Algebra

Hannah Markwig

gesetzt in LaTeX von

Lukas Schanz

mit

Emma Kraas
Sophie Hoff

Algebra

Inhaltsverzeichnis

1 Gruppen **2**
- 1.1 Operationen . . . 5
- 1.2 Konjugation . . . 16
- 1.3 Isomorphiesätze . . . 23
- 1.4 Direktes und Semidirektes Produkt von Gruppen . . . 29
- 1.5 Sylowsätze . . . 34
- 1.6 Auflösbare Gruppen . . . 46

2 Ringe **51**
- 2.1 Satz von Gauß . . . 56

3 Moduln und der Elementarteilersatz **61**
- 3.1 Matrizen über Ringen und die Smith-Normalform . . . 61
- 3.2 Moduln . . . 66
- 3.3 Endlich präsentierte Moduln . . . 71
- 3.4 Der Elementarteilersatz . . . 74
- 3.5 Die Jordannormalform . . . 79

4 Körper und Konstruierbarkeit **82**
- 4.1 Konstruierbarkeit . . . 82
- 4.2 Zerfällungskörper und algebraischer Abschluß . . . 88
- 4.3 Konstruktion mit Zirkel und Lineal . . . 92
- 4.4 Die Galoisgruppe . . . 104
- 4.5 Normale und separable Körpererweiterung . . . 107
- 4.6 Endliche Körper . . . 110
- 4.7 Die Galoiskorrespondenz . . . 121

5 Anwendungen **129**
- 5.1 Der Fundamentalsatz der Algebra . . . 129
- 5.2 Auflösbarkeit polynomischer Gleichungen . . . 131

6 Literatur **139**

Vorwort

Wir möchten uns an dieser Stelle auch bei Annkathrin Merkt und Benedikt Dilly für ihre Hilfe beim Setzen des Skriptes in LaTeX bedanken.

Hyperlinks:

Dieses Dokument ist für die digitale Verwendung vorgesehen und eignet sich eher weniger zum Ausdrucken.

Es ist mit sogenannten Hyperlinks versehen. Zum Beispiel:

1.1.2

Klickt man auf diese Zahlen, so springt man in der PDF zur Bemerkung 1.1.2.

Oft gibt es in einem Beweis eine Folgerung, die aus einem bestimmten Satz folgt. Wir verwenden:

$$\text{Tatsache } A \overset{1.1.2}{\Rightarrow} \text{Tatsache } B$$

Klickt man hier ebenfalls auf die Zahlen, so springt man wieder zur Bemerkung 1.1.2.

Sollten die Hyperlinks nicht funktionieren: Öffnet die PDF mal in einem anderen Programm dann sollte es klappen :)

Fehler:

Dieses Skript ist sicher nicht fehlerfrei! Daher bitten wir um eure Mithilfe:

Falls euch ein Fehler im Skript auffällt so schickt bitte eine Email an:

schanz.lukas@gmail.com

oder

emma.kraas@student.uni-tuebingen.de

mit genauer Seitenangabe und in welchem Abschnitt er sich befindet. Zum Beispiel:

„Auf Seite 34 ist bei Lemma 1.5.8 folgender Fehler: “

Vorausgesetztes Wissen:

Das Modul Algebra baut auf dem Modul Algebraische Strukturen auf. Dadurch braucht man für alle Kapitel ein gewisses Vorwissen. Vor den Kapiteln befinden sich als Erinnerungshilfe nochmal Kästchen, die das Notwendigste zusammenfassen. Sie haben folgende Form:

Überschrift:

Inhalt welchen man schon aus Algebraische Strukturen kennt

Hin und wieder sind auch sonstige Ergänzungen im Skript, welche nicht in die Nummerierung mit einfließen, in diesen grauen Kästchen gekennzeichnet.

Dokument durchsuchen:

Mit STRG + F kann man das Dokument nach Stichwörtern durchsuchen.

Werbung:

Wer möchte darf sich gerne mal die Website

www.lukasschanz.com

anschauen, das würde mich sehr freuen :)

Dieses Skript wurde das letzte Mal bearbeitet am:

18. August 2020

1 Gruppen

Definition: Gruppe

Eine Gruppe $(G, \circ)$ ist eine Menge G zusammen mit einer Verknüpfung

$$\begin{aligned} \circ : G \times G &\to G \\ (a, b) &\mapsto a \circ b, \end{aligned}$$

die folgende Axiome erfüllt:

(G1): Assoziativität:

$$a \circ (b \circ c) = (a \circ b) \circ c \quad \forall a, b, c \in G.$$

(G2): Existenz des neutralen Elements:

$$\exists\ e \in G : e \circ a = a \circ e = a\ \forall a, b, c \in G$$

(G3): Existenz des Inversen:

$$\forall\ a \in G\ \exists\ a^{-1} \in G : a^{-1} \circ a = a \circ a^{-1} = e$$

G heißt abelsch, falls:

(G4): Kommutativität:

$$a \circ b = b \circ a\ \forall\ a, b \in G$$

Untergruppenkriterium:

Sei $(G, \circ)$ eine Gruppe und $\varnothing \neq U \subset G$ eine nicht-leere Teilmenge. Dann sind folgende Aussagen äquivalent:

(1) U ist eine Untergruppe von G. (Man schreibt $U \leq G$.)

(2) $\forall\ u, v \in U : u \circ v \in U$ und $u_G^{-1} \in U$

(3) $\forall\ u, v \in U : uv_G^{-1} \in U$

Eine Untergruppe ist also eine nicht-leere Teilmenge von G, die selbst wieder eine Gruppe ist.

Definition: Gruppenhomomorphismus

Ein Gruppenhomomorphismus φ zwischen zwei Gruppen $(G, \circ)$ und $(H, *)$ ist eine Abbildung

$$\varphi : G \to H$$

die für alle $a, b \in G$

$$\varphi(a \circ b) = \varphi(a) * \varphi(b)$$

erfüllt, also die Verknüpfungsstruktur erhält.

Definition: Index

Für jede Untergruppe U in G bezeichnet der Index von U in G:

$$[G : U] := |\{aU \mid a \in G\}| = |\{Ua \mid a \in G\}|$$

die Anzahl der verschiedenen Links- bzw. Rechtsnebenklassen von U in G.

Definition: Normalteiler

Eine Untergruppe $U \leq G$ von G heißt Normalteiler, wenn folgende äquivalente Aussagen gelten:

(1) Für alle $g \in G, u \in U$ gilt : $gug^{-1} \in U$

(2) Für alle $g \in G$ gilt: $gU = Ug$ bzw. $gUg^{-1} = U$

(3) Für alle $g, h \in G$ gilt : $(gU) \cdot (hU) = ghU$

Man scheibt $U \trianglelefteq G$.

Beachte:

- Ist G abelsch, so ist jede Untergruppe von G Normalteiler.
- Jede Untergruppe vom Index 2 ist ein Normalteiler.
- Kerne von Gruppenhomomorphismen sind Normalteiler.

Satz von Lagrange:

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

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

Insbesondere gilt: $|U|$ und $\left|{}^{G}\!/_{U}\right| = [G : U]$ Teiler der Gruppenordnung.

Eine umgestellte Variante von dem Satz von Lagrange, welche wir oft verwenden werden,

$$\left|{}^{G}\!/_{U}\right| = \frac{|G|}{|U|}$$

da wir so mit einem Bruch weiter rechnen können.

Definition und Satz: Faktorgruppe

Sei $(G, \circ)$ eine Gruppe und $N \trianglelefteq G$ ein Normalteiler von G. Dann gilt:

(a) Die Menge ${}^{G}\!/_{N} = \{aN \mid a \in G\}$ bildet mit der Multiplikation

$$\cdot : (aN, bN) \mapsto (aN)(bN) = abN$$

eine Gruppe mit neutralem Element $eN = N$ und zu aN Inversem $a^{-1}N$.
Man nennt $\left({}^{G}\!/_{N}, \cdot\right)$ die Faktorgruppe von G nach N

(b) Es gilt $\left|{}^{G}\!/_{N}\right| = [G : N]$

(c) Die Abbildung

$$\begin{aligned} \pi : G &\to {}^{G}\!/_{N} \\ a &\mapsto aN \end{aligned}$$

ist der zu gehörige kanonische Epimorphismus von G nach N mit Kern N.

Homomorphiesatz

Sei $\alpha : G \to H$ ein Gruppenhomomorphismus. Dann ist

$$\begin{aligned} \varphi : {}^{G}\!/_{\mathrm{Kern}(\alpha)} &\to \mathrm{Bild}(\alpha) \\ \overline{g} &\mapsto \alpha(g) \end{aligned}$$

wohldefiniert und ein Isomorphismus. Insbesondere gilt also:

$${}^{G}\!/_{\mathrm{Kern}(\alpha)} \cong \mathrm{Bild}(\alpha)$$

Definition und Satz: Symmetrische Gruppe

Für eine nicht-leere Menge M ist

$$\mathrm{Sym}(M) := \{f : M \to M \mid f \text{ ist bijektiv}\}$$

mit der Kompostion $\circ$ die Symmetrische Gruppe.

Die Elemente von $(\mathrm{Sym}(M), \circ)$ werden auch Permutationen genannt.

Falls $M = \{1, \ldots, n\}$ schreibt man $\mathbb{S}_n$ für $\mathrm{Sym}(M)$

Definition: Zyklische Gruppe

Eine Gruppe G heißt zyklisch, wenn es ein $g \in G$ gibt, sodass das Erzeugnis von g ganz G ist, also:

$$\exists\ g \in G :\ \ G = \langle g \rangle = \{g^n \mid n \in \mathbb{Z}\}$$

Definition: Ordnung

Sei $g \in G$ ein Element einer Gruppe G. Dann heißt

$$\mathrm{ord}(g) = |\langle g \rangle|$$

die Ordnung von g.

1.1 Operationen

1.1.1 Definition: Operation

Sei $(G, *)$ eine Gruppe und M eine Menge. Eine Operation von G auf M ist eine Abbildung

$$\begin{aligned} \bullet : \; & G \times M \to M \\ & (g, m) \mapsto g \bullet m \end{aligned}$$

die folgende Eigenschaften erfüllt:

1. $e \bullet m = m \; \forall m \in M$
2. $(a * b) \bullet m = a \bullet (b \bullet m) \; \forall a, b \in G, \; m \in M$

1.1.2 Bemerkung:

Man kann eine Operation als einen Gruppenhomomorphismus

$$\begin{aligned} \varphi : G \to \mathbb{S}(M) = \{f \mid f : M \to M, \; f \text{ bijektiv}\} \\ g \mapsto \varphi(g) : M \to M \\ m \mapsto \varphi(g)(m) = g \bullet m \end{aligned}$$

auffassen.

Beweis:

„⇒“ – zZ. φ ist wohldefiniert:

$\varphi(g)$ ist injektiv:

$$\begin{aligned} & \varphi(g)(m_1) = \varphi(g)(m_2) \\ \Rightarrow \; & g \bullet m_1 = g \bullet m_2 \\ \Rightarrow \; & g^{-1} \bullet (g \bullet m_1) = g^{-1} \bullet (g \bullet m_2) \\ \Rightarrow \; & (g^{-1} * g) \bullet m_1 = (g^{-1} * g) \bullet m_2 \\ \Rightarrow \; & e \bullet m_1 = e \bullet m_2 \\ \Rightarrow \; & m_1 = m_2 \end{aligned}$$

$\varphi(g)$ ist surjektiv:

Für jedes $m \in M$ ist $g^{-1} \bullet m \in M$, da $\bullet$ eine wohldefinierte Abbildung ist. Es folgt

$$\varphi(g)(g^{-1} \bullet m) = g \bullet (g^{-1} \bullet m) = (g * g^{-1}) \bullet m = e \bullet m = m$$

$\Rightarrow \varphi(g)$ ist bijektiv $\Rightarrow \varphi(g) \in \mathbb{S}(M) \Rightarrow \varphi$ ist wohldefiniert.

– zZ. φ ist ein Gruppenhomomorphismus

$$\begin{aligned} & \varphi(g * h) : \; M \to M : \; m \mapsto (g * h) \bullet m = g \bullet (h \bullet m) \\ & \quad \| \\ & \varphi(g) \circ \varphi(h) : M \to M : \; m \mapsto \varphi(g)(\varphi(h)(m)) = g \bullet (h \bullet m) \end{aligned}$$

„⇐ “ – zZ. φ liefert durch den Gruppenhomomorphismus

$$\begin{aligned} \varphi : G \to \mathbb{S}(M) \\ g \mapsto g \bullet m := \varphi(g)(m) \end{aligned}$$

eine Operation denn:

1. $e \bullet m = \varphi(e)(m) = \mathrm{id}(m) = m$
2. $(g * h) \bullet m = \varphi(g * h)(m) = \varphi(g) \circ \varphi(h)(m) = \varphi(g)(\varphi(h)(m)) = \varphi(g)(h \bullet m) = g \bullet (h \bullet m)$

1.1.3 Beispiele:

1. $(\mathrm{Gl}_n(K), \cdot)$ wobei $\mathrm{Gl}_n(K) = \{\text{invertierbare } n \times n \text{ Matrizen über einem Körper } K\}$ operiert auf $M = K^n$ durch

$$A \bullet x := A \cdot x \quad \text{(Matrixmultiplikation)}$$

denn:

1. $\mathbb{1}_n \bullet x = \mathbb{1}_n \cdot x = x$
2. $(A \cdot B) \bullet x \overset{\text{Def}}{=} (A \cdot B) \cdot x = A \cdot (B \cdot x) \overset{\text{Def}}{=} A \bullet (B \bullet x)$

2. $(\mathbb{S}_n, \circ)$ wobei $\mathbb{S}_n = \mathbb{S}(\{1, ..., n\})$ operiert auf $M = \{1, ..., n\}$ durch

$$\sigma \bullet i := \sigma(i)$$

denn:

1. $\mathrm{id} \bullet i = \mathrm{id}(i) = i$
2. $(\sigma \circ \sigma') \bullet i = \sigma(\sigma'(i)) = \sigma \bullet (\sigma' \bullet i)$

3. $(\mathbb{S}_n, \circ)$ operiert auf $M = \mathbb{R}^n$ durch

$$\sigma \bullet x := A_\sigma \cdot x$$

indem wir für $\sigma \in \mathbb{S}_n$ die Permutation der Einheitsvektoren $e_i \mapsto e_{\sigma(i)}$ linear fortsetzen, zu einer Permutationsmatrix A_σ (in jeder Zeile und Spalte eine 1 und sonst nur Nullen).

$$\text{Bsp.: } n = 3, \quad A_{(1\ 2)} = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

zur Erklärung für $(a, b, c)^t \in \mathbb{R}^3$ gilt dann:

$$\left((1\ 2), \begin{pmatrix} a \\ b \\ c \end{pmatrix} \right) \mapsto A_{(1\ 2)} \begin{pmatrix} a \\ b \\ c \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} a \\ b \\ c \end{pmatrix} = \begin{pmatrix} b \\ a \\ c \end{pmatrix}$$

Denn für $x \in K^n$ gilt:

1. $\mathrm{id} \bullet x = A_{\mathrm{id}} \bullet x = \mathbb{1}_n \cdot x = x$
2. $(\sigma \circ \sigma') \bullet x = (A_\sigma \cdot A_{\sigma'}) \bullet x = (A_\sigma \cdot A_{\sigma'}) \cdot x = A_\sigma \cdot (A_{\sigma'} \cdot x) = \sigma \bullet (\sigma' \bullet x)$

