K-Isomorphie ist.

Definition 19.3. Sei $L \mathbin{/\!\!/} K$ eine algebraische Körpererweiterung.

1. $f(t) \in K[t]$ heißt separabel, falls $f(t)$ keine mehrfachen Nullstellen in $\overline{K}$ hat.
2. $a \in L$ heißt separabel, falls das Minimalpolynom von a separabel ist.
3. $L \mathbin{/\!\!/} K$ heißt separabel, falls jedes $a \in L$ separabel ist.

Definition 19.4. Ein Körper K heißt perfekt, falls $\operatorname{char} K = 0$ oder $\operatorname{char} K = p > 0$ und dann der Frobenius-Homomorphimus surjektiv ist.

Beispiel 2. Jeder endliche Körper $\mathbb{F}$ ist perfekt, da $\mathrm{Fr}\colon \mathbb{F} \to \mathbb{F}$ injektiv, da $\mathbb{F}$ ein Körper ist, und damit bijektiv ist, weil $|\mathbb{F}| < \infty$.

Beispiel 3.

1. Jedes irreduzible Polynom $f(t) \in K[t]$ mit $\operatorname{char} K = 0$ ist separabel.
2. Betrachte $\mathbb{F}_p(x) /\!\!/ \mathbb{F}_p(x^p)$ mit x transzendent über $\mathbb{F}_p$. Sei $f(t) = t^p - x^p \in \mathbb{F}_p(x^p)[t]$. Dann ist $f(t)$ irreduzibel (nachprüfen!), aber zerfällt über $\mathbb{F}_p(x)$ und hat mehrfache Nullstellen, da $t^p - x^p = (t-x)^p$.

Satz 19.10. *Jede algebraische Erweiterung $L /\!\!/ K$ über einem perfekten Körper K ist separabel.*

Beweis.

$\operatorname{char} K = 0$: Sei $a \in L$ und $m_a(t) \in K[t]$ das zugehörige (irreduzible) Minimalpolynom. Nach Beispiel 3 hat $m_a(t)$ keine mehrfachen Nullstellen, also ist a separabel über K. Da a beliebig gewählt war, ist L separabel über K.

$\operatorname{char} K = p > 0$: Sei $a \in L$ und $m_a(t) \in K[t]$ das zugehörige Minimalpolynom. Wir nehmen an, $m_a(t)$ habe eine mehrfache Nullstelle. Mit Korollar 18.4 folgt $m_a'(t) = 0$, $m_a(t) = Q(t^p)$ für ein $Q(t) \in K[t]$. Sei $Q(t) = \sum_{i=0}^n b_i t^i \in K[t]$. Weil K perfekt ist, existieren $a_1, \dots, a_n$ mit $a_i^p = b_i$. Dann folgt $(\sum_{i=0}^n a_i t^i)^p = \sum_{i=0}^n b_i (t^p)^i = Q(t^p) = m_a(t)$. Das ist ein Widerspruch zur Irreduzibilität von $m_a(t)$; folglich hat $m_a(t)$ keine mehrfachen Nullstellen. Damit ist a separabel über K für alle $a \in L$; $L /\!\!/ K$ ist folglich separabel. □

Definition 19.5. Sei $L /\!\!/ K$ eine algebraische Körpererweiterung. Wir definieren

$$[L : K]_{\mathrm{sep}} := |\{\varphi\colon L \to \overline{K} \mid \varphi \ K\text{-Homomorphismus}\}|$$

als den Separabilitätsgrad von $L /\!\!/ K$.

Bemerkung.

1. Der Separabilitätsgrad ist unabhängig von der Wahl von $\overline{K}$.
2. Seien $L_1 /\!\!/ K$ und $L_2 /\!\!/ K$ Körpererweiterungen und sei $\varphi\colon L_1 \to L_2$ ein K-Isomorphismus. Dann gilt $[L_1 : K]_{\mathrm{sep}} = [L_2 : K]_{\mathrm{sep}}$.
3. Wir nennen Elemente $a \in L$ für eine Körpererweiterung $L /\!\!/ K$ inseparabel, falls a nicht separabel ist.

Lemma 19.11. *Sei $L /\!\!/ K$ eine algebraische endliche Körpererweiterung. Dann gilt*

$$[L : K]_{\mathrm{sep}} \leq [L : K].$$

Beweis. Sei $L = K(a_1, \dots, a_n)$ für gewisse $a_1, \dots, a_n \in L$. Sei $L_0 = K$ und sei $L_i = K(a_1, \dots, a_i)$, also $L_i = L_{i-1}(a_i)$. Wir wissen, dass für eine einfache algebraische Erweiterung $M(a) \mathbin{/\!\!/} M$ für einen Körper M nach Satz 19.4

$$[M(a) : M]_{\text{sep}} = \left|\left\{\varphi\colon M(a) \to \overline{M} \,\middle|_{\deg \varphi \le \deg m_a(t) \in M[t]}^{\varphi\ M\text{-Homo},}\right\}\right|$$

gilt, wobei $\deg m_a(t) = [M(a) : M]$. Wir erhalten $[L : K]_{\text{sep}} = \prod_{i=1}^{n} [L_i : L_{i-1}]_{\text{sep}} \le \prod_{i=1}^{n} [L_i : L_{i-1}] = [L : K]$. □

Lemma 19.12 (Transitivität)**.** *Seien $L_1 \mathbin{/\!\!/} L_2$ und $L_2 \mathbin{/\!\!/} L_3$ Körpererweiterungen. Dann gilt*

$$[L_1 : L_3]_{\text{sep}} = [L_1 : L_2]_{\text{sep}} \cdot [L_2 : L_3]_{\text{sep}}.$$

Beweis. Siehe Übungsblatt 12. □

Bemerkung. Sei $L \mathbin{/\!\!/} K$ eine endliche, normale Körpererweiterung. Dann ist $\varphi(L) = L$ für jeden K-Homomorphismus nach Korollar 19.8. Also gilt

$$[L : K]_{\text{sep}} = |\{\varphi\colon L \to L\ K\text{-Homomorphismus}\}| = |\operatorname{Aut}_K(L)|,$$

weil jeder Homomorphismus injektiv und wegen der Endlichkeit von $\dim_L K$ sogar bijektiv ist.

[11. Januar 2018]

[15. Januar 2018]

Lemma 19.13 (Charakterisierung von Separabilität)**.** *Sei $L \mathbin{/\!\!/} K$ eine algebraische Körpererweiterung. Dann sind folgende Aussagen äquivalent:*

1. *$L \mathbin{/\!\!/} K$ ist separabel.*
2. *L wird (über K) von separablen Elementen erzeugt.*
3. *Für jeden Zwischenkörper $K \subseteq M \subseteq L$ gilt $[M : K]_{\text{sep}} = [M : K]$.*

Falls $L \mathbin{/\!\!/} K$ endlich ist, ist 3. äquivalent zu

3'. $[L : K]_{\text{sep}} = [L : K]$.

Beweis. Sei zunächst $L \mathbin{/\!\!/} K$ endlich.

$3 \Leftrightarrow 3'$: Es gilt in beiden Fällen $[L : K]_{\text{sep}} = [L : K]$. Sei M ein Zwischenkörper von L und K. Dann gilt $[L : M]_{\text{sep}} \le [L : M]$ und $[M : K]_{\text{sep}} \le [M : K]$; nach Transitivät (Lemma 19.12) gilt jeweils Gleichheit, also folgt 3.

Ab jetzt sei $L \mathbin{/\!\!/} K$ nicht mehr notwendigerweise endlich.

$1 \Rightarrow 2$: ✓

$2 \Rightarrow 3$: Betrachte $a \in L$. Dann folgt daraus, dass a separabel über K ist, auch, dass a separabel über M ist. Denn $m_{a,M}(t) \in M[t]$ teilt $m_{a,K}(t) \in K[t] \subseteq M[t]$ (das sind jeweils die Minimalpolynome von a über den entsprechenden Körpern).

Betrachte nun zunächst doch wieder $L \mathbin{/\!\!/} K$ endlich. Sei $L = K(a_1, \dots, a_n)$ mit separablen $a_1, \dots, a_n \in L$. Setze $L_0 := K, L_i = K(a_1, \dots, a_i)$; insbesondere $L_i = L_{i-1}(a_i)$, wobei a_i separabel über L_{i-1} ist. Daraus folgt $[L_i = L_{i-1}(a_i) : L_{i-1}]_{\text{sep}} = [L_i : L_{i-1}]$ und nach Transitivität (Lemma 19.12) erhalten wir $[L : K]_{\text{sep}} = [L : K]$. Daraus folgt $3'$ und damit für endliche Körper 3.

Jetzt $L \mathbin{/\!\!/} K$ beliebig (aber algebraisch). Betrachte zwei Fälle:

- Falls $M \mathbin{/\!\!/} K$ endlich ist, existieren algebraische und separable $a_1, \dots, a_n \in L$ mit $M \subseteq K(a_1, \dots, a_n)$. Damit können wir $K(a_1, \dots, a_n)$ betrachten und mit unserer Vorüberlegung folgt die Aussage.
- Falls $M \mathbin{/\!\!/} K$ nicht endlich ist, so gilt: $[M : K]_{\text{sep}} = [M : M']_{\text{sep}}[M' : K]_{\text{sep}}$ für jeden Zwischenkörper $K \subseteq M' \subseteq M$, also insbesondere für solche mit $M' \mathbin{/\!\!/} K$ endlich. Also erhalten wir

$$[M : K]_{\text{sep}} \geq [M' : K]_{\text{sep}} = [M' : K]$$

für jeden endlichen Zwischenkörper M'. Da man $[M' : K]$ beliebig groß wählen kann, folgt $[M : K]_{\text{sep}} = \infty = [M : K]$. Damit folgt 3.

$3 \Rightarrow 1$: Sei $a \in L$ und $M := K(a)$. Nach Voraussetzung ist $[K(a) : K]_{\text{sep}} = [K(a) : K]$, was äquivalent zur Separabilität von a über K ist. Da a beliebig ist, ist $L \mathbin{/\!\!/} K$ separabel, also folgt 1. □

Satz 19.14 (Satz vom primitiven Element)**.** *Sei $L \mathbin{/\!\!/} K$ eine endliche, separable Körpererweiterung. Dann existiert ein $a \in L$ mit $L = K(a)$. Man nennt a dann primitives Element.*

Beweis. Da $L \mathbin{/\!\!/} K$ endlich ist, reicht es zu zeigen, dass für alle $x, y \in L$ ein $a \in L$ existiert, sodass $K(x, y) = K(a)$ gilt.

Fall 1: $|K| < \infty$: Da K ein endlicher Körper ist, ist L endlicher Körper, da $L \mathbin{/\!\!/} K$ endlich ist. Auch $K(x, y)$ ist ein endlicher Körper. Folglich ist $K(x, y)^\times$ eine zyklische Gruppe (Eigenschaft endlicher Körper), also erzeugt als Gruppe von einem Element, sagen wir c. Es folgt $K(x, y) = K(c)$ (als Körper). Wir setzen $a =: c$.

Fall 2: $|K| = \infty$: Sei $N = K(x, y)$ und $\overline{K}$ der algebraische Abschluss von K. Sei $[N : K]_{\text{sep}} = m$ und $\{\varphi_1, \dots, \varphi_m\} = \{\varphi \colon N \to \overline{K} \mid \varphi \; K\text{-Homomorphismus}\}$. Es gilt $[N : K]_{\text{sep}} = [N : K]$ nach Lemma 19.13. Sei

$$f = \prod_{i<j} ((\varphi_i(x) - \varphi_j(x)) + (\varphi_i(y) - \varphi_j(y))t) \in \overline{K}[t]$$

Falls $1 \leq i \neq j \leq m$, so gilt $\varphi(x) \neq \varphi_j(x)$ oder $\varphi_i(y) \neq \varphi_j(y)$, da φ_i und φ_j bereits eindeutig durch ihre Werte auf x und y bestimmt sind.

Somit folgt $f \neq 0$. Da $|K|$ unendlich ist, existiert ein $c \in K$ mit $f(c) \neq 0$. Für $i < j$ gilt also $(\varphi_i(x) - \varphi_j(y)) + (\varphi_i(y) - \varphi_j(y))c \neq 0$. Damit folgt $\varphi_i(x) + c\varphi_i(y) \neq \varphi_j(x) + c\varphi_j(y)$ für $i \neq j$. Da $c \in K$ ist, gilt $\varphi_i(c) = \varphi_j(c) = c$. Damit folgt $\varphi_i(x+cy) \neq \varphi_j(x+cy)$, da φ_i und φ_j Körperhomomorphismen sind. Setze $a := x+cy$. Dann sind die $\varphi_i(a)$ für $1 \leq i \leq m$ paarweise verschieden. Die $\varphi_i(a)$ sind Nullstellen von $m_a(t) \in K[t]$. Folglich gilt

$$[K(a) : K] = \deg m_a(t) \geq m = [L : K] = [L : K(a)][K(a) : K]$$

also $[L : K(a)] = 1$ und damit $L = K(a)$. □

20. Galoisgruppen

Definition 20.1. Sei $L /\!\!/ K$ eine Körpererweiterung. Dann ist

$$\mathrm{Gal}(L /\!\!/ K) := \{\varphi\colon L \to L \mid \varphi \ K\text{-Isomorphismus}\}$$

die Galoisgruppe von $L /\!\!/ K$. Das ist eine Gruppe bezüglich der Komposition von Abbildungen.

Lemma 20.1. $\mathrm{Gal}(L /\!\!/ K) \subseteq A := \{\varphi\colon L \to L \mid \varphi\ K\text{-}Homomorphismus\}$. *Ist $L /\!\!/ K$ algebraisch, dann gilt sogar Gleichheit.*

Beweis. Falls $L /\!\!/ K$ endlich ist, ist für $\varphi \in A$ die Abbildung φ injektiv und, da $L /\!\!/ K$ endlich ist, bijektiv.

Falls $L /\!\!/ K$ nicht endlich, aber algebraisch ist, betrachten wir $a \in L$ und das zugehörige Minimalpolynom $m_a(t) \in K[t]$. Dann ist $\varphi(a)$ Nullstelle von $m_a(t)$ für alle $\varphi \in A$. Sei

$$L' = K(\{\text{Nullstelle von } m_a(t) \text{ in } L\}) \subseteq L.$$

Es gilt $a \in L'$, $\varphi(a) \in L'$ für alle $\varphi \in A$, $\varphi\colon L' \to L'$ und $\varphi(L') = L'$, weil φ Nullstellen permutiert. Folglich existiert ein Urbild von a unter φ; damit ist $\varphi \in A$ surjektiv und automatisch auch injektiv. Also ist φ bijektiv und $\varphi \in \mathrm{Gal}(L /\!\!/ K)$. □

Definition 20.2. Sei G eine Gruppe, X eine Menge und $G \circlearrowright X$ eine Operation von G auf X. Diese heißt

1. treu, falls $(\forall x \in X : g.x = x) \Rightarrow g = e$ gilt.
2. transitiv, falls $\forall x, y \in X : \exists g \in G : g.x = y$ gilt.

Satz 20.2. *Sei K Körper und $f \in K[t]$ irreduzibel. Sei L Zerfällungskörper von f über K. Dann operiert $G := \mathrm{Gal}(L /\!\!/ K)$ auf $X := \{$Nullstellen von f in $L\}$ treu und transitiv durch $\varphi.x = \varphi(x)$ für $\varphi \in G, x \in X$.*

Beweis.

Wohldefiniertheit der Operation: Für $y \in X$ gilt $\varphi(y) \in X$ für alle $\varphi \in G$, also ist $\varphi.y$ wohldefiniert. Seien $\varphi_1, \varphi_2 \in G$ sowie $x \in X$ beliebig. Dann gilt sowohl $(\varphi_1 \circ \varphi_2).x = (\varphi_1 \circ \varphi_2)(x) = \varphi_1(\varphi_2(x)) = \varphi_1.(\varphi_2.x)$ als auch $e.x = \mathrm{id}_L\,.x = \mathrm{id}_L(x) = x$; G operiert also tatsächlich auf X.

treu: Sei $\varphi \in G$. Da $L = K(a_1, \ldots, a_n)$ mit a_i als den Nullstellen von f gilt, folgt aus $\forall x \in X : \varphi.x = x$ dann $\forall 1 \leq i \leq n : \varphi(a_i) = a_i$. Da aber $\varphi \in G$ durch $\varphi(a_i)$ für $1 \leq i \leq n$ bereits eindeutig bestimmt ist, ist also $\varphi = \mathrm{id}_L = e$.

transitiv: Seien $x, y \in X$. Dann existiert genau ein K-Homomorphismus $\varphi\colon K(x) \to \overline{K}$ mit $\varphi(x) = y$. Nach dem Fortsetzungssatz existiert genau ein K-Homomorphismus $\hat{\varphi}\colon L \to \overline{K}$ mit $\hat{\varphi}|_{K(x)} = \varphi$. Da L ein Zerfällungskörper, also $L /\!\!/ K$ normal ist, ist $\hat{\varphi}(L) = L$ und somit existiert genau ein K-Homomorphismus $\varphi\colon L \to L$ mit $\varphi(x) = y$. Daraus folgt $\varphi.x = y$.

□

Bemerkung. Hat f genau n Nullstellen (in L), so gilt

$$\mathrm{Gal}(L /\!\!/ K) < S_n \cong \{\text{Permutationen der Nullstellen von } f\}.$$

21. Galoiserweiterungen

Definition 21.1. Eine Körpererweiterung $L /\!\!/ K$ heißt Galoiserweiterung, falls sie normal und separabel ist.

In diesem Fall gilt nach Lemma 20.1

$$\mathrm{Gal}(L /\!\!/ K) = \mathrm{Aut}(L /\!\!/ K) = \{\varphi\colon L \to L \mid \varphi\ K\text{-Homomorphismus}\}.$$

Satz 21.1 (Galoiserweiterungen)**.** *Sei $L /\!\!/ K$ endlich. Dann sind äquivalent:*

1. *$L /\!\!/ K$ ist galois.*
2. *$[L : K] = |\mathrm{Gal}(L /\!\!/ K)|$*
3. *$K = L^{\mathrm{Gal}(L/\!\!/K)} := \{x \in L \mid \forall \varphi \in \mathrm{Gal}(L /\!\!/ K) : \varphi(x) = x\}$*
4. *Für alle $a \in L$ ist*
$$m_a(t) = \prod_{b \in \mathrm{Gal}(L/\!\!/K).a} (t - b).$$

[15. Januar 2018]

[18. Januar 2018]

Beweis. Wir setzen $G := \mathrm{Gal}(L /\!\!/ K)$.