4. Eine Gruppe $(G, *)$ operiert auf $M = G$ durch (also auf sich selbst):

$$\begin{aligned} \bullet : G \times G &\to G \\ (g, h) &\mapsto g \bullet h := g * h \end{aligned}$$

denn:

1. $e \bullet h = e * h = h$
2. $(g_1 * g_2) \bullet h = (g_1 * g_2) * h = g_1 * (g_2 * h) = g_1 \bullet (g_2 \bullet h)$

5. Eine Untergruppe $U \subset G$ operiert auf $(G, *)$ durch

$$\begin{aligned} \bullet : U \times G &\to G \\ (u, g) &\mapsto u \bullet g := u * g \end{aligned}$$

Gruppenoperation: denn

1. $e \bullet g = e * g = g$
2. $(u_1 * u_2) \bullet g = (u_1 * u_2) * g = u_1 * (u_2 * g) = u_1 \bullet (u_2 \bullet g)$

1.1.4 Definiton: treu

Eine Operation $\bullet$ von G auf M heißt <u>treu</u>, wenn eine der folgenden äquivalenten Aussagen gilt:

1.) φ ist injektiv

2.) $\mathrm{Ker}(\varphi) = \{e_G\}$

3.) Nur e_G wird auf $\mathrm{id}_M \in \mathbb{S}_M$ abgebildet

4.) $\forall m \in M: \ g \bullet m = m \ \Rightarrow \ g = e_G$

1.1.5 Beispiele:

Wir betrachten die Beispiele von 1.1.3

1. Wir verwenden Aussage 4.)
$$\forall x \in K^n : \ A \bullet x = x \ \Rightarrow \ A = \mathbb{1}_n$$
deswegen ist die Operation treu.
2. Wir verwenden Aussage 4.)
$$\forall i \in \{1, ..., n\} : \ \sigma \bullet i = i \ \Rightarrow \ \sigma = \mathrm{id}$$
deswegen ist die Operation treu.
3. Wir verwenden Aussage 4.)
$$\forall x \in K^n : \ \sigma \bullet x = x \ \Rightarrow \ \sigma = A_{\mathrm{id}} = \mathbb{1}_n$$
deswegen ist die Operation treu.
4. Wir verwenden Aussage 4.)
$$\forall h \in G : \ g \bullet h = g * h = h \ \Rightarrow \ g = e \ \text{ (Eindeutigkeit neutrales Element)}$$
deswegen ist die Operation treu.
5. gleich wie 4.
6. Seien
$$G = \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \mid \text{obere Dreiecksmatrix, Einträge auf Diagonalen ungleich null} \right\} \leq \mathrm{Gl}_2(K)$$
$$U = \ \langle e_1 \rangle = \left\langle \begin{pmatrix} 1 \\ 0 \end{pmatrix} \right\rangle = \left\{ \lambda \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} \mid \lambda \in \mathbb{R} \right\}$$
und die Operation
$$\begin{aligned} \bullet : G \times U &\to U \\ (A, x) &\mapsto A \bullet x := A \cdot x \end{aligned}$$
welche erfüllt
   1. $\mathbb{1}_2 \bullet x = \mathbb{1}_2 \cdot x = x \ \forall x \in U$
   2. $(A \cdot B) \bullet x = (A \cdot B) \cdot x = A \cdot (B \cdot x) = A \bullet (B \bullet x)$.

   außerdem ist die Operation wohldefiniert, denn
$$A \bullet x = A \cdot x = \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \cdot \begin{pmatrix} \lambda \\ 0 \end{pmatrix} = \begin{pmatrix} \tilde{\lambda} \\ 0 \end{pmatrix} \in U$$
Als Gruppenhomomorphismus betrachtet:
$$\begin{aligned} \varphi : G &\to \mathbb{S}(U) \\ A &\mapsto f_A : U \to U \\ & \qquad x \mapsto f_A(x) := A \cdot x \end{aligned}$$
wobei f_A beschreibt die zugehörige Abbildung zur Matrix A. Es gilt:
$$\mathrm{Kern}(\varphi) = \{A \mid f_A = \mathrm{id}|_U\} = \left\{ \begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix} \right\} \supsetneq \{\mathbb{1}_2\} \ \text{ da } \ \begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix} \begin{pmatrix} a \\ 0 \end{pmatrix} = \begin{pmatrix} a \\ 0 \end{pmatrix}$$
Die Operation ist also nicht treu. Anders gesagt: $\exists \ A \neq \mathbb{1}_2$ mit $A \cdot x = x \ \forall x \in U$,. Zum Beispiel:
$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} a \\ 0 \end{pmatrix} = \begin{pmatrix} a \\ 0 \end{pmatrix}$$

Erinnerung: $\mathbb{R}^n$ ist ein euklidischer Vektorraum. Die orthogonale Gruppe:
$$O(n)=\{\text{orthogonale Matrizen}\} \ (\text{Spalten sind Orthonormalbasis, } A \cdot A^T = \mathrm{id}_n)$$
Es gilt:

A orthogonal $\Leftrightarrow$ f_A orthogonal
$\Leftrightarrow \langle x, y \rangle = \langle f_A(x), f_A(y) \rangle = \langle Ax, Ay \rangle \ \forall x, y \in \mathbb{R}^n$
$\Leftrightarrow$ f_A ist längen- und winkelerhaltend

1.1.6 Definition: affine Isometrien

Die Menge der affinen Isometrien auf $\mathbb{R}^n$ ist

$$E(n) := \{x \mapsto Ax + b \mid A \in O(n), b \in \mathbb{R}^n\}$$

Durch Hintereinanderausführung $\circ$ ist $(E(n), \circ)$ eine Gruppe.

Für $M \subset \mathbb{R}^n$ definieren wir eine Untergruppe von $E(n)$, die auf M operiert:

1.1.7 Definition: Symmetriegruppe

Sei $M \subset \mathbb{R}^n$ eine Teilmenge.

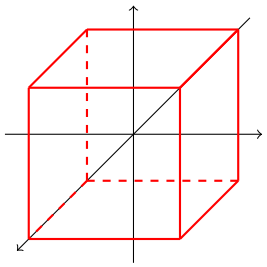
$$\mathrm{Sym}(M) = \{f \in E(n) \mid f(M) = M\}$$

heißt die Symmetriegruppe von M und ihre Elemente Symmetrien.

Beispiel:

Sei

$$Q = \{x \in \mathbb{R}^3 \mid ||x_i|| \leq 1 \ \forall i\}$$



ein Würfel. Da Symmetrien abstandserhaltend sind, muss die Teilmenge der Punkte mit dem größten Abstand zu 0 (also die Eckpunkte) auf sich selbst überführt werden.
Damit ist

$$\mathrm{Sym}(Q) \subset \left\{ \begin{pmatrix} \pm 1 & 0 & 0 \\ 0 & \pm 1 & 0 \\ 0 & 0 & \pm 1 \end{pmatrix} \cdot A_\sigma \mid \sigma \in \mathbb{S}_3 \right\}$$

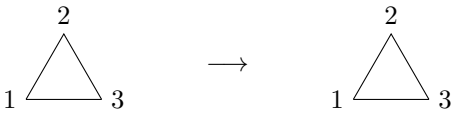
und da jede solche Abbildung in $\mathrm{Sym}(Q)$ ist, gilt Gleichheit.

Beispiel: Die Symmetriegruppe eines gleichseitigen Dreiecks $\triangle \subset \mathbb{R}^2$ ist

$$\mathbb{S}_3 = \{\mathrm{id}, (123), (132), (12), (13), (23)\}$$

und besteht aus:

Drehungen:

id 

Drehung um 0°

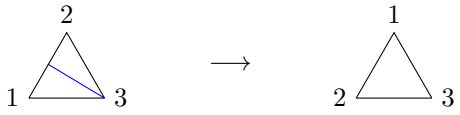
(1 2 3)

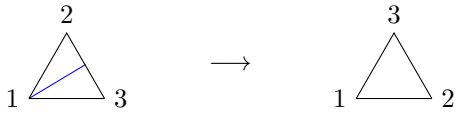
Drehung um $120° = \frac{360°}{3}$

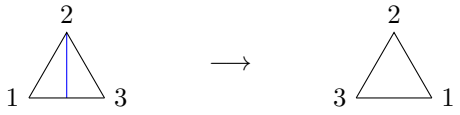
(1 3 2)

Drehung um $240° = 2 \cdot \frac{360°}{3}$

Spiegelungen:

(1 2) 

(2 3) 

(1 3) 

1.1.8 Bemerkung

Für $M \subset \mathbb{R}^n$ definiert

$$\begin{aligned} \bullet : \ & \mathrm{Sym}(M) \times M \to M \\ & (f, m) \mapsto f \bullet m := f(m) \end{aligned}$$

eine Operation, denn

1. $\mathrm{id} \bullet m = \mathrm{id}(m) = m$
2. $(f \circ g) \bullet m = f(g(m)) = f \bullet (g \bullet m))$

1.1.9 Definition: Bahn

Sei $G \times M \to M$ eine Operation.

$$G_m := \{g \bullet m \mid g \in G\} \subset M$$

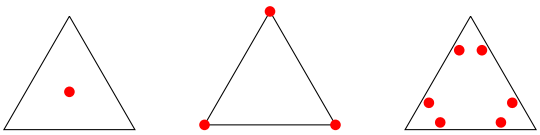
heißt die Bahn von m.

1.1.10 Beispiel

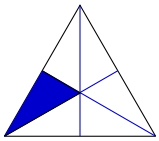
Sei $\triangle$ ein gleichseitiges Dreieck in $\mathbb{R}^n$, wir betrachten die Operation

$$\mathrm{Sym}(\triangle) \times \triangle \to \triangle$$

und Bahnen für verschiedene Punkte:



Man kann die Operation auf die Potenzmenge von $\triangle$ fortsetzen und hier Bahnen betrachten:
Die Bahn des kleinen blauen Dreiecks in $\triangle$ ist z.B.



Die einzelnen Felder können jede beliebige Position eines andern Feldes annehmen, das erreicht man durch Drehung oder Spiegelung.

1.1.11 Beispiel

Es gilt $m\mathbb{Z} \subset \mathbb{Z}$ ist eine Untergruppe bezüglich $+$.
Betrachte die dadurch induzierte Operation

$$\begin{aligned} \bullet : \; & m\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \\ & (mz, a) \mapsto mz \bullet a := mz + a \end{aligned}$$

Die Bahnen dieser Operation sind die Restklassen Modulo (mod) m.

1.1.12 Bemerkung

Man kann eine Untergruppe $U \leq G$ auch von rechts operieren lassen. Durch

$$\begin{aligned} \bullet : \; & U \times G \to G \\ & (u, g) \mapsto u \bullet g := gu \end{aligned}$$

Die Bahnen dieser Operation sind $gU = \{gu \mid u \in U\}$, die Linksnebenklassen.

Für die übliche Operation von links sind die Bahnen, die $Ug = \{ug \mid u \in U\}$, die Rechtsnebenklassen.

Normalteiler sind also Untergruppen, für die die Bahnen unter der Operation von links und rechts gleich sind.

(In dieser Vorlesung werden nur Operationen von links behandelt.)

1.1.13 Definition: Stabilisator

Sei $G \times M \to M$ eine Operation.
Für $N \subset M$ ist

$$\mathrm{Stab}(N) := \{g \in G \mid \{gn \mid n \in N\} =: gN = N\} \subset G$$

der Stabilisator von N.

1.1.14 Beispiel

Siehe: Beispiel 1.1.10

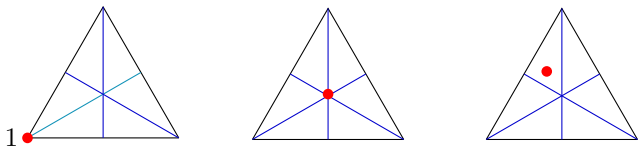


Fig a) *Fig* b) *Fig* c)

a) $\text{Stab}(\{1\}) = \{\text{id}, (2\ 3)\}$
→ id und die Spiegelung um die 23-Achse erhalten den Punkt

b) $\text{Stab}(\bullet) = \mathbb{S}_3$
→ Egal wie gespiegelt oder gedreht wird, der Mittelpunkt wird erhalten

c) $\text{Stab}(\bullet) = \{\text{id}\}$
→ Nur die Identität erhält den Punkt

1.1.15 Bemerkung

$\bigcap_{n \in M} \text{Stab}(\{n\})$ ist die Untergruppe von $\text{Sym}(M)$, die M punktweise festhält.

1.1.16 Lemma: Stab(N) ist eine Untergruppe

Sei $G \times M \to M$ eine Operation und $N \subset M$.

$\Rightarrow \text{Stab}(N)$ ist eine Untergruppe.

Beweis:

Seien $a, b \in \text{Stab}(N)$
$\Rightarrow\ aN = N, bN = N$
$\Rightarrow\ (ab)N = a(bN) = aN = N$
$\Rightarrow\ ab \in \text{Stab}(N)$

und

Sei $a \in \text{Stab}(N)$
$\Rightarrow\ a^{-1}aN = a^{-1}N = (a^{-1}a)N = eN = N$
$\Rightarrow\ a^{-1} \in \text{Stab}(N)$

$\text{Stab}(N) \neq \varnothing$, denn $\text{id} \in \text{Stab}(N)$. □

1.1.17 Lemma: Die Bahnen von zwei Elementen einer Menge sind entweder gleich oder disjunkt

Sei $G \times M \to M$ eine Operation, $m_1, m_2 \in M$.
Dann sind die Bahnen von m_1 und m_2 entweder gleich oder disjunkt, das heißt:

$$G_{m_1} = G_{m_2} \text{ oder } G_{m_1} \cap G_{m_2} = \varnothing$$

Beweis:

Angenommen, $G_{m_1} \cap G_{m_2} \neq \varnothing$
$\Rightarrow\ \exists\ m_3 \in G_{m_1} \cap G_{m_2}$
$\Rightarrow\ \exists\ g_1, g_2 \in G : m_3 = g_1 m_1 = g_2 m_2$
$\Rightarrow\ m_2 = g_2^{-1} g_1 m_1 \in Gm_1$
$\Rightarrow\ G_{m_2} \subset G_{m_1}$ und analog $G_{m_1} \subset G_{m_2}$, also Gleichheit.

□

1.1.18 Beispiel: Die Zerlegung in Bahnen entspricht der Zerlegung in Zykel

$\mathbb{S}_n$ operiert auf $\{1, \ldots, n\}$.

Sei $n = 4$, $\sigma = (1\ 2\ 3)$, dann zerlegt σ die Menge $\{1, 2, 3, 4\}$ in die disjunkten Bahnen $\{1, 2, 3\} \dot\cup \{4\}$.

Sei $n = 5$, $\sigma = (1\ 2\ 3)(4\ 5)$ dann zerlegt σ die Menge $\{1, 2, 3, 4, 5\}$ in die disjunkten Bahnen $\{1, 2, 3\} \dot\cup \{4, 5\}$.

Allgemeiner entspricht die Zerlegung in Bahnen der Zerlegung in Zykel.

1.1.19 Satz von Cayley

Sei G eine Gruppe.

Dann existiert eine Menge M und ein injektiver Gruppenhomomorphismus

$$f : G \to \mathbb{S}(M)$$

Ist G endlich, so kann man M auch endlich wählen.

Insbesondere kann man jede Gruppe als Untergruppe der Permutationsgruppe einer Menge auffassen.

Beweis:

Wir lassen G durch Gruppenoperation auf sich selbst operieren und erhalten dadurch den Gruppenhomomorphismus

$$\begin{aligned} \varphi : \ & G \to \mathbb{S}(G) \\ & g \mapsto \sigma_g : G \to G \\ & \qquad\quad h \mapsto gh \end{aligned}$$

Da die Gruppenoperation treu ist, ist φ injektiv. □

Bemerkung:

Man betrachtet oft Monomorphismen $\varphi : G \to \mathrm{Gl}_n(K)$ so erhält man Darstellungen von G durch Matrizen, diese heißen lineare Darstellungen von G.

1.1.20 Satz:

Sei $G \times M \to M$ eine Operation, $m \in M$, $U = \mathrm{Stab}(m)$. Dann ist folgende Abbildung bijektiv:

$$\begin{aligned} {}^{G}\!/_{U} &\to G_m \\ gU &\mapsto gm \end{aligned}$$

Beweis:

- Wohldefiniertheit:

  Sei $g \sim h$
  $\Rightarrow$ $gU = hU$
  $\Rightarrow$ $\exists\ u \in U :\ gu = h$
  $\Rightarrow$ $hm = (gu)m = g(um) = gm$ (da m von U stabilisiert wird)

- Injektiv:

  $gm = hm$
  $\Rightarrow$ $h^{-1}gm = m$
  $\Rightarrow$ $h^{-1}g$ stabilisiert m
  $\Rightarrow$ $h^{-1}g \in U$
  $\Rightarrow$ $g \sim h$
  $\Rightarrow$ $gU = hU$

- Surjektiv: klar □

1.1.21 Korollar:

Sei G endlich und $G \times M \to M$ eine Operation, $m \in M$, dann gilt

$$|G_m| \cdot |\mathrm{Stab}(m)| = |G|$$

Beweis:

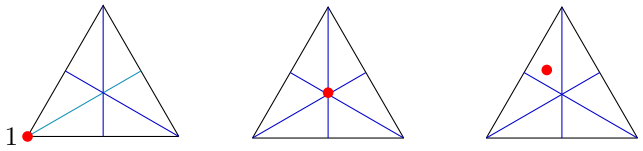
Sei $U = \mathrm{Stab}(m)$.

$$|G_m| \cdot |U| \overset{1.1.20}{=} \left|{}^{G}\!/_{U}\right| \cdot |U| \overset{\text{Lagrange: } 1}{=} |G|$$

□

1.1.22 Beispiel:

Im gleichseitigen Dreieck $\triangle \subset \mathbb{R}^2$ mit der Operation von Sym($\triangle$) gilt: (Siehe 1.1.10 und 1.1.14)



Bahnlänge	3	1	6
|Stab|	2	6	1

1.1.23 Satz: Bahnengleichung

Sei M endlich, $G \times M \to M$ eine Operation, $R \subset M$ eine Teilmenge, die aus jeder Bahn genau ein Element enthält. Dann gilt

$$|M| = \sum_{r \in R} \frac{|G|}{|\mathrm{Stab}(r)|} \overset{1.1.21}{=} \sum_{r \in R} |G_r|$$

in Worten: „Die Mächtigkeit von M ist gleich der Summe über die Länge aller Bahnen. “

Beweis:

M ist die disjunkte Vereinigung seiner Bahnen. Für $r \in R$ hat die Bahn G_r folgende Anzahl an Elementen: $\frac{|G|}{|\mathrm{Stab}(r)|}$ wegen Satz 1.1.20. □

Anwendung der Bahnengleichung: Klassifikation von Graphen bis auf Isomorphie:

1.1.24 Definition: Graph

Ein Graph ist ein Paar $G = (V, E)$ aus einer Menge V von Ecken und E von Kanten $E \subset V \times V$.

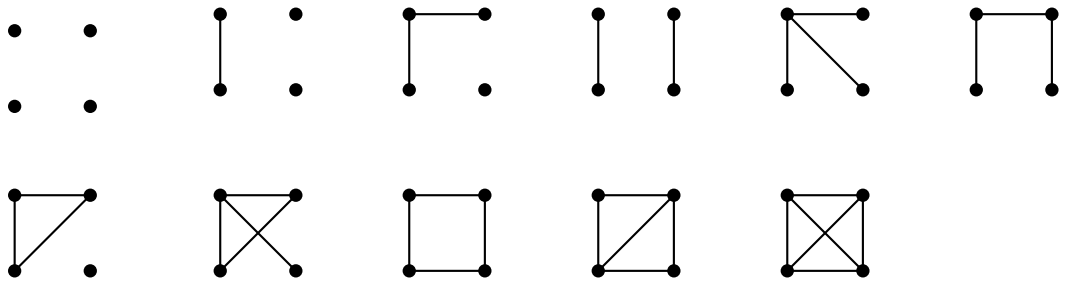
Wir betrachten ungerichtete Graphen, d.h. wir fordern, dass E symmetrisch ist, also aus $(i, j) \in E$ folgt $(j, i) \in E$. Dies steht dann für die Kante zwischen i und j. Wir erlauben keine mehrfachen Kanten und keine Schleifen $(i, i) \notin E \ \ \forall i$.

Ein Isomorphismus von Graphen (V, E), (V', E') ist eine Bijektion $\varphi : V \to V'$, die eine Bijektion $E \to E'$ induziert.

1.1.25 Satz:

Es gibt 11 Isomorphieklassen von Graphen mit 4 Ecken.

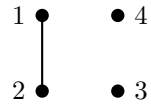
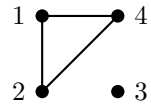
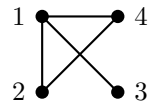
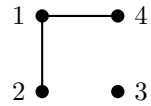
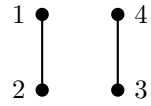
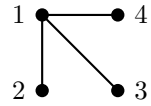
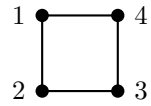
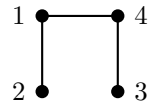
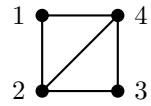
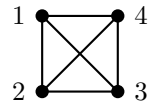
Beweis:



sind paarweise nicht isomorph.

Sei $V = \{1, 2, 3, 4\}$, $M = \{(V, E) \text{ Graph}\}$ und $|M| = 2^6 = 64$, da jede der Kanten $12,\ 13,\ 14,\ 23,\ 24,\ 34$ dabei sein kann oder nicht.

$\mathbb{S}_4$ operiert auf M durch Permutation der Ecken. Wir geben für jeden der 11 Typen den Stabilisator und dann mit Hilfe von Korollar 1.1.21 die Länge der Bahnen an:

Graph	Stabilisator	|Stab|	Bahnlänge
	$\mathbb{S}_4$	24	1
	$\{\mathrm{id}, (1\ 2), (3\ 4), (1\ 2)(3\ 4)\}$	4	6
	$\mathbb{S}_3 = \mathbb{S}(1,2,4)$	6	4
	$\{\mathrm{id}, (2\ 4)\}$	2	12
	$\{\mathrm{id}, (2\ 4)\}$	2	12
	$\{\mathrm{id}, (1\ 2\ 3\ 4), (1\ 3)(2\ 4), (1\ 4\ 2\ 3), (3\ 4), (1\ 2), (1\ 2)(3\ 4), (1\ 4)(2\ 3)\}$	8	3
	$\mathbb{S}_3(2,3,4)$	6	4
	$\{\mathrm{id}, (1\ 2\ 3\ 4), (1\ 3)(2\ 4), (1\ 4\ 3\ 2), (1\ 3), (2\ 4), (1\ 2)(3\ 4), (1\ 4)(2\ 3)\}$	8	3
	$\{\mathrm{id}, (1\ 4)(2\ 3)\}$	2	12
	$\{\mathrm{id}, (2\ 4), (1\ 3), (1\ 3)(2\ 4)\}$	4	6
	$\mathbb{S}_4$	24	1

(Beachte: und liefern die Symmetriegruppe des Quadrats.)

Wir addieren die Bahnenlängen:

$$1 + 6 + 4 + 12 + 12 + 3 + 4 + 12 + 3 + 6 + 1 = 64 = |M|$$

Damit haben wir alle Isomorphieklassen gefunden. □

1.2 Konjugation

1.2.1 Definition: Konjugation und Konjugationsklassen

Sei G eine Gruppe. Die Operation

$$\begin{aligned}\bullet : G \times G &\to G : \\ (g,h) &\mapsto g \bullet h := ghg^{-1}\end{aligned}$$

von G auf sich selbst heißt Konjugation.

Die Bahnen

$$\begin{aligned}h^G &= \{g \bullet h \mid g \in G\} \\ &= \{ghg^{-1} \mid g \in G\}\end{aligned}$$

heißen Konjugationsklassen.

Behauptung: Die Konjugation ist wohldefiniert:

Beweis:

1) $(e,g) \mapsto e \bullet g = ege^{-1} = g$

2) $(g_1g_2, h) \mapsto g_1g_2 \bullet h = g_1g_2h(g_1g_2)^{-1} = g_1g_2hg_2^{-1}g_1^{-1} = g_1(g_2hg_2^{-1})g_1^{-1}$

□

1.2.2 Beispiel:

Die Konjugationsklassen der $\mathbb{S}_n$:
Sei $n = 3$

- {id} ist eine Klasse.
- Klasse von (1 2):

$$\begin{aligned}(1\ 2)(1\ 2)(1\ 2)^{-1} &= (1\ 2) \\ (1\ 3)(1\ 2)(1\ 3)^{-1} &= (2\ 3) \\ (2\ 3)(1\ 2)(2\ 3)^{-1} &= (1\ 3) \\ (1\ 2\ 3)(1\ 2)(1\ 2\ 3)^{-1} = (1\ 2\ 3)(1\ 2)(1\ 3\ 2) &= (2\ 3) \\ (1\ 3\ 2)(1\ 2)(1\ 3\ 2)^{-1} = (1\ 3\ 2)(1\ 2)(1\ 2\ 3) &= (1\ 3)\end{aligned}$$

  ⇒ Wir erhalten alle Transpositionen, $\{(1\ 2), (1\ 3), (2\ 3)\}$

- Klasse von (1 2 3):

$$\begin{aligned}(1\ 2)(1\ 2\ 3)(1\ 2) &= (1\ 3\ 2) \\ (1\ 3)(1\ 2\ 3)(1\ 3) &= (1\ 3\ 2) \\ (2\ 3)(1\ 2\ 3)(2\ 3) &= (1\ 3\ 2) \\ (1\ 2\ 3)(1\ 2\ 3)(1\ 3\ 2) &= (1\ 2\ 3) \\ (1\ 3\ 2)(1\ 2\ 3)(1\ 2\ 3) &= (1\ 2\ 3)\end{aligned}$$

  ⇒ Wir erhalten alle 3-Zykel, $\{(1\ 2\ 3), (1\ 3\ 2)\}$

Allgemein gilt:

Die Zerlegung in Konjugationsklassen ist die Zerlegung in Zykeltypen:
Für

$$\sigma = c_1 \cdots c_s$$

Zerlegung in disjunkte Zykel der Länge

$$l(c_i) = l_i$$

setzen wir

$$p(z) = (l_1, \ldots, l_s),$$

dies ist eine Partition von n.
Zum Beispiel für $n = 4$:

$$p\left((1\ 2\ 3)\right) = (3, 1)$$
$$p\left((1\ 2)(3\ 4)\right) = (2, 2)$$

$p(\sigma)$ heißt der Zykeltyp von σ.

1.2.3 Satz:

$$\{\text{Konjugationsklassen der } \mathbb{S}_n\} \overset{1:1}{\longleftrightarrow} \{\text{Partitionen von } n\}$$

durch den Zykeltyp.

1.2.4 Definition: Innerer Automorphismus

Sei G eine Gruppe, $g \in G$.

$$\begin{aligned} i_g : G &\to G \\ h &\mapsto ghg^{-1} \end{aligned}$$

bezeichnet den inneren Automorphismus zu g.

(Erinnerung: Ein Automorphismus ist ein bijektiver Endomorphismus.)

Der innere Automorphismus ist wohldefiniert:

Beweis:

- Homomorphismus:

$$\begin{aligned} i_g(h_1 * h_2) &= gh_1h_2g^{-1} \\ &= gh_1g^{-1}gh_2g^{-1} \\ &= i_g(h_1) \cdot i_g(h_2) \end{aligned}$$

- Injektiv:

$$gh_1g^{-1} = gh_2g^{-1}$$

$$\Rightarrow \quad h_1 = h_2$$

- Surjektiv:

$$\begin{aligned} h &= i_g(g^{-1}hg) \\ &= gg^{-1}hgg^{-1} \end{aligned}$$

□

1.2.5 Definition: Konjugation einer Untergruppe

Sei $U \leq G$ eine Untergruppe, $g \in G$, dann ist die Konjugation von U mittels g

$$gUg^{-1} = \{gug^{-1} \mid u \in U\}.$$

1.2.6 Lemma:

$$gUg^{-1} \ \cong \ U$$

Beweis:

Da $gUg^{-1} = i_g(U)$ das Bild unter dem inneren Automorphismus zu g. □

1.2.7 Definition: Konjugationsklassen von Untergruppen

Sei

$$S = \{ U \mid U \text{ in } G \text{ Untergruppe } \}$$

G operiert auf S durch die Konjugation

$$\begin{aligned} \bullet : G \times S &\to S \\ (g, U) &\mapsto g \bullet U := gUg^{-1} \end{aligned}$$

Die Bahnen U^G diese Operation heißen die Konjugationsklassen von Untergruppen.

Die Operation ist wohldefiniert.

Beweis:

1) $(e, U) \mapsto e \bullet U = eUe^{-1} = U$

2) $(gh, U) \mapsto gh \bullet U = ghU(gh)^{-1} = ghUh^{-1}g^{-1}$

□

Bemerkung: Ein Normalteiler ist eine Untergruppe, die invariant unter Konjugation ist, d.h. deren Konjugationsklasse

$$u^G = \{ U \}$$

nur aus einem Element besteht.

1.2.8 Satz:

Sei $G \times M \to M$ eine Operation, $m, n \in G_m$ in der selben Bahn mit $n = gm$.
Dann sind die Stabilisatoren konjugiert.

$$\text{Stab}(n) = g\text{Stab}(m)g^{-1}$$

Beweis:

„$\supset$“ Sei $u \in \text{Stab}(m), u' = gug^{-1}$.
Dann gilt:

$$\begin{aligned} u' \cdot n &= gug^{-1} \cdot n \\ &= gum \\ &= gm \quad (\text{da } u \in \text{Stab}(m)) \\ &= n \end{aligned}$$

$\Rightarrow u' \in \text{Stab}(n)$.

„$\subset$“ Analog mit $m = g^{-1}n$ zeigen wir

$$g^{-1}\text{Stab}(n)g \subset \text{Stab}(m),$$

daraus folgt „$\subset$“ nach Multiplikation von rechts mit g^{-1} und von links mit g. □

Beispiel:

Die $\mathbb{S}_3$ hat 4 Konjugationsklassen von Untergruppen:

- $\{\text{id}\}$
- $\{\langle(1\ 2)\rangle, \langle(1\ 3)\rangle, \langle(2\ 3)\rangle\}$
- $\{\langle(1\ 2\ 3)\rangle\}$
- $\{\mathbb{S}_3\}$

Damit besitzt $\mathbb{S}_3$ Untergruppen jeder Größe, die nach Lagrange theoretisch möglich sind, das heißt für jeden Teiler von $|\mathbb{S}_3|$.