$1 \Rightarrow 2$: Sei $L /\!\!/ K$ galois, also insbesondere separabel. Dann folgt nach der Charakterisierung von Separabilität: $[L : K]_{\text{sep}} = [L : K]$. Deshalb gilt mit der Definition des Separabilitätsgrad und aufgrund der Normalität von $L /\!\!/ K$ bereits

$$\begin{aligned}[L : K] = [L : K]_{\text{sep}} &= |\{\varphi\colon L \to \overline{K} \mid \varphi \ K\text{-Homomorphismus}\}| \\ &= |\{\varphi\colon L \to L \mid \varphi \ K\text{-Homomorphismus}\}| \\ &= |\operatorname{Gal}(L /\!\!/ K)|.\end{aligned}$$

$2 \Rightarrow 3$: Offensichtlich ist $K \subseteq L^G \subseteq L$ ein Zwischenkörper. Dabei gilt nun die Ungleichungskette

$$\begin{aligned}[L : L^G] &\geq |\{\varphi\colon L \to L \mid \varphi \ L^G\text{-Homomorphismus}\}| = |\operatorname{Gal}(L /\!\!/ L^G)| \\ &\geq |G| = [L : K] \geq [L : L^G],\end{aligned}$$

wobei die erste Ungleichung dem aufmerksamen Leser als Übung überlassen bleibt. Da nun überall Gleichheit folgt, gilt $[L : L^G] = [L : K]$ und somit $K = L^G$.

$3 \Rightarrow 4$: Sei $a \in L$. Dann ist a Nullstelle des Minimalpolynoms $m_a(t) \in K[t]$ von a, und damit auch $\varphi(a)$ für alle $\varphi \in G$. Also teilt

$$f(t) := \prod_{b \in G.a = \{\varphi(a) \mid \varphi \in G\}} (t - b)$$

dann $m_a(t) \in L[t]$. Sei $f(t) = \sum_{i \geq 0} c_i t^i$. Für $\varphi \in G$ definieren wir $\varphi_*(f) := \sum_{i \geq 0} \varphi(c_i) t^i$. Andererseits ist $\varphi_*(f) = \prod_{b \in G.a}(t - \varphi(b)) = \prod_{b \in G.a}(t - b) = f$. Also muss $\varphi(c_i) = c_i$ für alle i gelten (und zwar für alle $\varphi \in G$). Damit ist $c_i \in L^G$ für alle i; nach Voraussetzung gilt $f \in K[t]$; $m_a(t)$ teilt folglich $f(t)$. Insgesamt gilt daher $m_a(t) = f(t)$.

$4 \Rightarrow 1$: Für alle a in L zerfällt $m_a(t)$ nach Voraussetzung in Linearfaktoren über L und hat keine mehrfachen Nullstellen. Also ist $L /\!\!/ K$ separabel.

Sei nun $f \in K[t]$ irreduzibel. Sei $f(a) = 0$ für ein $a \in L$. Da f irreduzibel ist und $f(a) = 0$, ist $f = \varepsilon m_a(t)$ mit $\varepsilon \in K^\times$. Da $m_a(t)$ über L in Linearfaktoren zerfällt, zerfällt auch f; $L /\!\!/ K$ ist also normal. Damit ist $L /\!\!/ K$ galois. □

Beispiel 1 (Berechnung der Galoisgruppe)**.** Sei L der Zerfällungskörper von $f(t) = t^3 - 2 \in \mathbb{Q}[t]$. Sei $K := \mathbb{Q}$. f hat 3 Nullstellen in L, nämlich $\sqrt[3]{2}, \sqrt[3]{2}\zeta, \sqrt[3]{2}\zeta^2$, wobei $\zeta = e^{\frac{2\pi i}{3}}$. Man beachte $\mathbb{Q}[\sqrt[3]{2}] \subseteq \mathbb{R}$. Nach Satz 20.2 ist $\operatorname{Gal}(L /\!\!/ K) \subseteq S_3$. Nun betrachte den surjektiven Ringhomomorphismus

$$\begin{aligned}\text{ev} := \text{ev}_{\sqrt[3]{2}}\colon \mathbb{Q}[t] &\longrightarrow \mathbb{Q}[\sqrt[3]{2}] \\ t &\longmapsto \sqrt[3]{2} \\ g(t) &\longmapsto g(\sqrt[3]{2})\end{aligned}$$

Er induziert einen Ringhomomorphismus $\overline{\text{ev}}\colon \mathbb{Q}[t]/(t^3 - 2) \to \mathbb{Q}(\sqrt[3]{2})$ nach Homomorphiesatz, welcher nachwievor surjektiv ist. Da $t^3 - 2$ irreduzibel ist, ist $\mathbb{Q}[t]/(t^3 - 2)$

ein Körper. Damit ist $\overline{\mathrm{ev}}$ injektiv, also bijektiv und damit ein Körperisomorphismus. Folglich ist $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = \deg m_{\sqrt[3]{2}}(t) = 3$. Aber L enthält echte komplexe Zahlen, also $[L : \mathbb{Q}(\sqrt[3]{2})] > 1$. Das heißt, dass $[L : \mathbb{Q}] = [L : \mathbb{Q}(\sqrt[3]{2})][\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] \geq 2 \cdot 3 = 6$. Da L Zerfällungskörper von f über K ist, ist $L /\!\!/ K$ also normal und separabel, da $\operatorname{char} \mathbb{Q} = 0$ (und $L /\!\!/ K$ algebraisch) ist. Insgesamt ist $L /\!\!/ K$ galois, und mit Satz 21.1 folgt $6 \leq [L : K] = |\operatorname{Gal}(L /\!\!/ K)| \leq 6$, also $|\operatorname{Gal}(L /\!\!/ K)| = 6$ und damit $\operatorname{Gal}(L /\!\!/ K) \cong S_3$.

22. Galoiskorrespondenz

Satz 22.1 (Galoiskorrespondenz)**.** *Sei $L /\!\!/ K$ eine endliche Galoiserweiterung. Wir setzen $G := \operatorname{Gal}(L /\!\!/ K)$. Dann existiert eine Bijektion*

$$\begin{aligned} \Phi\colon \{\textit{Untergruppen } H < G\} &\overset{1:1}{\longleftrightarrow} \{\textit{Zwischenkörper } K \subseteq M \subseteq L\} \\ H &\longmapsto L^H := \{x \in L \mid \forall \varphi \in H \varphi(x) = x\} \\ \{g \in G \mid \forall m \in M : g(m) = m\} =: H_M &\longmapsto M. \end{aligned}$$

Dabei entsprechen normale Untergruppen $N \lhd G$ genau den Zwischenkörpern $K \subseteq M \subseteq L$ mit $M /\!\!/ K$ normal. In diesem Fall gilt dann $\operatorname{Gal}(M /\!\!/ K) \cong G/N$.

Bemerkung. Φ ist verträglich mit Inklusion in folgender Weise: Sind $H_1, H_2 < G$, so gilt

$$H_1 \subseteq H_2 \iff \Phi(H_1) \supseteq \Phi(H_2).$$

Zum Beweis benötigen wir den folgenden

Satz 22.2. *Sei L ein Körper sowie G eine endliche Gruppe mit $G \subseteq \{\varphi\colon L \to L \mid \varphi \textit{ Körperisomorphismus}\}$. Dann ist $L /\!\!/ L^G$ galois und es gilt $\operatorname{Gal}(L /\!\!/ L^G) = G$.*

Beweis. Sei $K := L^G$ und $n = |G|$. Sei nun $a \in L$. Dann ist $X := \{\varphi(a) | \varphi \in G\}$ eine endliche Menge, da $|G|$ endlich ist. Betrachte $f := f_a := \prod_{b \in X}(t - b)$. Jedes $\varphi \in G$ definiert eine injektive Abbildung $\varphi\colon X \to X$, welche aufgrund der Endlichkeit von X schon bijektiv ist. Weiterhin sei $\varphi_*(f) := \prod_{b \in X}(t - \varphi(b)) = \prod_{b \in X}(t - b) = f$, weshalb $f \in L^G[t] = K[t]$ gilt. Somit ist a Nullstelle von f, f separabel (über K) und es liegen alle Nullstellen von f in L; L ist also Zerfällungskörper von allen f_a mit $a \in L$.

Nach der Charakterisierung von Normalität bzw. der nachfolgenden Bemerkung ist $L /\!\!/ K$ normal und nach Konstruktion separabel. Also ist $L /\!\!/ K = L /\!\!/ L^G$ galois.

Es bleibt $G = \operatorname{Gal}(L /\!\!/ L^G)$ zu zeigen. Dabei ist die Inklusion $G \subseteq \operatorname{Gal}(L /\!\!/ L^G)$ trivial. Weiterhin wissen wir, dass $[K(a) : K] \leq n$ ist, da f_a von $m_a(t)$ geteilt wird und somit $[K(a) : K] = \deg m_a(t) \geq \deg f_a \geq |G| = n$ gilt. Andererseits haben wir $n = |G| \leq |\operatorname{Gal}(L /\!\!/ L^G)| = [L : L^G] = [L : K] \leq n$. Folglich gilt überall Gleichheit und $|G| = |\operatorname{Gal}(L /\!\!/ K)|$, woraus $G = \operatorname{Gal}(L /\!\!/ K)$ folgt. □

Nun folgt der

Beweis der **??**. Sei zunächst $G := \operatorname{Gal}(L /\!\!/ K)$. Der aufmerksame Leser prüft geschwind nach, dass für eine Galoiserweiterung $L /\!\!/ K$ die Körpererweiterungen $L /\!\!/ M$ galois für alle Zwischenkörper $K \subseteq M \subseteq L$ sind. Sei $\Psi\colon M \mapsto H_M$ wie im Satz definiert.

$\Phi \circ \Psi = \mathrm{id}$: Sei M ein Zwischenkörper von K und L. Dann gilt $\Phi(\Psi(M)) = \Phi(H_M) = \Phi(\{g \in G \mid \forall m \in M : g(m) = m\}) = \Phi(\mathrm{Gal}(L /\!\!/ M)) = L^{\mathrm{Gal}(L/\!\!/M)} = M$ nach Satz 22.2, weil $|G|$ und damit auch $|\mathrm{Gal}(L /\!\!/ M)|$ endlich ist.

$\Psi \circ \Phi = \mathrm{id}$: Sei $H < G$. Dann gilt $\Psi(\Phi(H)) = \Psi(L^H) = H_{L^H}$ mit $H_{L^H} = \{g \in G \mid \forall x \in L^H : g(x) = x\} = \mathrm{Gal}(L /\!\!/ L^H) = H$ nach Satz 22.2.

Also ist Φ tatsächlich eine Bijektion.

Es bleibt die Korrespondenz zwischen normalen Untergruppen und normalen Körpererweiterungen zu zeigen. Dazu beweisen wir zunächst, dass für alle $g \in \mathrm{Gal}(L /\!\!/ K)$ dann $g(L^H) = L^{gHg^{-1}}$ für $H < G$ gilt.

„$\subseteq$“: Sei $x \in g(L^H)$. Dann existiert ein $y \in L^H$ mit $x = g(y)$. Für alle $\varphi \in H$ gilt $\varphi(y) = y$, weshalb $(g \circ \varphi \circ g^{-1})(x) = g(\varphi(g^{-1}(x))) = g(\varphi(y)) = g(y) = x$ für alle $\varphi \in H$ gilt. Das bedeutet aber gerade $x \in L^{gHg^{-1}}$.

„$\supseteq$“: Sei x in $L^{gHg^{-1}}$; es gilt also $(g \circ \varphi \circ g^{-1})(x) = x$ für alle $\varphi \in H$, und damit $g^{-1}(x) = \varphi(g^{-1}(x))$ für alle $\varphi \in H$. Setzt man $y := g^{-1}(x) \in L^H$, so ist $x = g(y) \in g(L^H)$.

Sei $H < G$. Dann ist $L^H /\!\!/ K$ genau dann normal, wenn für alle $a \in L^H$ die Nullstellen von $m_a(t)$ in $K[t]$ enthalten sind. Das ist genau dann der Fall, wenn $g(a) \in L^H$ für alle $a \in L^H$ und $g \in G$ gilt, weil G transitiv auf den Nullstellen operiert. Äquivalent dazu ist $g(L^H) = L^H$ für alle $g \in G$, weil $[L : K]$ endlich ist. Nach der Vorbemerkung wissen wir nun aber, dass genau dann $L^H = L^{gHg^{-1}}$, also $H = gHg^{-1}$ für alle $g \in G$ gilt, da Φ bijektiv ist. Das bedeutet aber gerade, dass $H \lhd G$ ein Normalteiler ist.

Schließlich zeigen wir $\mathrm{Gal}(L^H /\!\!/ K) \cong G/H$ für $H \lhd G$. Da $L /\!\!/ K$ nach Voraussetzung separabel ist, ist insbesondere $L^H /\!\!/ K$ separabel. Da $H \lhd G$ gilt, folgt nach dem vorherigen Absatz $g(L^H) = L^H$ für alle $g \in G$, wir erhalten also eine wohldefinierte Abbildung

$$\begin{aligned} \mathrm{res}\colon G &\longrightarrow \mathrm{Gal}(L^H /\!\!/ K) \\ g &\longmapsto g|_{L^H}. \end{aligned}$$

res ist offensichtlich ein Gruppenhomomorphismus mit

$$\ker \mathrm{res} = \{g \in \mathrm{Gal}(L /\!\!/ K) \mid g|_{L^H} = \mathrm{id}_{L^H}\} = \Psi(L^H) = H.$$

Wir erhalten also einen induzierten Gruppenhomomorphismus $\overline{\mathrm{res}}\colon G/H \to \mathrm{Gal}(L^H /\!\!/ K)$, der nach Konstruktion injektiv ist. Außerdem ist $|\mathrm{Gal}(L^H /\!\!/ K)| = [L^H : K]$ nach Satz 21.1 und $[L : K] = [L : L^H][L^H : K]$, wobei $[L : K] = |G|$ nach Satz 21.1 und $[L : L^H] = |H|$ nach Satz 22.2; folglich muss $[L^H : K] = |G/H|$ gelten. Also ist $\overline{\mathrm{res}}$ ein Gruppenisomorphismus zwischen G/H und $\mathrm{Gal}(L^H /\!\!/ K)$. □

[18. Januar 2018]

[22. Januar 2018]

Beispiel 1.

- Sei $\mathbb{C}/\mathbb{R}$ eine Galoiserweiterung vom Grad $[\mathbb{C} : \mathbb{R}] = 2$. Dann gilt $G = \mathrm{Gal}(\mathbb{C}/\mathbb{R})$. Nach Satz 21.1 ist $|G| = 2 \Rightarrow G \cong \mathbb{Z}/2\mathbb{Z}$.
- $f = (t^2 - 2)(t^2 - 3) \in \mathbb{Q}[t]$, L sei der Zerfällungskörper von f. Behauptung: $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ hat Basis über $\mathbb{Q}$: $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$ (Übung).

23. Fundamentalsatz der Algebra

Wir wollen nun die Galoiskorrespondenz verwenden, um den Fundamentalsatz der Algebra mithilfe des Zwischenwertsatzes aus der Analysis zu beweisen.

Satz 23.1 (Fundamentalsatz der Algebra)**.** $\mathbb{C}$ *ist algebraisch abgeschlossen.*

Beweis. Sei $L /\!\!/ \mathbb{C}$ endliche algebraische Körpererweiterung. Es ist $L = \mathbb{C}$ zu zeigen. Da $L /\!\!/ \mathbb{C}$ endlich ist, ist $L /\!\!/ \mathbb{R}$ ebenfalls endlich. Weil $\mathrm{char}\,\mathbb{R} = 0$ ist, ist $L /\!\!/ \mathbb{R}$ separabel. Nach Satz 19.7 können wir $L /\!\!/ \mathbb{R}$ als normal voraussetzen. Damit ist $L /\!\!/ \mathbb{R}$ eine Galoiserweiterung.

Sei $G := \mathrm{Gal}(L /\!\!/ \mathbb{R})$ und $S \subseteq G$ eine 2-Sylowgruppe. $L^S /\!\!/ R$ ist eine endliche, algebraische Körpererweiterung. Außerdem gilt $[L : \mathbb{R}] = [L : L^S][L^S : \mathbb{R}]$, wobei $[L : \mathbb{R}] = |G|$ nach Satz 21.1 und $[L : L^S] = |S|$ nach Satz 22.2, da $S \subseteq G$ eine Untergruppe der endlichen Gruppe G ist. Nach Satz 22.2 ist $L /\!\!/ L^S$ außerdem galois. Nun ist S aber eine 2-Sylowgrppe; folglich ist $[L^S : \mathbb{R}]$ ungerade. Nach dem Satz vom primitiven Element folgt $L^S = \mathbb{R}(a)$ mit $\deg(m_a(t))$ ungerade ($m_a(t) \in \mathbb{R}[t]$). Da $m_a(t)$ ungeraden Grad hat, hat $m_a(t)$ nach dem Zwischenwertsatz mindestens eine Nullstelle in $\mathbb{R}$. Daraus folgt $\deg(m_a(t)) = 1$, weil $m_a(t) \in \mathbb{R}[t]$ irreduzibel ist. Damit ist $L^S = \mathbb{R}$ und $G = S$ insbesondere 2-Gruppe. Da G nun eine 2-Gruppe ist, existiert nach Satz 6.2 eine Normalreihe $\{e\} = G_0 \subseteq G_1 \subseteq G_2 \subseteq \cdots \subseteq G_r = G = \mathrm{Gal}(L /\!\!/ \mathbb{R})$ von Untergruppen mit $r \in \mathbb{N}$, sodass $G_i/G_{i-1} \cong \mathbb{Z}/2\mathbb{Z}$ für alle $1 \leq i \leq r$ gilt.

Mit der **??** erhalten wir eine Sequenz von Körpererweiterungen $L = L^{\{e\}} \supseteq L^{G_1} \supseteq L^{G_2} \supseteq \cdots \supseteq L^{G_r} = L^G = \mathbb{R}$, wobei die letzte Gleichheit aus Satz 21.1 folgt. Setze $L^{G_i} = L_i$. Damit ist $L_i /\!\!/ L_{i+1}$ galois mit der Galoisgruppe G_{i+1}/G_i nach der Korrespondenz von Normalteilern. Insgesamt erhalten wir L also aus $\mathbb{R}$ sukzessive durch endlich viele Körpererweiterungen von Grad 2.