1.2.9 Definition: Zentrum

Sei G eine Gruppe und $g \in G$.

Das Zentrum $Z(G)$ ist :

$$\begin{aligned} Z(G) &= \{g \mid hg = gh \ \forall h \in G\} \\ &= \{g \mid h = ghg^{-1} \ \forall h \in G\} \end{aligned}$$

1.2.10 Lemma:

Sei G eine Gruppe.

Sei

$$\begin{aligned} \varphi : G &\to \mathrm{Aut}(G) \\ g &\mapsto i_g \end{aligned}$$

Dann ist φ ein Homomorphismus mit $\mathrm{Kern}(\varphi) = Z(G)$.
Insbesondere ist $Z(G)$ ein Normalteiler.

Beweis:

Sei $g_1, g_2, h \in G$

Zeige Homomorphismus:

$$\begin{aligned} \varphi(g_1) \circ \varphi(g_2)\ (h) &= i_{g_1} \circ i_{g_2}\ (h) \\ &= i_{g_1}\ (i_{g_2}\ (h)) \\ &= g_1\ (g_2 h g_2^{-1})\ g_1^{-1} \\ &= g_1 g_2 h\ (g_1 g_2)^{-1} \\ &= i_{g_1 g_2}\ (h) \\ &= \varphi(g_1 g_2)\ (h) \end{aligned}$$

□

Zeige $\mathrm{Kern}(\varphi) = Z(G)$:

$$\begin{aligned} g \in \mathrm{Kern}(\varphi) &\Leftrightarrow i_g = id \\ &\Leftrightarrow \forall\ h \in G :\ ghg^{-1} = h \\ &\Leftrightarrow g \in Z(G) \end{aligned}$$

□

1.2.11 Definition: Zentralisator

Der Stabilisator der Konjugationsoperation heißt Zentralisator:

$$Z_G(h) \ = \ \{g \mid ghg^{-1} = h\}$$

Auch für Teilmengen $M \subset G$ heißt:

$$Z_G(M) \ = \ \{g \mid ghg^{-1} = h \ \forall\ h \in M\}$$

der Zentralisator von M.

Der Zentralisator von $M = G$ ist das Zentrum.

1.2.12 Satz: Klassengleichung

Sei G eine Gruppe, $R \subset G$ eine Teilmenge, die aus jeder Konjugationsklasse genau ein Element enthält.

Dann gilt die Klassengleichung:

$$|G| \ = \ |Z(G)| \ + \sum_{r \in R \setminus Z(G)} \frac{|G|}{|Z_G(r)|} \overset{1.1.21}{=} |Z(G)| \ + \sum_{r \in R \setminus Z(G)} |G_r|$$

Beweis:

Aus der Bahngleichung 1.1.23 folgt:

$$\begin{aligned} |G| &= \sum_{r \in R} \frac{|G|}{|\mathrm{Stab}(r)|} \\ &= \sum_{r \in R} \frac{|G|}{|Z_G(r)|} \end{aligned}$$

Die Konjugationsklassen von Elementen im Zentrum sind einelementig, denn:

$$\begin{aligned} gh = hg \ \forall h &\Rightarrow g = hgh^{-1} \ \forall h \\ &\Rightarrow g^G = \{g\} \\ &\Rightarrow Z(G) \subset R \end{aligned}$$

Falls r invariant unter Konjugation folgt

$$Z_G(r) = G \text{ und } \frac{|G|}{|Z_G(r)|} = \frac{|G|}{|G|} = 1$$

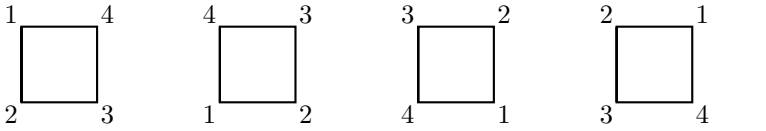
$$\begin{aligned} \Rightarrow |G| &= \sum_{r \in Z(G)} 1 + \sum_{r \in R \setminus Z(G)} \frac{|G|}{|Z_G(r)|} \\ &= |Z(G)| + \sum_{r \in R \setminus Z(G)} \frac{|G|}{|Z_G(r)|} \end{aligned}$$

□

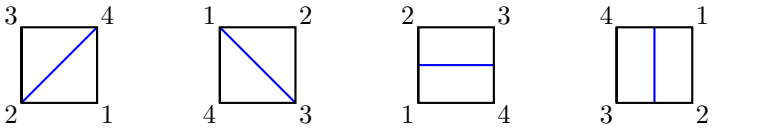
Beispiel:

Sei G die Symmetriegruppe eines Quadrats:

$G = \{$ id , (1 2 3 4) , (1 3)(2 4) , (1 4 3 2) ,



(1 3) , (2 4) , (1 2)(3 4) , (1 4)(2 3) $\}$



Betrachte die Konjugation von G:

r	Konjugationsklasse r^G	Zentralisator $Z_G(r)$
id	$\{\mathrm{id}\}$	G
(1 3)(2 4)	$\{(1\ 3)(2\ 4)\}$	G
(1 3)	$\{(1\ 3), (2\ 4)\}$	$\{\mathrm{id}, (1\ 3), (2\ 4), (1\ 3)(2\ 4)\}$
(1 2)(3 4)	$\{(1\ 2)(3\ 4), (1\ 4)(2\ 3)\}$	$\{\mathrm{id}, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$
(1 2 3 4)	$\{(1\ 2\ 3\ 4), (1\ 4\ 3\ 2)\}$	$\{\mathrm{id}, (1\ 2\ 3\ 4), (1\ 3)(2\ 4), (1\ 4\ 3\ 2)\}$

Hier ist $Z(G) = \{\mathrm{id}, (1\ 3)(2\ 4)\}$

Es gilt:

$$\begin{aligned} \text{Bahngleichung: } 8 &= 1+1+2+2+2 \\ \text{Klassengleichung: } 8 &= \underbrace{2}_{=|Z(G)|} +2+2+2 \end{aligned}$$

1.2.13 Korollar:

Sei G eine Gruppe der Ordnung p^k, p Primzahl, $k > 0$, dann wird $|Z(G)|$ von p geteilt.

Beweis:

$$\begin{aligned} r \notin Z(G) &\Leftrightarrow \exists g \text{ mit } r \neq grg^{-1} \\ &\Leftrightarrow g \notin Z_G(r) \\ &\Leftrightarrow Z_G(r) \subsetneq G \\ &\Leftrightarrow \frac{|G|}{|Z_G(r)|} > 1 \end{aligned}$$

Da $\frac{|G|}{|Z_G(r)|}$ wie $|Z_G(r)|$ ein Teiler von $|G| = p^k$ ist, folgt $p \mid \frac{|G|}{|Z_G(r)|}$.

Damit wird auch

$$\begin{aligned} |Z(G)| &= |G| - \sum_{r \in R \setminus Z(G)} \frac{|G|}{|Z_G(r)|} \\ &= p^k - \text{durch } p \text{ teilbare Zahlen} \end{aligned}$$

durch p geteilt.

(Klassengleichung 1.2.12, R ist eine Menge, die aus jeder Konjugationsklasse genau ein Element enthält.) □

Bemerkung:

Daraus folgt, dass die Symmetriegruppe des Quadrats der Ordnung $8 = 2^3$ mindestens ein weiteres Element neben id im Zentrum besitzt.

Wir haben im Beispiel gesehen, dass dies die Drehung um 180° ist.

1.2.14 Korollar:

Sei G eine Gruppe der Ordnung p^2, p prim. Dann ist G abelsch.

Beweis:

Wegen 1.2.13 wird $|Z(G)|$ von p geteilt, ist also p oder p^2.

$$\begin{aligned} &\text{Falls } |Z(G)| = p^2 \Rightarrow G = Z(G) \text{ und } G \text{ ist abelsch.} \\ &\text{Falls } |Z(G)| = p \Rightarrow \frac{|G|}{|Z(G)|} = p \\ &\qquad\qquad \Rightarrow \left| {}^{G}\!/_{Z(G)} \right| = p \end{aligned}$$

Da $Z(G)$ Normalteiler, ist ${}^{G}\!/_{Z(G)}$ eine Gruppe.

Eine Gruppe von Primzahlordnungen ist zyklisch:

$\Rightarrow \exists\ g:\ {}^{G}\!/_{Z(G)} = \langle gZ(G) \rangle$

Seien $g_1, g_2 \in G$, schreibe $g_i = g^{k_i} \cdot z_i$ mit $z_i \in Z(G)$.

Dann gilt:

$$\begin{aligned} g_1 g_2 &= g^{k_1} z_1 g^{k_2} z_2 \\ &= g^{k_1+k_2} z_1 z_2 \\ &= g^{k_1+k_2} z_2 z_1 \\ &= g^{k_2} z_2 g^{k_1} z_1 \\ &= g_2 g_1 \end{aligned}$$

da die z_i mit jedem Element vertauschen.

Damit ist G abelsch und $G = Z(G)$, $|Z(G)| = p^2$ $\square$

1.3 Isomorphiesätze

1.3.1 Definition: Normalisieren

Sei G eine Gruppe und H, N Untergruppen. Wenn $\forall h \in H: \; hNh^{-1} \subset N$ so wird <u>N von H normalisiert.</u>

Beispiel:

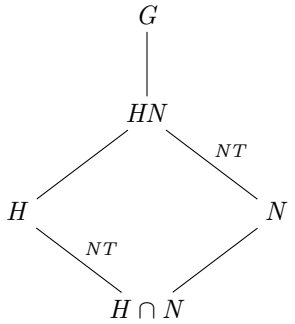
Falls N Normalteiler ist, so wird N von jeder Untergruppe normalisiert.

1.3.2 Lemma:

Sei G eine Gruppe, H, N Untergruppen, N werde von H normalisiert. Dann gilt:

1) $H \cap N$ ist Normalteiler in H
2) $HN = \{hn \mid h \in H, n \in N\}$ ist Untergruppe von G und N ist Normalteiler von HN.

Ein Teil des Untergruppenverbandes ist also:



Beweis:

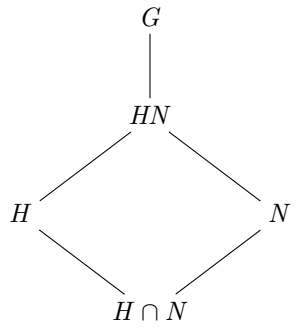
1) Sei $h \in H, n \in H \cap N$, dann gilt $hnh^{-1} \in N$, da H N normalisiert und $hnh^{-1} \in H$, da alle in H sind.
   $\Rightarrow \; hnh^{-1} \in H \cap N$
2) $HN \neq \varnothing$. Sei $hn \in HN$, dann ist $(hn)^{-1} = n^{-1}h^{-1} = h^{-1}\underbrace{hn^{-1}h^{-1}}_{\in N} \in HN$ (da N von H normalisiert wird)
   Seien h_1n_1, $h_2n_2 \in HN$. Dann ist $h_1n_1h_2n_2 = h_1h_2\underbrace{h_2^{-1}n_1h_2}_{\in N}n_2 \in HN$
   $\Rightarrow$ HN ist Untergruppe. (Untergruppenkriterium)
   Sei $hn_1 \in HN$, $n_2 \in N$, dann gilt $h_1n_1n_2(hn_1)^{-1} = \underbrace{h\underbrace{n_1n_2n_1^{-1}}_{\in N}h^{-1}}_{\in N} \in N$
   $\Rightarrow N$ ist Normalteiler □

Beispiel:

1) $G = \mathbb{S}_3$, $H = \{\mathrm{id}, (1\ 2)\}$, $N = \{\mathrm{id}, (1\ 2\ 3), (1\ 3\ 2)\} = \mathbb{A}_3$.
   Dann ist $G = HN$, da (1 2) und (1 2 3) G erzeugen. N ist Normalteiler in $HN = G$.
2) $G = \mathbb{S}_4$, $H = \{\mathrm{id}, (1\ 4)\}$, $N = \{\mathrm{id}, (1\ 2\ 3), (1\ 3\ 2)\}$
   Dann wird N nicht von H normalisiert, denn z.B ist
   $$(1\ 4)(1\ 2\ 3)(1\ 4)^{-1} = (1\ 4)(1\ 2\ 3)(1\ 4) = (2\ 3\ 4) \notin N$$
   Die Menge $HN = N \cup \{(1\ 4), (1\ 2\ 3\ 4), (1\ 3\ 2\ 4)\}$ ist keine Untergruppe, da z.B.
   $$(1\ 2\ 3\ 4)^2 = ((1\ 4)(1\ 2\ 3))^2 = (1\ 3)(2\ 4) \notin HN.$$

1.3.3 Satz: 1. Isomorphiesatz

Sei G eine Gruppe und H, N Untergruppen, so dass N von H normalisiert wird. Dann gilt ${}^{HN}\!/_{N} \cong {}^{H}\!/_{H \cap N}$



Beweis:

Wegen 1.3.2 ist N in HN und $H \cap N$ in H Normalteiler. Setze $\varphi: \; H \hookrightarrow HN \to {}^{HN}\!/_{N}$

φ ist surjektiv, denn für $[hn] = hnN \in {}^{HN}\!/_{N}$ ist $hnN = hN = \varphi(h)$.

$$\begin{aligned}\mathrm{Ker}(\varphi) &= \{h \in H \mid [h] = hN = [e] = N\} \\ &= \{h \in H \mid h \in N\} \\ &= H \cap N\end{aligned}$$

Aus dem Homomorphiesatz folgt

$${}^{H}\!/_{\mathrm{Ker}(\varphi)} = {}^{H}\!/_{H \cap N} \cong \mathrm{Im}(\varphi) = {}^{HN}\!/_{N}$$

□

Beispiel:

$G = \mathbb{Z}$, $H = a\mathbb{Z}$, $N = b\mathbb{Z}$

$$\begin{aligned}&HN = H + N = d\mathbb{Z} \text{ mit } d = \mathrm{ggT}(a, b) \\ &H \cap N = m\mathbb{Z} \text{ mit } m = \mathrm{kgV}(a, b) \\ &H + {}^{N}\!/_{N} = {}^{d\mathbb{Z}}\!/_{b\mathbb{Z}} \cong {}^{\mathbb{Z}}\!/_{\frac{b}{d}\mathbb{Z}} \\ &{}^{H}\!/_{H \cap N} = {}^{a\mathbb{Z}}\!/_{m\mathbb{Z}} \cong {}^{\mathbb{Z}}\!/_{\frac{m}{a}\mathbb{Z}}\end{aligned}$$

Der 1. Isomorphiesatz 1.3.3 besagt hier $\frac{b}{d} = \frac{m}{a} \Leftrightarrow \frac{ab}{d} = m$

1.3.4 Lemma:

Seien $H_2 \subset H_1$ Untergruppen von G. Dann gilt

$$\left|G/H_2\right| = \left|G/H_1\right| \cdot \left|H_1/H_2\right|$$

Beweis:

Wähle einen Vertreter x_i für jede Äquivalenzklasse $[x_i] = x_i H_1$ in G/H_1

Wähle einen Vertreter y_j für jede Äquivalenzklasse $[y_j] = y_j H_2$ in H_1/H_2

- Behauptung: $[x_i y_j] \neq [x_k y_l]$ in G/H_2 $\forall\ (i,j) \neq (k,l)$.

  Angenommen:

  $$\begin{aligned} & [x_i y_j] = [x_k y_l] \\ \Rightarrow\ & x_i y_j H_2 = x_k y_l H_2 \\ \Rightarrow\ & x_k^{-1} x_i y_j H_2 \in y_l H_2 \end{aligned}$$

  Da $y_l \in H_1$ und $H_2 \subset H_1$ folgt $x_k^{-1} x_i y_j \in H_1$ und da $y_j \in H_1$

  $$\begin{aligned} & x_k^{-1} x_i \in H_1 \\ \Rightarrow\ & [x_i] = x_i H_1 = [x_k] = x_k H_1 \\ \Rightarrow\ & \boxed{x_i = x_k} \end{aligned}$$

  nach Wahl der x_m. Aus

  $$[x_i y_j] = x_i y_j H_2 = [x_k y_l] = x_k y_l H_2$$

  folgt dann durch Kürzen $y_j H_2 = y_l H_2$ und nach Wahl der y_n damit $\boxed{y_j = y_l}$.

- Behauptung: Für $g \in G\ \exists\ (i,j):\ [g] = gH_2 = x_i y_j H_2 = [x_i y_j]$.

  $\exists\ x_i:\ [g] = gH_1 = x_i H_1\ \Rightarrow\ x_i^{-1} g \in H_1$

  Für $x_i^{-1} g\ \exists\ y_j:\ x_i^{-1} g H_2 = y_j H_2\ \Rightarrow\ gH_2 = x_i y_j H_2$

Aus den beiden Behauptungen folgt

$$\left|G/H_1\right| = |\{(i,j)\}| = |\{i\}| \cdot |\{j\}| = \left|G/H_1\right| \cdot \left|H_1/H_2\right|$$

□

1.3.5 Satz: 2. Isomorphiesatz

Seien H_1, H_2 Normalteiler von G, $H_2 \subset H_1$. Dann ist ${}^{H_1}\!/_{H_2}$ Normalteiler in ${}^{G}\!/_{H_2}$ und

$$ {}^{G}\!/_{H_2} \Big/ {}^{H_1}\!/_{H_2} \cong {}^{G}\!/_{H_1} $$

Beweis:

$$ \begin{aligned} \varphi : \ {}^{G}\!/_{H_2} &\to {}^{G}\!/_{H_1} \\ aH_2 &\mapsto aH_1 \end{aligned} $$

- φ ist wohldefiniert

$$ \begin{aligned} & aH_2 = bH_2 \\ \Rightarrow \ & b^{-1}a \in H_2 \subset H_1 \\ \Rightarrow \ & bH_1 = aH_1 \end{aligned} $$

- φ ist ein surjektiver Gruppenhomomorphismus

$$ \mathrm{Ker}(\varphi) = \left\{ aH_2 \in {}^{G}\!/_{H_2} \mid aH_1 = [a] = [e] = H_1 \right\} = \left\{ aH_2 \in {}^{G}\!/_{H_2} \mid a \in H_1 \right\} = {}^{H_1}\!/_{H_2} $$

Erinnerung:

${}^{H_1}\!/_{H_2}$ ist damit Normalteiler, da Kerne von Homomorphismen Normalteiler sind. (Lina 2).

Aus dem Homomorphiesatz folgt

$$ {}^{G}\!/_{H_2} \Big/ \mathrm{Ker}(\varphi) = {}^{G}\!/_{H_2} \Big/ {}^{H_1}\!/_{H_2} \cong {}^{G}\!/_{H_1} \cong \mathrm{Im}(\varphi) = {}^{G}\!/_{H_1} $$

□

Beispiel:

Seien $G = \mathbb{Z}$, $H_2 = ab\mathbb{Z}$, $H_1 = a\mathbb{Z}$ also

$$ {}^{G}\!/_{H_2} = {}^{\mathbb{Z}}\!/_{ab\mathbb{Z}} \qquad {}^{H_1}\!/_{H_2} = {}^{a\mathbb{Z}}\!/_{ab\mathbb{Z}} \cong {}^{\mathbb{Z}}\!/_{b\mathbb{Z}} $$

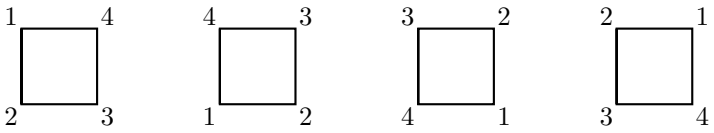
Man erhält:

$$ {}^{\mathbb{Z}}\!/_{ab\mathbb{Z}} \Big/ {}^{\mathbb{Z}}\!/_{b\mathbb{Z}} \cong {}^{G}\!/_{H_1} \cong {}^{\mathbb{Z}}\!/_{a\mathbb{Z}} = {}^{G}\!/_{H_1} $$

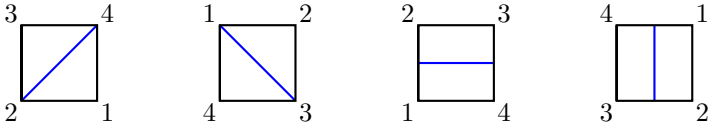
1.3.6 Beispiel:

Sei G = Symmetriegruppe des Quadrats $\subset \mathbb{S}_4$

$G = \{$ id , $(1\ 2\ 3\ 4)$, $(1\ 3)(2\ 4)$, $(1\ 4\ 3\ 2)$,



$(1\ 3)$, $(2\ 4)$, $(1\ 2)(3\ 4)$, $(1\ 4)(2\ 3)$ $\}$



Sei H_1 die Untergruppe der Drehungen. Da $\left|{}^{G}\!/_{H_1}\right| = 2$ ist H_1 Normalteiler. Sei $H_2 = \{\mathrm{id}, (1\ 3)(2\ 4)\} = Z(G)$ also auch Normalteiler.

${}^{G}\!/_{H_2}$ hat 4 Elemente:

$$
\begin{array}{lcccccl}
e & := & H_2 & = & \{\mathrm{id}, (1\ 3)(2\ 4)\} & \widehat{=} & \text{Drehung um } 0°,\ 180° \\
a & := & (1\ 2\ 3\ 4)H_2 & = & \{(1\ 2\ 3\ 4), (1\ 4\ 3\ 2)\} & \widehat{=} & \text{Drehung um } 90°,\ 270° \\
b & := & (1\ 3)H_2 & = & \{(1\ 3), (2\ 4)\} & \widehat{=} & \text{Diagonalspiegelungen} \\
c & := & (1\ 2)(3\ 4)H_2 & = & \{(1\ 2)(3\ 4), (1\ 4)(3\ 2)\} & \widehat{=} & \text{Seitenmittelspiegelungen}
\end{array}
$$

Wir analysieren die Gruppenstruktur von ${}^{G}\!/_{H_2}$. Die möglichen Ordnungen der Elemente sind 1,2,4. Falls ein Element der Ordnung 4 existiere, würde folgen ${}^{G}\!/_{H_2}$ ist zyklisch, also ${}^{Z}\!/_{4\mathbb{Z}}$. Weil ${}^{G}\!/_{H_2} \cong \mathbb{Z}_4 = {}^{\mathbb{Z}}\!/_{4\mathbb{Z}}$

Aber a, b, c haben Ordnung 2. Wir erstellen die Gruppenverknüpfungstabelle:

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

Es gilt $ab \neq a$, denn $b \neq e$ und $ab \neq b$, denn $a \neq e \ \Rightarrow ab = c$.

Genauso: $ac = b,\ ba = c,\ ca = b,\ bc = a,\ cb = a$. Also:

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

Vergleiche dazu die Verknüpfungstabelle der zyklischen Gruppe der Ordnung 4 mit Erzeuger a, $b = a^2$, $c = a^3$, $(e = a^4)$:

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

An der Verknüpfungstabelle erkennen wir:

$$
{}^{G}\!/_{H_2} \cong \{\mathrm{id}, (1\ 2), (3\ 4), (1\ 2)(3\ 4)\} \subset \mathbb{S}_4
$$

Die kleinsche Vierergruppe K_4.

Oder:

$$\begin{aligned}\mathbb{Z}_2 \times \mathbb{Z}_2 &= {}^{\mathbb{Z}}\!/_{2\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{2\mathbb{Z}} \\ &= \{(0,0),(1,0),(0,1),(1,1)\}\end{aligned}$$

$$\begin{aligned}{}^{G}\!/_{H_2} \Big/ {}^{H_1}\!/_{H_2} \cong {}^{G}\!/_{H_1} &= {}^{\{e,a,b,c\}}\!/_{\{e,a\}} \\ &= \{\{e,a\}, b \cdot \{e,a\}\} \\ &\cong {}^{(\mathbb{Z}_2 \times \mathbb{Z}_2)}\!/_{\mathbb{Z}_2} \\ &\cong \mathbb{Z}_2 \\ &\cong {}^{G}\!/_{H_1}\end{aligned}$$

Hierbei ist ein direktes Produkt von Gruppen aufgetaucht, dies wollen wir im Folgenden weiter untersuchen.

1.4 Direktes und Semidirektes Produkt von Gruppen

1.4.1 Definition: Direktes Produkt

Seien $(H_1, \cdot)$, $(H_2, *)$ Gruppen. Das direkte Produkt $(H_1 \times H_2, \circ)$ ist eine Gruppe mit

$$(h_1, h_2) \circ (g_1, g_2) = (h_1 \cdot g_1, h_2 * g_2)$$

1.4.2 Lemma

Seien H_1, H_2 Gruppen.

1) $\tilde{H}_1 := \{(h_1, e_2) \mid h_1 \in H_1\} \subset H_1 \times H_2$ und
   $\tilde{H}_2 := \{(e_1, h_2) \mid h_2 \in H_2\} \subset H_1 \times H_2$
   sind Normalteiler in $H_1 \times H_2$ mit $\tilde{H}_1 \cap \tilde{H}_2 = \{(e_1, e_2)\}$.
   Je zwei Elemente von $\tilde{H}_1$ und $\tilde{H}_2$ vertauschen:
   $$\tilde{h}_1\tilde{h}_2 = \tilde{h}_2\tilde{h}_1 \quad \forall \tilde{h}_1 \in \tilde{H}_1,\ \tilde{h}_2 \in \tilde{H}_2$$

2) $H_1 \times H_2 = \tilde{H}_1\tilde{H}_2$

3) $H_1 \times H_2 / \tilde{H}_1 \cong \tilde{H}_2$
   $H_1 \times H_2 / \tilde{H}_2 \cong \tilde{H}_1$

Beweis:

1) Sei $(g_1, g_2) \in H_1 \times H_2$ und $(h_1, e_2) \in \tilde{H}_1$, dann gilt

   $$\begin{aligned}(g_1, g_2) \cdot (h_1, e_2) \cdot (g_1, g_2)^{-1} &= (g_1, g_2) \cdot (h_1, e_2) \cdot (g_1^{-1}, g_2^{-1}) \\ &= (g_1 h_1 g_1^{-1}, g_2 e_2 g_2^{-1}) \\ &= (g_1 h_1 g_1^{-1}, e_2) \in \tilde{H}_1\end{aligned}$$

   $\Rightarrow \tilde{H}_1$ ist Normalteiler. $\tilde{H}_2$ ebenso.

   Sei $\tilde{h}_1 = (h_1, e_2)$, $\tilde{h}_2 = (e_1, h_2)$

   $$\begin{aligned}\Rightarrow \quad \tilde{h}_1\tilde{h}_2 &= (h_1, e_2)(e_1, h_2) \\ &= (h_1, h_2) \\ &= (e_1, h_2)(h_1, e_2) \\ &= \tilde{h}_2\tilde{h}_1\end{aligned}$$

2) „$\supset$“klar
   „$\subset$ “Sei $(h_1, h_2) \in H_1 \times H_2$
   $\Rightarrow\ (h_1, h_2) = (h_1, e_2) \circ (e_1, h_2) \in \tilde{H}_1 \circ \tilde{H}_2$

3) Aus dem 1. Isomorphiesatz 1.3.3 folgt

   $$H_1 \times H_2 / \tilde{H}_1 = \tilde{H}_1\tilde{H}_2 / \tilde{H}_1 \cong \tilde{H}_2 / \tilde{H}_1 \cap \tilde{H}_2 = \tilde{H}_2 / \{e\} = \tilde{H}_2$$

□

Diese Eigenschaften sind charakteristisch für das direkte Produkt:

1.4.3 Proposition:

Sei G eine Gruppe mit Untergruppen H_1, H_2. Es gilt

1) $H_1 \cap H_2 = \{e\}$

2) je zwei Elemente von $H_1,\ H_2$ vertauschen

3) $H_1 H_2 = G$

Dann ist

$$\begin{aligned} \varphi:\ H_1 \times H_2 &\overset{\cong}{\to} G \\ (h_1, h_2) &\mapsto h_1 h_2 \end{aligned}$$

und $H_1,\ H_2$ sind Normalteiler mit ${}^{G}\!/_{H_1} \cong H_2$ und ${}^{G}\!/_{H_2} \cong H_1$. (Es kann also jedes Element von G eindeutig aus zwei Elementen von H_1 und H_2 geschrieben werden.)

Beweis:

φ ist Homomorphismus, denn

$$\begin{aligned} \varphi((h_1, h_2) \cdot (g_1, g_2)) &= \varphi((h_1 g_1, h_2 g_2)) \\ &= h_1 g_1 h_2 g_2 \\ &\overset{2)}{=} h_1 h_2 g_1 g_2 \\ &= \varphi((h_1, h_2)) \cdot \varphi((g_1, g_2)) \end{aligned}$$

Wegen 3) ist φ surjektiv.

Sei $(h_1, h_2) \in \mathrm{Ker}(\varphi)$

$\Rightarrow\ h_1 h_2 = e$

$\Rightarrow\ h_1 = h_2^{-1}$ mit $h_1 \in H_1,\ h_2^{-1} \in H_2$

$\Rightarrow\ h_1, h_2 \in H_1 \cap H_2 \overset{1)}{=} \{e\}$

$\Rightarrow\ \mathrm{Ker}(\varphi) = \{(e, e)\}$

$\Rightarrow\ \varphi$ ist Isomorphismus

Unter φ gehen $\tilde{H}_1,\ \tilde{H}_2$ aus 1.4.2 auf $H_1,\ H_2$, daher folgt der Rest aus 1.4.2. □

Wir betrachten jetzt eine allgemeinere Konstruktion, bei der 2) weggelassen wird.