Aber jede Körpererweiterung vom Grad 2 ist durch Adjunktion eines Elementes a mit $\deg(m_a(t)) = 2$ gegeben. Wir wissen, dass jedes quadratische Polynom in $\mathbb{C}[t]$ eine Nullstelle (sogar 2) in $\mathbb{C}$ hat. Folglich kann $\mathbb{C}$ nicht durch quadratische Erweiterungen echt vergrößert werden. Damit ist $L = \mathbb{C}$ (starte mit $\mathbb{R} \subseteq \mathbb{C} = L^{G_{r-1}}$). □

24. Zyklotomische Körper

Sei $n \in \mathbb{Z}_{>0}$ und K ein Körper. Betrachte $f = t^n - 1 \in K[t]$. Frage: Was ist der Zerfällungskörper L von f?

Im Fall $K = \mathbb{C}$ sind die Nullstellen von f genau die n-ten Einheitswurzeln in $\mathbb{C}$. Für $K = \mathbb{R}$ gilt also $L = \mathbb{R}(\{\zeta \mid \zeta \text{ } n\text{-te Einheitswurzel}\}) \subseteq \overline{\mathbb{R}} = \mathbb{C}$. Der Fall $K = \mathbb{Q}$ funktioniert genauso. Was passiert für Körper K mit $\mathrm{char}\,K = p > 0$?

Falls $\operatorname{char} K = p > 0$ und $n = p^s m$ mit $p \nmid m$, dann $f = t^n - 1 = t^{mp^s} - 1 = (t^m - 1)^{p^s}$. Wir sehen: Der Zerfällungskörper von f entspricht dem Zerfällungskörper von $t^m - 1$. Sei nun o.B.d.A.

$$\operatorname{char} K = 0 \text{ oder } (\operatorname{char} K = p \text{ und } p \nmid n) \tag{*}$$

1. Behauptung: $f = t^n - 1 \in K[t]$ mit (*) ist separabel.

   Beweis. Der Fall $\operatorname{char} K = 0$ ist trivial. Sei also $\operatorname{char} K = p$ mit $p \nmid n$. Es gilt $f' = nt^{n-1} \in K[t]$ hat mit (2) nur 0 als Nullstelle; f somit hat keine mehrfachen Nullstellen. □

Sei nun $Z = \{z_1, \dots, z_n\}$ die Menge der Nullstellen von $f \in K[t]$ in $\overline{K}$.

2. Behauptung: $Z \subseteq \overline{K}^\times$ ist eine zyklische Untergrupe.

   Beweis. Offensichtlich ist $e = 1 \in Z$. Sind $z_i, z_j \in Z$, so folgt $(z_i z_j)^n - 1 = z_i^n z_j^n - 1 = 1 \cdot 1 - 1 = 0$, also ist $z_i z_j \in Z$; und es gilt $(z_i^{-1})^n - 1 = (z_i^n)^{-1} - 1 = 1 - 1 = 0$; folglich ist auch $z_i^{-1} \in Z$. Damit ist Z eine Untergruppe von $\overline{K}^\times$. Da $Z < \overline{K}^\times$ endlich ist, ist Z nach Satz 17.3 zyklisch. □

Folglich gilt $Z \cong \mathbb{Z}/n\mathbb{Z}$ als Gruppe, weil nach der 2. Behauptung $|Z| = n$ ist. Damit hat Z genau $\varphi(n)$ verschiedene Erzeuger, da $\varphi(n) = |\{\overline{m} \in \mathbb{Z}/n\mathbb{Z} \mid \operatorname{ggT}(m, n) = 1\}|$ ist. Wir nennen diese Erzeuger von Z die primitive n-ten Einheitswurzeln über K (analog zum Fall $K = \mathbb{C}$). Wähle nun eine solche n-te Einheitswurzel ξ_n.

Lemma 24.1. *Es gelte (*). Der Zerfällungskörper von $f = t^n - 1 \in K[t]$ ist $K(\xi_n)$.*

Beweis. Sei $\xi := \xi_n$. Es gilt $\xi^n = 1$ per Definition. Die ξ^i sind für $1 \le i \le n$ paarweise verschieden, $\xi^i = \xi^j$ mit $1 \le j < i \le n$ in dem Widerspruch $\xi^{i-j} = 1$ resultiert, da $i - j < n$, aber ξ eine primitive n-te Einheitswurzel ist.

Außerdem gilt $(\xi^i)^n - 1 = (\xi^n)^i - 1 = 1 - 1 = 0$; ξ^i ist also eine Nullstelle von f. $K(\xi)$ ist also Zerfällungskörper von f. □

Definition 24.1. Es gelte (*). Der Zerfällungskörper von $f = t^n - 1 \in K[t]$ heißt zyklotomischer Körper der Ordnung n über K.

Lemma 24.2. *Es gelte (*). Sei $f = t^n - 1 \in K[t]$. Sei L Zerfällungskörper von f. Dann ist $G := \operatorname{Gal}(L /\!\!/ K)$ abelsch und $|G|$ teilt $\varphi(n)$.*

Beweis. Wir haben einen Gruppenhomomorphismus

$$\begin{aligned} \varphi\colon G &\longrightarrow \operatorname{Aut}(Z) = \{\varphi\colon Z \to Z \mid \varphi \text{ Gruppenisomorphismus}\} \\ g &\longmapsto g|_Z \end{aligned}$$

wobei Z so wie in der 2. Behauptung oben definiert ist.

Dieser Gruppenhomomorphismus ist injektiv, weil g bereits durch $g|_Z$ eindeutig bestimmt ist, da L der Zerfällungskörper von f ist. Da $Z = \mathbb{Z}/n\mathbb{Z}$ (siehe 2. Behauptung), ist $\operatorname{Aut}(Z) \cong \operatorname{Aut}(\mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$. Folglich ist $\operatorname{Aut}(Z)$ und $\operatorname{im}\varphi < \operatorname{Aut}(Z)$ abelsch; damit ist auch G abelsch. Außerdem teilt $|G| = |\operatorname{Gal}(L /\!\!/ K)|$ dann $|\operatorname{Aut}(\mathbb{Z}/n\mathbb{Z})|$ nach dem Satz von Lagrange, und es gilt $|\operatorname{Aut}(\mathbb{Z}/n\mathbb{Z})| = |(\mathbb{Z}/n\mathbb{Z})^\times| = \varphi(n)$. □

Beispiel 1.

- Seien $K = \mathbb{F}_2$ und $f = t^3 - 1 = (t-1)(t^2+t+1) \in \mathbb{F}_2[t]$, wobei (t^2+t+1) irreduzibel in $\mathbb{F}_2[t]$ ist. Jede Nullstelle $a \neq 1$ von f in $\overline{\mathbb{F}_2}$ ist eine primitive dritte Einheitswurzel. Dann ist $[\mathbb{F}_2(a) : \mathbb{F}_2] = 2$.
- $f = t^7 - 1 = (t-1)(t^3+t^2+1)(t^3+t+1)$. Es existieren 6 primitive 7-te Einheitswurzeln; (t^3+t^2+1) und (t^3+t+1) treten als Minimalpolynome davon auf; im Gegensatz zu $K = \mathbb{Q}$, wo jede primitive n-te Einheitswurzel dasselbe Minimalpolynom hat (siehe Satz 24.4)

[22. Januar 2018]

[25. Januar 2018]

Lemma 24.3. *Sei ξ eine primitive n-te Einheitwurzel über K sowie $m \in \mathbb{Z}$. Dann gilt*

$$\xi^m \text{ primitiv} \iff \operatorname{ggT}(m,n) = 1.$$

Beweis. Sei $f = t^n - 1 \in K[t]$ sowie Z die Menge der Nullstellen von f in $\overline{K}$. Z ist eine zyklische Gruppe bezüglich Multiplikation; Erzeuger sind die primitiven n-ten Einheitswurzeln.

Wir haben also einen Isomorphismus von Gruppen gegeben durch

$$\begin{aligned} \mathbb{Z}/n\mathbb{Z} &\longrightarrow Z \\ \overline{1} &\longmapsto \xi. \end{aligned}$$

Nun ist ξ^m primitiv genau dann, wenn $\operatorname{ord}(\xi^m) = n$, also wenn $\operatorname{ord}(\overline{m}) = n$ in $\mathbb{Z}/n\mathbb{Z}$, was äquivalent zu $\operatorname{ggT}(m,n) = 1$ ist. □

Satz 24.4. *Sei $\xi \in \overline{\mathbb{Q}}$ eine primitive n-te Einheitswurzel (über $\mathbb{Q}$). Dann ist $\mathbb{Q}(\xi) /\!\!/ \mathbb{Q}$ galois und $[\mathbb{Q}(\xi) : \mathbb{Q}] = \varphi(n)$.*

Beweis. Nach Lemma 24.2 wissen wir, dass $\mathbb{Q}(\xi) /\!\!/ \mathbb{Q}$ galois ist und $[\mathbb{Q}(\xi) : \mathbb{Q}] \leq \varphi(n)$ gilt. Es bleibt also zu zeigen,dass für das Minimalpolynom $f = m_\xi(t) \in \mathbb{Q}[t]$ von ξ dann $\deg(f) = \varphi(n)$ gilt.

Dafür reicht es nach Lemma 24.3 zu zeigen, dass jede primitive n-te Einheitswurzel eine Nullstelle von f (über $\overline{\mathbb{Q}}$) ist. Es ist nach der Definition des Minimalpolynoms klar, dass $f \mid t^n - 1$ gilt. Folglich gilt $t^n - 1 = f \cdot h$ in $\mathbb{Q}[t]$ mit normiertem $h \in \mathbb{Q}[t]$. Aus Lemma 24.5 folgt $f, h \in \mathbb{Z}[t]$, da f und h normiert sind.