1.4.4 Beispiel:

Sei $G = \mathbb{S}_n$, $N = \mathbb{A}_n$. N ist Normalteiler in G, da $\left|{}^{G}\!/_{N}\right| = 2$, bzw. da $N = \mathrm{Ker}(\mathrm{sgn})$. $H = \langle (1\ 2) \rangle \cong \mathbb{Z}_2$.
Es gilt $\mathbb{S}_n = NH$, denn jede Permutation σ ist entweder gerade (und damit in $\mathbb{A}_n = N = Ne$) oder ungerade, aber dann ist $\sigma \circ (1\ 2)$ gerade und in Ne, und damit

$$\sigma = \sigma \circ \mathrm{id} = (\sigma \circ (1\ 2)) \circ (1\ 2) \in N(1\ 2)$$

Aber es gilt nicht $\mathbb{S}_n \cong N \times H$, denn die Tupel vertauschen nicht:
Im direkten Produkt $NH \cong N \times H$ würde gelten

$$n_1 h_1 \cdot n_2 h_2 \mathrel{\widehat{=}} (n_1, h_1)(n_2, h_2) = (n_1 n_2, h_1 h_2) \mathrel{\widehat{=}} n_1 n_2 h_1 h_2$$

aber hier gilt z.B. für $h_1 = h_2 = (1\ 2)$, $n_1 = n_2 = (1\ 2\ 3)$:

$$\begin{aligned} (1\ 2\ 3)(1\ 2)(1\ 2\ 3)(1\ 2) = (1\ 3)(1\ 3) = \mathrm{id} \text{ aber} \\ (1\ 2)(1\ 2)(1\ 2\ 3)(1\ 2\ 3) = (1\ 3\ 2) \neq \mathrm{id} \end{aligned}$$

Wir versuchen, $n_1 h_1 \cdot n_2 h_2$ anders umzuformen:

$$\begin{aligned} n_1 h_1 n_2 h_2 &= n_1 \underbrace{h_1 n_2 h_1^{-1}}_{\in N} h_1 h_2 \quad \text{da } N \text{ Normalteiler} \\ &= n_1 i_{h_1}(n_2) h_1 h_2 \end{aligned}$$

Dies motiviert die folgende Definition:

1.4.5 Definition und Satz: Semidirektes Produkt

Seien H, N Gruppen und

$$\varphi : \ H \to \mathrm{Aut}(N)$$

ein Homomorphismus. Dann ist die Menge $N \times H$ mit der Verknüpfung

$$(n_1, h_1) \cdot (n_2, h_2) := (n_1 \varphi(h_1)(n_2), h_1 h_2)$$

eine Gruppe, das semidirekte Produkt $N \rtimes_\varphi H$ von N und H bezüglich φ.
Man schreibt oft $N \rtimes H$.

$$N \cong N \times \{e_H\} \subset N \rtimes H$$

ist Normalteiler in $N \rtimes H$ und es gilt:

$$N \rtimes H /_N \cong H$$

Beweis:

- Assoziativität

$$\begin{aligned}((n_1, h_1) \cdot (n_2, h_2)) \cdot (n_3, h_3) &= (n_1 \varphi(h_1)(n_2), h_1, h_2) \cdot (n_3, h_3) \\ &= (n_1 \varphi(h_1)(n_2) \cdot \varphi(h_1 h_2)(n_3), h_1 h_2 h_3) \\ &= (n_1 \cdot \varphi(h_1)(n_2) \cdot \varphi(h_1) \circ \varphi(h_2)(n_3), h_1 h_2 h_3) \\ &= (n_1 \cdot \varphi(h_1)(n_2) \cdot \varphi(h_1)(\varphi(h_2)(n_3)), h_1 h_2 h_3) \\ &= (n_1 \cdot \varphi(h_1)(n_2 \varphi(h_2)(n_3)), h_1 h_2 h_3) \\ &= (n_1, h_1)(n_2 \varphi(h_2)(n_3), h_2 h_3) \\ &= (n_1, h_1)((n_2, h_2) \cdot (n_3, h_3))\end{aligned}$$

- Neutrales

$$\begin{aligned}(e_N, e_H) \cdot (n, h) &= (e_N \cdot \varphi(e_H)(n), e_H \cdot h) \\ &= (e_N \cdot \mathrm{id}(n), h) \\ &= (n, h)\end{aligned}$$

- Inverse

  $\varphi(h) \in \mathrm{Aut}(N)$, $\varphi(h)^{-1}$ bezeichne sein Inverses. Damit gilt:

$$\begin{aligned}\left(\left(\varphi(h)^{-1}(n)\right)^{-1}, h^{-1}\right) \cdot (n, h) &= \left(\left(\varphi(h)^{-1}(n)\right)^{-1} \cdot \varphi(h^{-1})(n), h^{-1} h\right) \\ &= \left(\left(\varphi(h)^{-1}(n)\right)^{-1} \cdot \varphi(h)^{-1}(n), e_H\right) \quad \text{da } \varphi \text{ Homomorphismus} \\ &= (e_N, e_H)\end{aligned}$$

Damit ist $N \rtimes H$ eine Gruppe

zZ. N ist Normalteiler: Seien $(n, h) \in N \rtimes H$ und $(m, e_H) \in N$ es gilt:

$$\begin{aligned}(n, h)(m, e_H) \cdot (n, h)^{-1} &= (n, h)(m, e_H) \cdot \left(\left(\varphi(h)^{-1}(n)\right)^{-1}, h^{-1}\right) \\ &= (\cdots, h e_h h^{-1}) \\ &= (\cdots, e_H) \in N\end{aligned}$$

Die Abbildung

$$\Psi: \{e_n\} \times H \hookrightarrow N \rtimes H \to {}^{N \rtimes H}\!/_{N}$$

ist surjektiv, denn jede Klasse $(n,h) \cdot N \times \{e_H\}$ kann man schreiben als $(e_n, h) \cdot N \times \{e_H\}$, indem man den Vertreter mit $\left(\varphi(h)^{-1}(n^{-1}), e_H\right) \in N \times \{e_H\}$ multipliziert.

$$\begin{aligned}(n,h) \cdot \left(\varphi(h)^{-1}(n^{-1}), e_H\right) &= \left(n \cdot \varphi(h)\left(\varphi(h)^{-1}(n^{-1})\right), he_H\right) \\ &= \left(n \cdot \varphi(h) \circ \varphi(h)^{-1}(n^{-1}), h\right) \\ &= (n \cdot \mathrm{id}(n^{-1}), h) \\ &= (nn^{-1}, h) \\ &= (e_N, h)\end{aligned}$$

Der Kern von Ψ ist:

$$\begin{aligned}\mathrm{Ker}(\Psi) &= \{(e_N, h) \mid [(e_N, h)] = (e_N, h) \cdot N \times \{e_H\}\} \\ &= (e_N, e_H) \cdot N \times \{e_H\} \\ &= [(e_N, e_H)] \\ &= \{(e_N, h) \mid (e_N, h) \in N \times \{e_H\}\} \\ &= \{(e_N, e_H)\}\end{aligned}$$

Aus dem Homomorphiesatz folgt:

$$H \cong \{e_N\} \times H = {}^{\{e_N\} \times H}\!/_{\mathrm{Ker}(\Psi)} \cong \mathrm{Im}(\Psi) = {}^{N \rtimes H}\!/_{N}$$

□

1.4.6 Beispiel:

1) Für

$$\begin{aligned}\varphi: H &\to \mathrm{Aut}(N) \\ h &\mapsto \mathrm{id}_N\end{aligned}$$

ist das semidirekte Produkt gleich dem direkten Produkt.

2) Beispiel 1.4.4 zeigt

$$\mathbb{S}_n = \mathbb{A}_n \rtimes_\varphi \mathbb{Z}_2$$

mit

$$\begin{aligned}\varphi: \mathbb{Z}_2 &\to \mathrm{Aut}(\mathbb{A}_n) \\ 0 &\mapsto \mathrm{id} \\ 1 &\mapsto i_{(1\ 2)},\ \text{Konjugation mit } (1\ 2)\end{aligned}$$

denn $\langle (1\ 2) \rangle \cong \mathbb{Z}_2$

3) Sei $N = \mathbb{Z}_3$, $H = \mathbb{Z}_2$ und die Abbildung

$$\begin{aligned}\varphi: H &\to \mathrm{Aut}(N) \\ 0 &\mapsto \mathrm{id} \\ 1 &\mapsto \begin{pmatrix} N \to N \\ x \mapsto -x \end{pmatrix}\end{aligned}$$

Setze

$$\begin{aligned}\Psi: \mathbb{Z}_3 \rtimes_\varphi \mathbb{Z}_2 &\overset{\Psi}{\to} \mathbb{S}_3 \\ (a,0) &\mapsto (1\ 2\ 3)^a \\ (a,1) &\mapsto (1\ 2\ 3)^a (1\ 2)\end{aligned}$$

Behauptung: Ψ ist ein Isomorphismus

Beweis:

- Ψ ist Homomorphismus

  Fallunterscheidung nach dem 2. Eintrag:

  1) $\begin{aligned}\Psi((a,0)+(b,0)) &= \Psi(a+b,0)\\ &= (1\ 2\ 3)^{a+b}\\ &= (1\ 2\ 3)^a \circ (1\ 2\ 3)^b\\ &= \Psi(a,0)\circ\Psi(b,0)\end{aligned}$

  2) $\begin{aligned}\Psi((a,0)+(b,1)) &= \Psi((a+b,1))\\ &= (1\ 2\ 3)^{a+b}(1\ 2)\\ &= (1\ 2\ 3)^a \circ (1\ 2\ 3)^b(1\ 2)\\ &= \Psi(a,0)\circ\Psi(b,1)\end{aligned}$

  3) $\begin{aligned}\Psi((a,1)+(b,0)) &= \Psi(a+\varphi(1)(b),1)\\ &= \Psi(a-b,1)\\ &= (1\ 2\ 3)^{a-b}(1\ 2)\\ &= (1\ 2\ 3)^a(1\ 2\ 3)^{-b}(1\ 2)\\ &= (1\ 2\ 3)^a((1\ 2\ 3)^{-1})^b(1\ 2)\\ &= (1\ 2\ 3)^a(1\ 3\ 2)^b(1\ 2)\\ &= (1\ 2\ 3)^a\,((1\ 2)(1\ 2\ 3)(1\ 2))\,((1\ 2)(1\ 2\ 3)(1\ 2))\cdots((1\ 2)(1\ 2\ 3)(1\ 2))\,(1\ 2)\\ &= (1\ 2\ 3)^a(1\ 2)\,((1\ 2\ 3)(1\ 2)(1\ 2))^b\\ &= (1\ 2\ 3)^a(1\ 2)(1\ 2\ 3)^b\\ &= \Psi(a,1)\circ\Psi(b,0)\end{aligned}$

  4) $\begin{aligned}\Psi((a,1)+(b,1)) &= \Psi(a-b,0)\\ &= (1\ 2\ 3)^{a-b}\\ &= (1\ 2\ 3)^{a-b}(1\ 2)(1\ 2)\\ &= (1\ 2\ 3)^a(1\ 2)(1\ 2\ 3)^b(1\ 2) \quad \text{wie in 3)}\\ &= \Psi(a,1)\circ\Psi(b,1)\end{aligned}$

- Ψ ist surjektiv, denn

  $$(1\ 2\ 3) = \Psi(1,0) \text{ und } (1\ 2) = \Psi(0,1)$$

  sind im Bild und diese erzeugen $\mathbb{S}_3$.

- Ψ ist injektiv

  $\Psi(a,0) = \Psi(a',0)$

  $\Rightarrow\ (1\ 2\ 3)^a = (1\ 2\ 3)^{a'}$

  $\Rightarrow\ a \equiv a' \mod 3$

  $\Rightarrow\ a = a'$ in $\mathbb{Z}/3\mathbb{Z} = \mathbb{Z}_3$

  $\Psi(a,1) = \Psi(a',1)$ genauso

  $\Psi(a,0) = \Psi(a',1)$

  $\Rightarrow\ (1\ 2\ 3)^a = (1\ 2\ 3)^{a'}(1\ 2)$ $\quad \lightning$

  Denn links ist eine gerade Permutation und rechts eine ungerade.

1.5 Sylowsätze

Es gilt mit Lagrange (1) , dass die Ordnung einer Untergruppe die Gruppenordnung teilt.

Es stellt sich die Frage, ob es für jeden Teiler der Gruppenordnung eine Untergruppe gibt?

Dies ist im Allgemeinen unklar, wir werden mittels der Sylowsätze Ergebnisse für Primzahlpotenzen erhalten.

1.5.1 Beispiel

Sei $\mathbb{S}_4 =$ die Symmetriegruppe des Tetraeders. Für diese gilt:

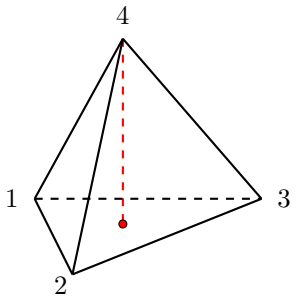
$$|\mathbb{S}_4| = 24 = 2^3 \cdot 3$$

Wir wissen Untergruppen der Ordnung 3 sind zyklisch und werden von einem $3-$Zykel erzeugt.

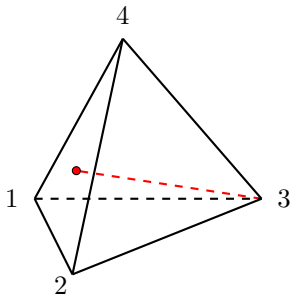
Es gibt also $8 = \frac{4 \cdot 3 \cdot 2}{3}$ $3-$Zykel, von denen jeweils zwei zueinander invers sind.

Damit gibt es dann 4 Untergruppen der Ordnung 3:

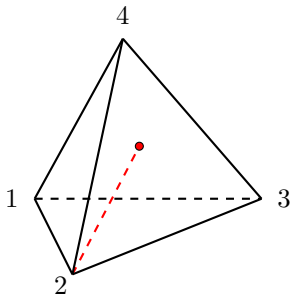
- $\{\mathrm{id}, (1\ 2\ 3), (1\ 3\ 2)\}$



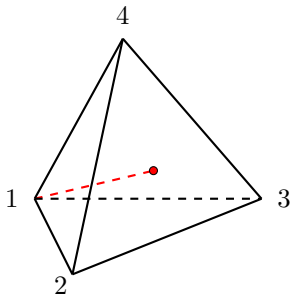
- $\{\mathrm{id}, (1\ 2\ 4), (1\ 4\ 2)\}$



- $\{\mathrm{id}, (1\ 3\ 4), (1\ 4\ 3)\}$



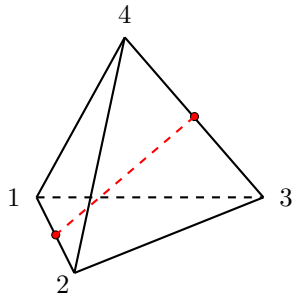
- $\{\mathrm{id}, (2\ 3\ 4), (2\ 4\ 3)\}$



- wobei - - - - - - - - Drehachse ist

Diese werden jeweils von einer Drehung um 120° um eine Ecke erzeugt.

Für die Kantendiagonalen: z.B. 12 nach 34:



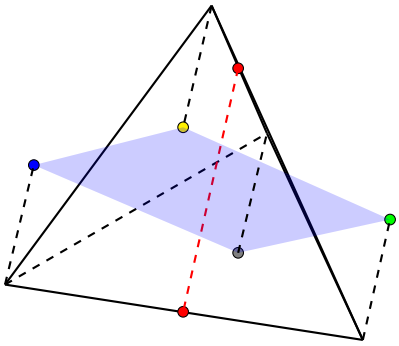
Dazu betrachtet man den Stabilisator der Kantenmittendiagonalen.

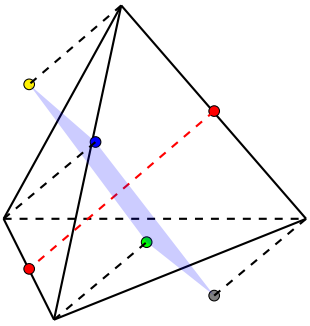
Die Kante 12 muss festgehalten werden ($1, 2$ fest) oder ($1, 2$ vertauscht). Analog für die Kante 34.