Sei nun p prim mit $p \nmid n$. Wir behaupten, dass $f(\xi^p) = 0$ gilt. Ist das nicht der Fall, so folgt $h(\xi^p) = 0$, weil $(\xi^p)^n - 1 = 0$ ist. Dann ist ξ eine Nullstelle von $h(t^p)$. Also teilt f schon $h(t^p)$ aufgrund der Definition des Minimalpolynoms und der Normiertheit von h. Damit folgt $h(t^p) = f \cdot g$ für ein normiertes $g \in \mathbb{Q}[t]$. Wieder mit Lemma 24.5 folgt $f, g \in \mathbb{Z}[t]$. Betrachte den Ringhomomorphismus

$$\begin{aligned} \mathbb{Z}[t] &\longrightarrow \mathbb{F}_p[t] = \mathbb{Z}[t]/p\mathbb{Z}[t] \\ \sum_{i \geq 0} c_i t^i &\longmapsto \sum_{i \geq 0} \overline{c_i} t^i. \end{aligned}$$

Damit folgt $\overline{h(t^p)} = \overline{f}\overline{g}$, wobei $\overline{h(t^p)} = \overline{h(t)}^p$ gilt. Folglich haben $\overline{f(t)}$ und $\overline{h(t)}$ eine gemeinsame Nullstelle, sind also nicht teilerfremd. Damit hat $t^n - 1 = \overline{t^n - 1} = \overline{fh}$ eine mehrfache Nullstelle im Widerspruch zu $p \nmid n$. Es folgt sofort $f(\xi^p) = 0$.

Sei nun ξ' eine beliebige primitive n-te Einheitswurzel. Es ist $f(\xi') = 0$ zu zeigen. Sei $\xi' = \xi^m$ ($m \in \mathbb{N}$, $\mathrm{ggT}(m, n) = 1$ nach Lemma 24.3). Wir erhalten die Darstellung $\xi' = \xi^{p_1 \cdots p_r}$ mit $p_1 \dots p_r = m$ und primen p_i mit $p_i \nmid n$ für alle i. Wende nun obiges Argument wiederholt an und erhalte $f(\xi') = f(\xi^{p_1 \cdots p_r}) = 0$. □

Lemma 24.5. *Seien $\beta, \gamma \in \mathbb{Q}[t]$ und $\alpha \in \mathbb{Z}[t]$ mit $\alpha = \beta\gamma$, wobei β und γ normiert sind. Dann folgt bereits $\beta, \gamma \in \mathbb{Z}[t]$.*

Beweis. Seien $\beta = \frac{1}{a}\tilde{\beta}$ mit $\tilde{\beta} \in \mathbb{Z}[t], \tilde{\beta} = \sum_{i=0}^{m} a_i t^i$ und $\gamma = \frac{1}{b}\tilde{\gamma}$ mit $\tilde{\gamma} \in \mathbb{Z}[t], \tilde{\gamma} = \sum_{i=0}^{n} b_i t^i$ mit $a_m \neq 0, b_n \neq 0$ und $\mathrm{ggT}(a_1, \dots, a_m) = 1 = ggT(b_1, \dots, b_n)$.

Damit gilt also $ab\alpha = \tilde{\beta}\tilde{\gamma}$. Wir zeigen nun $a = 1 - b$. Sei dafür p prim mit $p \mid ab$. Nach Reduktion modulo p ergibt sich $0 = \overline{\beta}\overline{\gamma}$ in $\mathbb{F}_p[t]$, also $\overline{\tilde{\beta}} = 0$ oder $\overline{\tilde{\gamma}} = 0$.

Es folgt $\mathrm{ggT}(a_1, \dots, a_m) > 1$ oder $\mathrm{ggT}(b_1, \dots, b_n) > 1$, wobei $a_m = a$, $b_n = b$ nach Voraussetzung. Das ist ein Widerspruch zu obiger Annahme. Folglich existiert kein p mit $p \mid ab$, also $ab = 1$ und $a = \frac{1}{b}$, woraus die Aussage mit obiger Darstellung folgt. □

Definition 24.2. Sei K ein Körper, $n \in \mathbb{Z}_{>0}$ und $\mathrm{char}(K) \nmid n$. Dann sei

$$\Phi_n(t) = \prod_{i=1}^{\varphi(n)} (t - \xi_i) \in \overline{K}[t] \ ,$$

wobei $\xi_1, \dots, \xi_{\varphi(n)}$ die primitiven n-ten Einheitswurzeln über K sind, das n-te Kreisteilungspolynom über K.

Satz 24.6. *Es gelte (*). Dann gilt:*

1. *$\Phi_n(t) \in K[t]$ ist normiert, separabel und vom Grad $\varphi(n)$.*
2. *Für $K = \mathbb{Q}$ ist $\Phi_n(t) \in \mathbb{Z}[t]$ und irreduzibel in $\mathbb{Q}[t]$ und $\mathbb{Z}[t]$.*
3. *$t^n - 1 = \prod_{d \mid n} \Phi_d(t)$*
4. *Das n-te Kreisteilungspolynom $\Phi_{n,K}(t)$ über K erhält man aus $\Phi_n(t) \in \mathbb{Z}[t]$ (dem n-ten Kreisteilungspolynom über $\mathbb{Q}$), indem man auf die Koeffizienten den Ringhomomorphismus gegeben durch $\mathbb{Z} \to K, 1 \mapsto 1$ anwendet.*

Beweis.

1. Normiertheit, Separabilität und $\deg \Phi_n(t) = \varphi(n)$ sind klar.

   Es bleibt $\Phi_k(t) \in K[t]$ zu zeigen. Sei $L = K(\xi_1, \dots, \xi_{\varphi(n)}) = K(\xi_1)$ nach Lemma 24.2. Dann ist $\Phi_n(t) \in L[t]$. Jedes $\varphi \in \mathrm{Gal}(L /\!\!/ K)$ bildet primitive n-te Einheitswurzeln auf ebensolche ab und permutiert somit die primitiven Einheitswurzeln. Also gilt $\varphi_*(\Phi_n(t)) = \Phi_n(t)$ für alle $\varphi \in \mathrm{Gal}(L /\!\!/ K)$. Daraus folgt $\Phi_n(t) \in L^{\mathrm{Gal}(L /\!\!/ K)}[t] = K[t]$ nach Satz 21.1, da $L /\!\!/ K$ galois ist.

2. Sei $K = \mathbb{Q}$. Offensichtlich gilt $m_\xi(t) \in \mathbb{Q}[t]$ und $m_\xi(t) \mid \Phi_n(t)$ für jede primitive n-te Einheitswurzel ξ nach der Definition des Minimalpolynoms.

   Mit Satz 24.4 folgt $\deg(m_\xi(t)) = [\mathbb{Q}(\xi) : \mathbb{Q}] = \varphi(n)$, nach Punkt 1 dieses Satzes gilt also $m_\xi(t) = \Phi_n(t)$, da $\Phi_n(t)$ normiert ist. Daher ist $\Phi_n(t)$ irreduzibel in $\mathbb{Q}[t]$, da $m_\xi(t)$ irreduzibel ist.

   Außerdem teilt $\Phi_n(t)$ das Polynom $t^n - 1$, weil $\Phi_n(t) = m_\xi(t)$ ist. Wir erhalten $t^n - 1 = \Phi_n(t) \cdot h(t) \in \mathbb{Q}[t]$ mit normierten Polynomen $h(t), \Phi_n(t) \in \mathbb{Q}[t]$. Aus Lemma 24.5 folgt nun $\Phi_n(t), h(t) \in \mathbb{Z}[t]$ und damit die Irreduzibilität von $\Phi_n(t) \in \mathbb{Z}[t]$, weil $\Phi_n(t)$ in $\mathbb{Q}[t]$ irreduzibel und primitiv ist.

3. Sei $\mathcal{P}_d$ die Menge der primitiven d-ten Einheitswurzeln. Dann ist $Z = \bigcup_{d|n} \mathcal{P}_d$. Also gilt
$$t^n - 1 = \prod_{d|n} \prod_{\xi \in \mathcal{P}_d} (t - \xi) = \prod_{d|n} \Phi(t).$$

4. Es ist zu zeigen, dass die kanonische Abbildung
$$\begin{array}{rcl} \alpha\colon \mathbb{Z}[t] & \longrightarrow & K[t] \\ \sum_{i\geq 0} b_i t^i & \longmapsto & \sum_{i\geq 0} \mathrm{can}(b_i) t^i \end{array}$$
   (mit dem Ringhomomorphismus $\mathrm{can}\colon \mathbb{Z} \to K, 1 \mapsto 1$) $\Phi_{n,\mathbb{Q}}(t)$ auf $\Phi_{n,K}(t)$ abbildet, wobei $\Phi_{n,\mathbb{Q}}(t)$ in $\mathbb{Z}[t]$ liegt. Beweis per Induktion:

   $n = 1$: Offenbar ist $\mathbb{Z}[t] \ni t - 1 \mapsto t - 1 \in K[t]$ erfüllt.

   $n > 1$: Nach Induktionsannahme sowie Teil 3 des Satzes folgt
$$t^n - 1 = \alpha(t^n - 1) = \alpha(\Phi_{n,\mathbb{Q}}(t)) \prod_{\substack{d|n,\\ d<n}} \Phi_{d,K}(t),$$
   andererseits gilt
$$t^n - 1 = \Phi_{n,K}(t) \prod_{\substack{d|n,\\ d<n}} \Phi_{d,K}(t).$$
   Da K nullteilerfrei ist, impliziert das bereits $\Phi_{n,K}(t) = \alpha(\Phi_{n,\mathbb{Q}}(t))$. □

Lemma 24.7. *Sei $f = t^n - b \in K[t]$ für einen Körper K, sodass K genau n verschiedene Nullstellen von $t^n - 1$ enthält. Sei L der Zerfällungskörper von f. Dann ist* $\mathrm{Gal}(L /\!\!/ K)$ *zyklisch und* $|\mathrm{Gal}(L /\!\!/ K)|$ *teilt n.*

Beweis. Sei $Z \subseteq K$ wie bisher die Menge der Nullstellen von $t^n - 1$. Sei $a \in L$ Nullstelle von f. Dann sind $az_1, az_2, \ldots, az_n$ mit $Z = \{z_1, \ldots, z_n\}$ genau die Nullstellen von f (paarweise verschieden, weil z_i paarweise verschieden sind und $a \neq 0$). Also $L = K(az_1, \ldots, az_n) = K(a)$, da $z_i \in K$.

Seien $\varphi_1, \varphi_2 \in \mathrm{Gal}(L /\!\!/ K)$. Dann gilt $\varphi_1(a) = az_i, \varphi_2(a) = az_j$ für gewisse $i, j \in \{1, \dots, n\}$ und φ_1, φ_2 sind daduruch bestimmt. $\varphi_2 \circ \varphi_1(a) = \varphi_2(az_i) = az_iz_j$. Dann ist

$$\begin{aligned} \mathrm{Gal}(L /\!\!/ K) &\longrightarrow Z \subseteq \overline{K}^\times \\ \varphi &\longmapsto z_j = \frac{\varphi(a)}{a} \end{aligned}$$

ein injektiver Gruppenhomomorphismus. Da Z zyklisch der Ordnung n ist, gilt: $|\mathrm{Gal}(L /\!\!/ K)| = |\operatorname{im}\Psi| \leq |Z| = n$, sogar $|\mathrm{Gal}(L /\!\!/ K)|$ teilt n nach Lagrange. Weil Ψ injektiv ist und Z zyklisch ist, ist $\mathrm{Gal}(L /\!\!/ K)$ zyklisch. □

Hintergrund/Ausblick

Fermats letzter Satz: Sei $n \in \mathbb{N}, n \neq 0$. Existiert ein Tripel $(x, y, z) \in \mathbb{Z}^3$ mit

$$x^n + y^n = z^n \ ?$$

Für $n = 1$ gibt es natürlich unendlich viele Lösungen; für $n = 2$ löst jedes pythagoräische Tripel die Gleichung. Da für $u, v \in \mathbb{Z}$ das Tripel $(u^2 - v^2, 2uv, u^2 + v^2)$ pythagoräisch ist, gibt es auch für $n = 2$ unendlich viele Lösungen.

Fermat behaupete: $x^n + y^n = z^n$ hat für $n > 2$ keine nichttriviale Lösung, was gegen Ende des 20. Jahrhunderts von Andrew Wiles bewiesen wurde.

Wie ist Fermat möglicherweise auf die Idee gekommen, das einfach bewiesen zu haben?

Seien $X, Y \in \mathbb{Z}$ und $n \in \mathbb{Z}_{>0}$, n ungerade. Betrachte den Ausdruck $X^n + Y^n \in \mathbb{Z}[\xi]$, wobei ξ eine primitive n-te Einheitswurzel ist. Mit Lemma 24.7 und durch Nachrechnen erhält man $X^n + Y^n = (X + Y)(X + \xi Y) \dots (X + \xi^{n-1}Y)$.

Falls nun $X^n + Y^n = Z^n \in \mathbb{Z}$ gilt, können wir $X^n + Y^n = p_1 \dots p_r$ als Produkt von Primzahlen schreiben, welche irreduzibel in $\mathbb{Z}[\xi]$ sind. Wenn $\mathbb{Z}[\xi]$ faktoriell wäre (was aber nicht der Fall ist), dann ist das ein Widerspruch zur eindeutigen Zerlegung in irreduzible Elemente.

[25. Januar 2018]

[29. Januar 2018]

25. Inverses Galoisproblem

Wir wissen: Wenn ξ eine primtitve n-te Einheitswurzel ist (über $\mathbb{Q}$ in $\mathbb{C}$), dann ist $\mathbb{Q}(\xi) /\!\!/ \mathbb{Q}$ galois und $\mathrm{Gal}(\mathbb{Q}(\xi) /\!\!/ \mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$.

Falls $n_1, \dots, n_r \in \mathbb{Z}_{>0}$ teilerfremd sind und ε_i eine primitive n_i-te Einheitwurzel ist, dann ist $\varepsilon = \varepsilon_1 \dots \varepsilon_r$ eine primitve $n = n_1 \dots n_r$-te Einheitwurzel (nachprüfen!), also $\mathrm{Gal}(\mathbb{Q}(\varepsilon) /\!\!/ \mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/n_1\mathbb{Z})^\times \times \dots \times (\mathbb{Z}/n_r\mathbb{Z})^\times$, wobei die letzte Isomorphie noch nachzuprüfen ist.

Frage: Welche Gruppen treten als $\mathrm{Gal}(L /\!\!/ \mathbb{Q})$ auf (mit $L /\!\!/ \mathbb{Q}$ etwa endlich oder galois)? Tritt jede endliche Gruppe auf?

Satz 25.1 (Dirichlet)**.** *Sei $n \in \mathbb{Z}_{>0}$. Dann existieren unendlich viele Primzahlen p mit $p \equiv 1 \pmod{n}$.*

Beweis. Wir nehmen an, es existieren nur endlich viele solche Primzahlen, sagen wir $p_1, \dots, p_r$. Sei $m \coloneqq p_1 \dots p_r$. Dann ist

$$\Phi_m(t) \in \mathbb{Z}[t] \text{ normiert und } \Phi(0) \neq 0. \tag{*}$$

Deswegen gilt $\lim\limits_{z\to\infty} \Phi_m(mz) = \infty$ (wobei $z \in \mathbb{N}$). Daraus folgt, dass ein $z_0 \in \mathbb{N}$ existiert, sodass $\Phi_m(mz_0) > p_i$ für alle i gilt. Mit (*) folgt, dass eine Primzahl p mit $p \mid \Phi_m(mz_0)$ und $p \neq p_i$ für alle i existiert. Also gilt $p \mid (mz_0)^m - 1$, aber $p \nmid (mz_0)^m$, weshalb $\operatorname{ggT}(m, p) = 1$ und $\overline{\Phi_m(mz_0)} = 0 \in \mathbb{F}_p$. Nach Lemma 25.2 folgt daraus $p \equiv 1 \pmod{m}$ und mit der Definition von m folgt $p \equiv 1 \pmod{n}$. □

Lemma 25.2. *Sei $m \in \mathbb{Z}_{>0}$, p prim mit $\operatorname{ggT}(m, p) = 1$, wobei $\overline{\Phi_m(t)}$ eine Nullstelle $\overline{a}$ in $\mathbb{F}_p$ mit $a \in \mathbb{Z}$ hat. Dann gilt $p \equiv 1 \pmod{m}$.*

Beweis. p teilt $\Phi_m(a)$, da $\overline{\Phi_m(\overline{a})} = 0$ in $\mathbb{F}_p$. Daraus folgt $p \mid a^m - 1$, also $a^m \equiv 1 \pmod{p}$ und damit $\overline{a}^m = 1 \in \mathbb{F}_p^\times \subseteq \mathbb{F}_p$, wobei $\mathbb{F}_p^\times$ die zyklische Gruppe der Ordnung $p - 1$ ist.

Wir behaupten $\operatorname{ord}(\overline{a}) = m$ in $\mathbb{F}_p^\times$. Da $\overline{a}^m = 1$ ist, gilt auf jeden Fall $\operatorname{ord}(\overline{a}) \leq m$. Angenommen, $\operatorname{ord}(\overline{a}) = s < m$, wobei dann $s | m$ gilt. Nun folgt

$$t^m - 1 = \prod_{d|m} \Phi_d(t) = \Phi_m(t) \prod_{\substack{d|m,\\ d<m}} \Phi_d(t) = \Phi_m(t) \left(\prod_{d|s} \Phi_d(t) \right) h(t) = \Phi_m(t)(t^s - 1)h(t)$$

für ein gewisses $h(t) \in \mathbb{Z}[t]$.

Also gilt $\overline{a}^m - 1 = \overline{\Phi_m(\overline{a})}(\overline{a}^s - 1)\overline{h(\overline{a})}$, wobei die ersten beiden Faktoren beide 0 sind. Somit hat $f(t) = t^m - 1 \in \mathbb{F}_p[t]$ eine mehrfache Nullstelle im Widerspruch zu $f'(t) = mt^{m-1} \in \mathbb{F}_p[t]$, wobei $m \neq 0$ nach Voraussetzung.