Oder die Kante 12 geht auf die Kante 34:

$$\{\mathrm{id}, (1\ 2), (3\ 4), (1\ 2)(3\ 4), (1\ 3\ 2\ 4), (1\ 4\ 2\ 3), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\} = \text{Symmetriegruppe des Quadrats}$$

Geometrisch sieht man das, indem man den Tetraeder auf die Ebene senkrecht zur Kantenmittendiagonalen durch den Mittelpunkt der Kantenmittendiagonalen projeziert: Der gesuchte Stabilisator hält die Kantenmittendiagonale fest und wirkt nur auf der Projektion des Tetraeders auf die senkrechte Ebene, dies ist ein Quadrat:





Es gibt 3 Kantenmittendiagonalen und 3 zugehörige Stabilisatoren, damit also 3 Untergruppen der Ordnung 8:

- $\{\mathrm{id}, (1\ 2), (3\ 4), (1\ 2)(3\ 4), (1\ 3\ 2\ 4), (1\ 4\ 2\ 3), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$
- $\{\mathrm{id}, (1\ 3), (2\ 4), (1\ 3)(2\ 4), (1\ 2\ 3\ 4), (1\ 4\ 2\ 3), (1\ 2)(3\ 4), (1\ 4)(2\ 3)\}$
- $\{\mathrm{id}, (1\ 4), (2\ 3), (1\ 4)(2\ 3), (1\ 3\ 2\ 4), (1\ 2\ 4\ 3), (1\ 3)(2\ 4), (1\ 2)(3\ 4)\}$

Die Untergruppen der Ordnung 4 werden alle drei von Drehspiegelungen erzeugt:

- $\{\mathrm{id}, (1\ 2\ 3\ 4), (1\ 3)(2\ 4), (1\ 4\ 3\ 2)\}$
- $\{\mathrm{id}, (1\ 2\ 4\ 3), (1\ 4)(2\ 3), (1\ 3\ 2\ 4)\}$
- $\{\mathrm{id}, (1\ 3\ 2\ 4), (1\ 2)(3\ 4), (1\ 4\ 2\ 3)\}$

Es gibt auch Vier Klein'sche Vierergruppen:

- $\{\mathrm{id}, (1\ 2), (3\ 4), (1\ 2)(3\ 4)\}$
- $\{\mathrm{id}, (1\ 3), (2\ 4), (1\ 3)(2\ 4)\}$
- $\{\mathrm{id}, (1\ 4), (2\ 3), (1\ 4)(2\ 3)\}$
- $\{\mathrm{id}, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$

Von den Spiegelungen werden 6 Untergruppen der Ordnung 2 erzeugt:

$$\langle(1\ 2)\rangle, \langle(1\ 3)\rangle, \langle(1\ 4)\rangle, \langle(2\ 3)\rangle, \langle(2\ 4)\rangle, \langle(3\ 4)\rangle$$

Die 4 Untergruppen der Ordnung 6 gleich der Stabilisatoren von den Ecken und isomorph zur $\mathbb{S}_3$:

$$\mathbb{S}(1,2,3), \mathbb{S}(1,3,4), \mathbb{S}(1,2,4), \mathbb{S}(2,3,4)$$

Die einzige Untergruppe der Ordnung 12 ist die $\mathbb{A}_4$.

24 hat die Teiler :

$$24,\ 12,\ 8,\ 6,\ 4,\ 3,\ 2,\ 1$$

und zu jedem dieser Teiler haben wir Untergruppen gefunden.

1.5.2 Beispiel:

Wir nehmen die Gruppe $\mathbb{A}_4$.

Es gilt $|\mathbb{A}_4| = 12$ und $6 \mid 12$ aber die $\mathbb{A}_4$ hat keine Untergruppe der Ordnung 6.

Angenommen, sie hätte, N (Normalteiler), denn $\left|{}^{\mathbb{A}_4}\!/_{N}\right| = 2$. Sei H eine Untergruppe der Ordnung 3, die von einer Drehung erzeugt wird. z.B.:

$$\langle(1\ 2\ 3)\rangle = H$$

Mit dem 1. Isomorphiesatz 1.3.3 folgt:

$$\begin{aligned}
{}^{HN}\!/_{N} \cong {}^{H}\!/_{H \cap N} &\Rightarrow \left|{}^{HN}\!/_{N}\right| = \left|{}^{H}\!/_{H \cap N}\right| \\
&\Rightarrow \frac{|HN|}{|N|} = \frac{|H|}{|H \cap N|} \\
&\Rightarrow 12 = |\mathbb{A}_4| \geqslant |HN| = \frac{|H| \cdot |N|}{|H \cap N|} = \frac{3 \cdot 6}{|H \cap N|} = \frac{18}{|H \cap N|} \\
&\Rightarrow |H \cap N| \supsetneq \{\mathrm{id}\}
\end{aligned}$$

Damit existiert dann ein $3-$Zykel in $H \cap N$. Da $H \cap N$ eine Untergruppe ist, liegt auch sein Inverses in $H \cap N$.

$$\begin{aligned}
&\Rightarrow |H \cap N| = 3 \\
&\Rightarrow H \subset H \cap N \\
&\Rightarrow H \subset N
\end{aligned}$$

Da dieses Argument für jede Wahl von H greift, folgt:

$$\{3 - \text{Zykel}\} \subset N$$

Es gibt 8 3-Zykel $\lightning$

1.5.3 Definition

Sei G eine endliche Gruppe, p eine Primzahl.

1. G heißt $p-$Gruppe, falls $|G| = p^r$ für ein $r \in \mathbb{N}$.
2. Ist $|G| = p^k \cdot m$ mit $p \nmid m$ so heißt eine Untergruppe $H \subset G$ mit $|H| = p^k$ eine $p-$Sylow(-Unter-)Gruppe von G.

Beispiel

Es gilt (siehe 1.5.1)

$$\text{Stab(Kantenmittendiagonalen)} = \text{Sym(Quadrat)}$$

sind $2-$Sylowgruppen, der $\mathbb{S}_4$. Denn $|\mathbb{S}_4| = 24 = 2^3 \cdot 3$ und $2 \nmid 3$ und die Mächtigkeit ist $8 = 2^3$.

Die Erzeugnisse von Drehungen (z.B.: $\langle(1\ 2\ 3)\rangle$) sind $3-$Sylowgruppen der $\mathbb{S}_4$.

1.5.4 Satz

Sei G endlich, p eine Primzahl, mit $p \mid |G|$, $|G| = p^k \cdot m$ und $p \nmid m$.

Dann gibt es zu jedem r mit $1 \leqslant r \leqslant k$ eine Untergruppe H von G mit $|H| = p^r$.

Insbesondere hat G für jedes p eine p-Sylowuntergruppe.

1.5.5 Definition: Exponent

Sei G eine Gruppe, der Exponent von G ist:

$$Exp(G) := \min\left\{k \in \mathbb{N}_{>0} \mid g^k = e \ \forall\ g \in G\right\}$$

Beispiel

- $Exp(\mathbb{Z}_2 \times \mathbb{Z}_2) = 2$ da jedes Element zu sich selbst invers ist.
- $Exp(\mathbb{Z}_4) = 4$
- $Exp(\mathbb{S}_3) = 6$ da $\text{kgV}(2,3) = 6$
- $Exp(\text{Sym}(\square)) = 4$

1.5.6 Lemma

Sei $|G| = n$

1. Der Exponent m von G ist das kleinste gemeinsame Vielfache der Ordnung der Elemente von G.
2. Falls $g^k = e \ \forall\ g \in G \Rightarrow m \mid k$
3. $m \mid n$

Beweis:

1. Es gilt:

   $g^k = e \Leftrightarrow \text{ord}(g) \mid k$

   m wird also von allen $\text{ord}(g)$ geteilt und das es nach Definition das Kleinste ist, folgt :

   $m =$ kleinste gemeinsame Vielfache $(\text{ord}(g) \mid g \in G)$

2. folgt aus 1)
3. folgt, da n ein Vielfaches von $\text{ord}(g)$ ist und es für alle $g \in G$ gilt. $\square$

1.5.7 Lemma

Sei G endlich und abelsch, $m := Exp(G)$. Dann gilt:

$$\exists\ k \in \mathbb{N} > 0 :\ |G| \mid m^k$$

Beweis: Per Induktion nach $|G|$.

Induktionsanfang: $|G| = 1$ ist klar.

Induktionsvorraussetzung: Die Behauptung gelte für alle abelschen G' mit $|G'| < |G|$

Induktionsschluss: Sei $e \neq g \in G,\ H = \langle g \rangle,\ |H| = \text{ord}(g) \mid m$.

Da G abelsch, ist H Normalteiler und G/H eine Gruppe.

Sei $g'H \in G/H$, dann ist

$$(g'H)^m = g'^m H = eH = H$$

Also teilt der Exponent von G/H m nach Lemma 1.5.6 2).

Da $|G/H| < |G|$ greift die Induktionsvorraussetzung und wir erhalten k' mit

$$\left|G/H\right| \mid Exp\left(G/H\right)^{k'} \Rightarrow \left|G/H\right| \mid m^{k'}$$

Setze $k = k' + 1$, dann gilt:

$$|G| = |H| \cdot \left|G/H\right| = \text{ord}(g) \cdot \left|G/H\right| \mid m \cdot m^{k'} = m^{k'+1} = m^k$$

1.5.8 Lemma

Sei G endlich und abelsch, p Primzahl, $p \mid |G|$, dann hat G eine Untergruppe der Ordnung p.

Beweis:

Es gilt: $p \mid |G|$ und $|G| \mid m^k$, wobei $m = Exp(G)$

$\Rightarrow p \mid m^k$
$\Rightarrow p \mid m$ da p prim

Da $m = \text{kgV}(\text{ord}(g) \mid g \in G)$

$\Rightarrow \exists\ g :\ p \mid \text{ord}(g)$.

Sei $\text{ord}(g) = r \cdot p$.

Dann hat g^r Ordnung p und $\langle g^r \rangle$ ist eine (notwendigerweise zyklische) Untergruppe der Ordnung p. □

Beweis von Satz 1.5.4 Induktion nach $n = |G|$.

Induktionsanfang: $n = 1, n = 2$ klar

Induktionsvoraussetzung: Die Behauptung gelte für alle G' mit $|G'| < n$.

Induktionsschluss:

Hat G eine echte Untergruppe $U \leq G$ mit $p^k \mid |G|$, so wenden wir die Induktionsvoraussetzung auf U an und die Behauptung folgt, da Untergruppen von U auch Untergruppen von G sind.

Hat G keine solche Untergruppe, so folgt aus

$$|G| = |U| \cdot \left|{}^{G}\!/_{U}\right| \;\Rightarrow\; p \mid \left|{}^{G}\!/_{U}\right|$$

$\forall$ echten Untergruppen U.

Betrachte die Konjugation von G

Sei $R \subset G$ eine Teilmenge, die aus jeder Konjugationsklasse genau ein Element enthält.

Nach der Klassengleichung 1.2.12 gilt:

$$|G| = |Z(G)| + \sum_{r \in R \setminus Z(G)} \left|{}^{G}\!/_{Z_G(r)}\right|$$

wobei für $r \in R \setminus Z(G)$ der Zentralisator $Z_G(r)$ eine echte Untergruppe ist, daher gilt:

$$p \mid \left|{}^{G}\!/_{Z_G(r)}\right| \;\Rightarrow\; p \mid |Z(G)|\,.$$

Da $Z(G)$ abelsch ist, folgt mit Lemma 1.5.8, dass $Z(G)$ eine Untergruppe N der Ordnung p hat.

Als Untergruppe des Zentrums, das Normalteiler in G und abelsch ist, ist N Normalteiler in G und wir können ${}^{G}\!/_{N}$ betrachten.

Es gilt:

$$\left|{}^{G}\!/_{N}\right| = \frac{|G|}{|N|} = \frac{p^k m}{p} = p^{k-1} \cdot m$$

Nach Induktionsvoraussetzung hat ${}^{G}\!/_{N}$ für jedes r' mit $1 \leq r' \leq k-1$ eine Untergruppe H' der Ordnung $p^{r'}$.

${}^{G}\!/_{N}$ hat auch die Untergruppe $\{e\}$ der Ordnung $1 = p^0$. Sei

$$\pi : G \to {}^{G}\!/_{N}$$

Setze:

$$H = \pi^{-1}(H')$$

Dann ist H eine Untergruppe von G der Ordnung $p^{r'+1}$, und mit $r = r' + 1$ haben wir solche $\forall\ 1 \leq r' \leq k$. □

1.5.9 Korollar

Für jede Primzahl $p \mid |G|$ existiert ein Element der Ordnung p

Beweis:

Aus Satz 1.5.4 folgt, dass es für jedes $p \mid |G|$ eine Untergruppe der Ordnung p gibt, diese ist notwendigerweise zyklisch und daher erzeugt von einem Element der Ordnung p.

□

1.5.10 Satz (Sylowsche Sätze)

Sei G endlich, $p \mid |G|$, p prim.

1) Jede p-Untergruppe H ist in einer p-Sylowgruppe enthalten.

2) Alle p-Sylowgruppen sind zueinander konjugiert.

3) Die Anzahl n_p der p-Sylowgruppen von G ist ein Teiler von $|G|$ mit $n_p \equiv 1 \mod p$.

Beispiel:

Sei $G = \mathbb{S}_4$ mit $|G| = 24 = 2^3 \cdot 3$. Die 2-Sylowgruppen haben Ordnung 8.

$$n_2 \mid 24 \text{ und } n_2 \equiv 1 \mod 2 \Rightarrow n_2 \mid 3$$

Wir kennen 3 2−Sylowgruppen (Beispiel: 1.5.1), die drei Sym(□), also $n_2 = 3$.

Die 3-Sylowgruppen haben Ordnung 3.

$$n_3 \mid 24 \text{ und } n_3 \equiv 1 \mod 3 \Rightarrow n_3 \in \{1, 4\}$$

Wir kennen schon 4 Untergruppen der Ordnung 3 – die 4 Sym(△) der Seiten, erzeugt von einer Drehung:

$$\langle(1\ 2\ 3)\rangle, \langle(1\ 2\ 4)\rangle, \langle(1\ 3\ 4)\rangle, \langle(2\ 3\ 4)\rangle \Rightarrow n_3 = 4$$

1.5.11 Korollar:

Sei $|G| = p^k \cdot m$, $p \nmid m$, so gilt:

$$n_p \mid m$$

Beweis:

$n_p \equiv 1 \mod p$

$\Rightarrow p \nmid n_p$, aber $n_p \mid |G| = p^k \cdot m$ □

Satz:

$$p-\text{Sylowgruppe ist Normalteiler} \Leftrightarrow n_p = 1$$

Beweis:

„⇒ “ Sei $p-$Sylowgruppe Normalteiler

$\Rightarrow gSg^{-1} = S$

$\Rightarrow \{\text{Konjugationen von } S\} = S$

$\overset{1.5.10\ 2)}{\Rightarrow} n_p = 1$

„⇐ “ Sei n_p=1

$\Rightarrow$ Es gibt nur eine $p-$Sylowgruppe S

$\overset{1.5.10\ 2)}{\Rightarrow}$ Es ist gSg^{-1} eine p-Sylowgruppe

$\Rightarrow gSg^{-1} = S$

$\Rightarrow S$ ist Normalteiler.

1.5.12 Definition Normalisator

Sei G eine Gruppe, S eine Untergruppe.

Der Normalisator von S ist

$$N_G(S) = \{g \in G \mid gSg^{-1} = S\}$$

1.5.13 Lemma

Sei $H \subset G$ eine p-Gruppe, S eine p-Sylowgruppe von G.

Ist H im Normalisator $N_G(S)$ enthalten, so gilt schon $H \subset S$.

Beweis:

Sei $|G| = p^k \cdot m$, $p \nmid m$.