Folglich gilt die Behauptung; es ist $\operatorname{ord}(\overline{a}) = m$ und mit dem Satz von Lagrange erhalten wir $m \mid p - 1$, also $p \equiv 1 \pmod{m}$. □

Satz 25.3. *Jede endliche abelsche Gruppe G ist isomorph zu $\operatorname{Gal}(L /\!\!/ \mathbb{Q})$ für eine endliche Galoiserweiterung $L /\!\!/ \mathbb{Q}$.*

Beweis. Sei G eine endliche abelsche Gruppe. Mit den Sylowsätzen und **??** folgt, dass $n_1, \dots, n_r \in \mathbb{Z}_{>0}$ mit $G \cong \mathbb{Z}/n_1\mathbb{Z} \times \dots \times \mathbb{Z}/n_r\mathbb{Z}$ existieren. Nach Dirichlet finden wir paarweise verschiedene Primzahlen p_i $(1 \leq i \leq r)$ mit $p_i \equiv 1 \pmod{n_i}$. Es gilt also $p_i - 1 = m_i n_i$ für gewisse $m_i \in \mathbb{Z}$.

Es sei dem aufmerksamen Leser als Übung überlassen, die Existenz einer Untergrupe $H_i < (\mathbb{Z}/p_i\mathbb{Z})^\times$ der Ordnung m_i mit $(\mathbb{Z}/p_i\mathbb{Z})^\times / H_i = \mathbb{Z}/n_i\mathbb{Z}$ zu zeigen.

Seien nun ε_i für $1 \leq i \leq r$ primitive p_i-te Einheitwurzeln. Sei $\varepsilon = \varepsilon_1 \dots \varepsilon_r$, also eine primitive $p_1 \dots p_r$-te Einheitswurzel und $\mathrm{Gal} \coloneqq \operatorname{Gal}(\mathbb{Q}(\varepsilon) /\!\!/ \mathbb{Q}) \cong (\mathbb{Z}/p_1\mathbb{Z})^\times \times \dots \times (\mathbb{Z}/p_r\mathbb{Z})^\times$. Sei $H < \operatorname{Gal}(\mathbb{Q}(\varepsilon) /\!\!/ \mathbb{Q})$ die Untergruppe, die $H_1 \times \dots \times H_r$ entspricht. Sei $M = L^H$ mit $L = \mathbb{Q}(\varepsilon)$, wobei M ein Zwischenkörper $\mathbb{Q} \subseteq M \subseteq L$ ist. Da Gal abelsch ist,

ist $H < \mathrm{Gal}$ automatisch normal. Die Galoiskorrespondenz sagt uns nun, dass $M /\!\!/ \mathbb{Q}$ normal ist. Da $M /\!\!/ \mathbb{Q}$ außerdem separabel ist (da $\mathrm{char}\,\mathbb{Q} = 0$), ist diese Körpererweiterung galois mit $\mathrm{Gal}(M /\!\!/ \mathbb{Q}) = \mathrm{Gal}\,/H \cong (\mathbb{Z}/p_1\mathbb{Z})^\times/H_1 \times \cdots \times (\mathbb{Z}/p_r\mathbb{Z})^\times/H_r \cong \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z}$. □

Im Allgemeinen ist das inverse Galoisproblem aber ungelöst!

26. Auflösbarkeit von algebraischen Gleichungen

Eine algebraische Gleichung entspricht

$$f(t) = 0$$

für $f(t) = t^n + a_{n-1}t^{n-1} + \cdots + a_1 t + a_0 \in \mathbb{Q}[t]$ (oder $\mathbb{R}[t], \mathbb{C}[t]$).

$n = 1$: $t_1 = -a_0$ (einzige Lösung)

$n = 2$: $t_{1,2} = \frac{-a_1 \pm \sqrt{a_1^2 - 4a_0}}{2} \in \mathbb{C}$. Schon die Babylonier konnten das, allerdings nur geometrisch und nur für bestimmte Werte, weil sie noch nicht so viele Skillz im Wurzelziehen hatten. Im 16. Jahrhundert wurde dann diese allgemeine Formel entdeckt.

$n = 3, 4$: Auch hier gibt es explizite Formeln (entdeckt circa 1550).

Definition 26.1. Sei $L /\!\!/ K$ eine endliche Körpererweiterung. Sie heißt durch Radikale (von lat.: radix, dt.: Wurzel) auflösbar, falls ein $E /\!\!/ K$ existiert mit $L \subseteq E$ und außerdem Körpererweiterungen

$$K = E_0 \subset E_1 \subset E_2 \subset \cdots \subset E_r = E$$

sodass $E_i = E_{i-1}(a_i)$ für ein $a_i \in E_i$, sodass a_i Nullstelle eines Polynoms $Q(t) \in E_{i-1}[t]$ mit

- $Q(t) = t^n - c$, wobei $\mathrm{char}\,K \nmid n$ oder
- $Q(t) = t^p - t - c \in E_{n-1}[t]$ mit $\mathrm{char}\,K = p > 0$.

Definition 26.2. Sei $L /\!\!/ K$ eine endliche Körpererweiterung. Wir nennen $L /\!\!/ K$ auflösbar, falls Körpererweiterungen $K \subseteq L \subseteq E$ existieren, sodass $E /\!\!/ K$ galois und $\mathrm{Gal}(E /\!\!/ K)$ als Gruppe auflösbar ist.

Lemma 26.1. *Sei N die normale Hülle von $L /\!\!/ K$ in $\overline{K}$. Dann ist $L /\!\!/ K$ genau dann auflösbar, wenn $L /\!\!/ K$ separabel und $\mathrm{Gal}(N /\!\!/ K)$ auflösbar ist.*

Beweis.

„⇒“: Sei E wie in der Definition; also ist insbesondere $L /\!\!/ K$ separabel, weil $K \subseteq L \subseteq E$ gilt. Nach dem Fortsetzungssatz ist $\mathrm{res}\colon \mathrm{Gal}(E /\!\!/ K) \to \mathrm{Gal}(N /\!\!/ K), \varphi \mapsto \varphi|_N$ (wohldefiniert aufgrund der Normalität von N) surjektiv. Dabei ist $\mathrm{Gal}(E /\!\!/ K)$ nach Voraussetzung auflösbar. Als Quotient einer auflösbaren Gruppe ist $\mathrm{Gal}(N /\!\!/ K)$ auflösbar.

„⇐“: Per Definition $N /\!\!/ K$ endlich sowie galois mit $\mathrm{Gal}(N /\!\!/ K)$ auflösbar. Man setze nun $E \coloneqq N$. □

Insbesondere gilt, wenn $L /\!\!/ K$ endlich und galois ist, dass $L /\!\!/ K$ genau dann auflösbar ist, wenn $\mathrm{Gal}(L /\!\!/ K)$ auflösbar ist.

Satz 26.2. *Sei $L /\!\!/ K$ eine endliche Körpererweiterung. Dann sind folgende Aussagen äquivalent:*

1. *$L /\!\!/ K$ durch Radikale auflösbar.*
2. *$L /\!\!/ K$ auflösbar.*

Beweis. Bosch: Algebra. □

Korollar 26.3. *Jede separable Körpererweiterung vom Grad $[L : K] \leq 4$ ist (durch Radikale) auflösbar.*

Beweis. Nach dem Satz vom primitiven Element wissen wir $L = K(a)$ für ein $a \in L$. Sei M der Zerfällungskörper von $m_a(t) \in K[t]$. Nun hat $m_a(t) \geq 4$ Nullstellen. Also ist $\mathrm{Gal}(M /\!\!/ K) < S_n$, wobei N die Anzahl der Nullstellen von $m_a(t)$ ist. Da Untergruppen von auflösbaren Gruppen auflösbar sind, reicht es also zu zeigen, dass S_2, S_3, S_4 auflösbar sind. Für S_2, S_3 wissen wir das; für S_4 ist $\{e\} \lhd V_4 \lhd A_4 \lhd S_4$ eine Normalreihe mit abelschen Quotienten. Folglich ist auch S_4 auflösbar. □

Satz 26.4 (Abel-Ruffini)**.** *Im Allgemeinen ist eine Gleichung 5. Grades $f(t) = 0$ nicht auflösbar. (Das heißt, dass der Zerfällungskörper von $f(t)$ über $\mathbb{Q}$ nicht durch Radikale auflösbar ist.)*

Beweis. Eine „allgemeine“ Gleichung n-ten Grades hat Galoisgruppe S_n, es existiert also ein $f(t)$ wie eben von Grad n mit $\mathrm{Gal}(L /\!\!/ \mathbb{Q}) \cong S_n$, wobei L Zerfällungskörper von $f(t)$ ist. Ein Beweis für primes n findet man im Bosch.

Für $n = 5$ (man kann sogar zeigen für $n \geq 5$) ist S_n nicht auflösbar (siehe unten). □

Es kann also keine allgemeine Lösungsformel mit Wurzelausdrücken für Polynome vom Grad 5 geben.

Bemerkung. S_5 ist nicht auflösbar. Wir wissen: $A_5 = [S_5, S_5]$. Es reicht zu zeigen: A_5 ist nicht auflösbar. Dafür reicht es zu zeigen: $A_5 = [A_5, A_5]$.

1. Behauptung: 3-er-Zykel $(a, b, c) \in S_5$ erzeugen A_5 (Übung)
2. Behauptung: Jeder 3-er-Zyklus (i, j, k) lässt sich schreiben als

$$(i,j,k) = (i,k,j)(i,k,j) = (i,k)(k,j)(i,k)(k,j) = \\ (i,k)(l,m)(k,j)(l,m)(l,m)(i,k)(l,m)(k,j) = ghg^{-1}h^{-1}$$

mit $g = (i,k)(l,m)$, $h = (k,j)(l,m)$.