Da $H \subset N_G(S)$ wird S schon von H normalisiert.

Mit dem 1. Isomorphiesatz 1.3.3 erhalten wir

$$HS/S \cong H/H \cap S$$

Damit ist $\left|HS/S\right|$ ein Teiler von $|H|$ und daher eine p-Potenz.
Also ist auch

$$|HS| = \left|HS/S\right| \cdot |S|$$

eine p-Potenz, größer gleich $|S| = p^k$.

Wegen 1.3.2 2) (Vorbereitung zum 1. Isomorphiesatz) ist HS eine Untergruppe von G

$\Rightarrow |HS| \mid |G|$
$\Rightarrow |HS| \mid p^k \cdot m$
$\Rightarrow |HS| = p^k$
$\Rightarrow \left|HS/S\right| = 1$
$\Rightarrow HS = S$
$\Rightarrow h_s \in S \ \forall \ h \in H, s \in S$
$\Rightarrow h = (hs)s^{-1} \in S \ \forall \ h \in H$ mit $hs \in S$ und $s^{-1} \in S$
$\Rightarrow H \subset S$ $\square$

1.5.14 Definition: transitiv

Eine Gruppenoperation mit nur einer Bahn heißt transitiv.

1.5.15 Proposition

Sei $U \subset G$ eine p-Sylowgruppe, $H \subset G$ eine p-Gruppe,
dann

$$\exists\ g \in G : H \subset gUg^{-1}$$

und gUg^{-1} ist auch p-Sylowgruppe.

Beweis:

Sei

$$\begin{aligned} U^G &= \{\text{Menge der Konjugationsklassen von } U\} \\ &= \{gUg^{-1} \mid g \in G\} \end{aligned}$$

Betrachte die Konjugationsoperation von G auf U^G:

$$\begin{aligned} G \times U^G &\to U^G \\ (g, S) &\mapsto gSg^{-1} \end{aligned}$$

Sie ist per Definition transitiv.

Aus Korollar 1.1.21 folgt

$$\begin{aligned} |G| &= \text{ Bahnlänge } \cdot |\text{Stab}| \\ &= |U^G| \cdot |\text{Stab}(U)| \\ &= |U^G| \cdot |N_G(U)|, \end{aligned}$$

da der Normalisator $N_G(U)$ per Definition der Stabilisator dieser Operation ist.

Sei $|G| = p^k \cdot m, p \nmid m$, dann ist

$$|U| = p^k$$

Da $U \subset N_G(U)$ Untergruppe gilt

$$p^k \mid |N_G(U)| \Rightarrow p \nmid |U^G|$$

Wir schränken die Operation jetzt auf H ein:

$$\begin{aligned} H \times U^G &\to U^G \\ (h, S) &\mapsto hSh^{-1} \end{aligned}$$

Dann zerfällt U^G in eine disjunkte Vereinigung von Bahnen.

Sei $R \subset U^G$ eine Menge, die aus jeder Bahn genau ein Element enthält.
Dann gilt mit der Bahnengleichung 1.1.23

$$|U^G| = \sum_{S \in R} \frac{|H|}{|\text{Stab}_H(S)|} = \sum_{S \in R} p^{j_s}$$

für geeignete $js \geq 0$, da H eine p-Gruppe ist und daher die Ordnungen von Untergruppen und Faktorgruppen auch p-Potenzen sind.

Da $p \nmid |U^G| \ \exists\ s : j_s = 0$
Wir schreiben dieses $s \in R \subset U^G$ als gUg^{-1} für ein $g \in U$.
Für dieses s gilt:

$$\Rightarrow \frac{|H|}{|\text{Stab}_H(s)|} = 1$$
$$\Rightarrow H = \text{Stab}_H(s) = \{h \in H \mid hSh^{-1} = S\} \subset \text{Stab}_G(s) = N_G(s)$$
$$\overset{1.5.13}{\Rightarrow} H \subset S = gUg^{-1}$$

S ist das Bild von U unter eine Konjugation und damit isomorph zu U, insbesondere ist S eine $p-$Sylowgruppe.

□

Beweis der Sylowschen Sätze 1.5.10:

1) Wegen Satz 1.5.4 existiert eine p-Sylowgruppe $U \subset G$.

   Wegen Prop. 1.5.15 existiert g mit $H \subset gUg^{-1}$ und dies ist eine p-Sylowgruppe.

2) Sei H eine (weitere) p-Sylowgruppe, dann ist H eine p-Gruppe und wir können Prop. 1.5.15 auf H anwenden.

   Wir erhalten g mit $H \subset gUg^{-1}$, und

$$\begin{aligned} p^k = |H| &= |gUg^{-1}| \\ \Rightarrow H &= gUg^{-1} \end{aligned}$$

   Damit ist H zu U konjugiert.

3) Sei U p-Sylowgruppe, jede zu U konjugierte Untergruppe ist auch p-Sylowgruppe, aus 2) folgt

$$\begin{aligned} U^G &= \{p - \text{Sylowgruppe von } G\} \\ \Rightarrow n_p &= |\,U^G|. \end{aligned}$$

   Wie in 1.5.15 sehen wir

$$\begin{aligned} |G| &= |\,U^G| \cdot |\mathrm{Stab}(u)| = n_p \cdot |\mathrm{Stab}(u)| \\ \Rightarrow n_p &\mid G \end{aligned}$$

   Wir schränken die Konjugation auf U ein:

$$\begin{aligned} U \times U^G &\to U^G \\ (u, S) &\mapsto uSu^{-1} \end{aligned}$$

   Sei $R \subset U^G$ eine Teilmenge, die aus jeder Bahn genau ein Element enthält.

   Die Bahn von U ist

$$\{uUu^{-1} \mid u \in U\} = \{U\}.$$

   Angenommen, es gäbe eine weitere Bahn mit nur einem Element, also $S \in U^G$ mit $uSu^{-1} = S \;\forall\; u \in U$.

   Dann wäre $U \subset N_G(S)$ und mit 1.5.13 folgte $U \subset S$.

   $\Rightarrow U = S$, da beides p-Sylowgruppen sind.

   Mit der Bahngleichung 1.1.23 gilt also

$$n_p = |\,U^G| = \sum_{s \in R} \frac{|\,U|}{|\mathrm{Stab}_U(s)|} = \sum_{s \in R} p^{js}$$

   mit geeigneten $js \geq 0$, da $Up-$Gruppe.

   Weiter gilt $U \in R$ und $j_U = 0$ sowie $j_s > 0 \;\forall\; S \neq U$,
   denn

$$\frac{|\,U|}{|\mathrm{Stab}_U(s)|} = \text{ Bahnlänge(s)}$$

   nach 1.1.21 und damit

$$n_p = 1 + \sum_{s \in R \setminus \{U\}} p^{js} \equiv 1 \mod p.$$

□

Die Sylowsätze sind wichtig bei der Klassifikation der endlichen Gruppen.

Der folgende Satz liefert eine Anwendung:

1.5.16 Satz

Seien p, q prim, $p < q$, $p \nmid q - 1$.

Dann ist jede Gruppe G der Ordnung pq zyklisch, es gilt

$$G \cong \mathbb{Z}_{pq}$$

Beweis

$n_p = 1 + k \cdot p$ wegen der Sylowsätze 1.5.10 3) und $n_p \mid q$ wegen Korollar 1.5.11.

$\Rightarrow n_p \in \{1, q\}$

Wäre $n_p = q$

$\Rightarrow n_p = q$
$\Rightarrow q = 1 + kp$
$\Rightarrow q - 1 = kp$
$\Rightarrow p \mid q - 1$ $\lightning$
$\Rightarrow n_p = 1$

Sei P die einzige p-Sylowgruppe.

Mit $n_q = 1 + lq, n_q \mid p$ folgt $n_q \in \{1, p\}$.

Wäre $n_q = p$, dann würde folgen $p = 1 + lq$. Dies steht aber im Widerspruch zu $p < q$.
$\Rightarrow n_q = 1$

Sei Q die einzige $q-$Sylowgruppe.

P und Q haben Primzahlordnung p bzw. q, sind also zyklisch:

$$P \cong \mathbb{Z}_p, \quad Q \cong \mathbb{Z}_q$$

Betrachte die Bahnen von P und Q unter Konjugation.

Nach 1.5.10 2) sind es jeweils alle p- bzw. $q-$ Sylowgruppen, also einelementig.

$$\Rightarrow gPg^{-1} = P, \ gQg^{-1} = Q \ \forall \ g \in G$$
$$\Rightarrow P, Q \text{ Normalteiler}$$

Da P und Q teilerfremde Ordnungen haben gilt $P \cap Q = \{e\}$. (Erinnerung: Der Schnitt von zwei Untergruppen ist wieder eine Untergruppe)

Mit 1.3.2 2) und dem 1. Isomorphiesatz folgt:

PQ ist Untergruppe von G und

$$PQ/P \cong Q/(P \cap Q) \cong Q$$

$\Rightarrow |PQ|/|P| = |Q|$
$\Rightarrow |PQ| = p \cdot q$
$\Rightarrow PQ = G$

Sei $g \in P, h \in Q$.

$\Rightarrow ghg^{-1} \in Q$ da Q Normalteiler.
$\Rightarrow ghg^{-1}h^{-1} \in Q$

Andererseits ist $hg^{-1}h^{-1} \in P$ da P Normalteiler.

$\Rightarrow ghg^{-1}h^{-1} \in P$
$\Rightarrow ghg^{-1}h^{-1} \in P \cap Q = \{e\}$
$\Rightarrow gh = hg$
$\Rightarrow g$ und h vertauschen.
$\overset{1.4.3}{\Rightarrow} G = P \times Q = \mathbb{Z}_p \times \mathbb{Z}_q$

aufgrund der Charakterisierung des direkten Produkts. $\square$

Behauptung: $\mathbb{Z}_{pq} = \mathbb{Z}_p \times \mathbb{Z}_q$

Dies folgt direkt aus dem chinesischen Restsatz.

Betrachte:

$$\begin{aligned} \varphi : \mathbb{Z} &\to \mathbb{Z}_p \times \mathbb{Z}_q \\ a &\mapsto (a + p\mathbb{Z}, a + q\mathbb{Z}) \end{aligned}$$

φ ist Homomorphismus.

φ ist surjektiv wegen des chinesischen Restsatzes:

Für $(a_1, a_2) \in \mathbb{Z}_p \times \mathbb{Z}_q$ suchen wir a mit

$$a \equiv a_1 \mod p \text{ und } a \equiv a_2 \mod q$$

dies existiert nach dem chinesischen Restsatz und ist eindeutig $\mod pq$.

$\mathrm{Ker}(\varphi) = pq\mathbb{Z}$

$\overset{*}{\Rightarrow} \mathbb{Z}_{pq} = {}^{\mathbb{Z}}\!/_{pq\mathbb{Z}} = {}^{\mathbb{Z}}\!/_{\mathrm{Ker}(\varphi)} \cong \mathrm{Im}(\varphi) = \mathbb{Z}_p \times \mathbb{Z}_q$

$\Rightarrow G \cong \mathbb{Z}_{pq}$ ist zyklisch. □

$*$ = Homomorphiesatz

1.5.17 Korollar

Jede Gruppe der Ordnung 15 ist zyklisch.

Anders gesagt: Bis auf Isomorphie existiert genau eine Gruppe der Ordnung 15, $\mathbb{Z}_{15}$.

1.6 Auflösbare Gruppen

1.6.1 Definition: Einfache Gruppe

Eine Gruppe G heißt einfach, wenn sie nur die Normalteiler $\{e\}$ und G besitzt.

1.6.2 Lemma:

Sei $G \supsetneq \{e\}$ eine abelsche Gruppe. Dann gilt:

$$G \text{ ist einfach} \quad \Leftrightarrow \quad G \text{ zyklisch von Primzahlordnung}$$

Beweis:

„$\Leftarrow$“ Eine zyklische Gruppe von Primzahlordnung hat nur $\{e\}$ und G als Untergruppen.

„$\Rightarrow$“ Ist $|G|$ keine Primzahl, so existiert eine primzahl p mit $p \mid |G|$.

Nach Satz 1.5.4 $\exists$ Untergruppe U mit $|U| = p$, da G abelsch, ist U Normalteiler. $\square$

1.6.3 Proposition:

Die alternierende Gruppe $\mathbb{A}_5$ ist einfach.

Beweis:

$\mathbb{A}_5$ hat $\frac{5!}{5} = 24$ 5-Zykel und $\frac{5 \cdot 4 \cdot 3}{3} = 20$ 3-Zykel.

$$|\mathbb{A}_5| = 60 = 2^2 \cdot 3 \cdot 5$$

$\Rightarrow$ Die 5-Sylowgruppen haben Ordnung 5, sind zyklisch von einem 5-Zykel erzeugt und enthalten je 4 5-Zykel.

$\Rightarrow$ $\exists$ 6 5-Sylowgruppen.

Genauso die 3-Sylowgruppen haben Ordnung 3, sind zyklisch und enthalten je 2 3-Zykel

$\Rightarrow$ $\exists$ 10 3-Sylowgruppen

Sei $\{e\} \subsetneq N \subsetneq \mathbb{A}_5$ ein Normalteiler.

- Angenommen $5 \mid |N|$.

  Dann enthält N eine 5-Sylowuntergruppe, die auch 5-Sylowgruppe von $\mathbb{A}_5$ ist.

  Da alle 5-Sylowgruppen konjugiert sind, und $gNg^{-1} \subset N$, da N Normalteiler folgt, alle 5-Sylowgruppen der $\mathbb{A}_5$ sind in N

  $\Rightarrow$ $|N| \geq 1 + 24 = 25$
  $\Rightarrow$ $|N| \in \{30, 60\}$
  $\Rightarrow$ $3 \mid |N|$

  Damit enthält N auch eine (und damit alle) 3-Sylowgruppen, also folgt

  $\Rightarrow$ $|N| \geq 1 + 24 + 20 = 45$
  $\Rightarrow$ $|N| = 60$
  $\Rightarrow$ $N = \mathbb{A}_5$ $\lightning$

- Angenommen $3 \mid |N|$.

  $\Rightarrow$ N enthält eine (und damit alle) 3-Sylowgruppen
  $\Rightarrow$ $|N| \geq 1 + 20 = 21$
  $\Rightarrow$ $|N| \in \{30, 60\}$
  $\Rightarrow$ $5 \mid |N|$
  $\Rightarrow$ $N = \mathbb{A}_5$ $\lightning$

- Angenommen $|N| = 4$.

  Dann ist N 2-Sylowgruppe.

  Da die 2-Sylowgruppen konjugiert sind, und N Normalteiler ist, ist N die einzige 2-Sylowgruppe.

  Aber alle $(2,2)$-Zykel haben Ordnung 2, also

$$\frac{5 \cdot 4}{2} \cdot \frac{3 \cdot 2}{2} \cdot \frac{1}{2} = 15$$

  Elemente, und jeweils 3 davon liegen in einer kleinschen Vierergruppe

  $\Rightarrow \exists$ 5 4-Sylowgruppen $\lightning$

- Angenommen $|N| = 2$.

  Dann ist $N = \langle n \rangle$ für ein Element n der Ordnung 2, also einen $(2,2)$-Zykel.

  Da N Normalteiler gilt

$$gng^{-1} = n \ \forall g \in \mathbb{A}_5$$

  aber für $n = (a\ b)(c\ d)$ und $g = (a\ b\ e)$ gilt

$$gng^{-1} = (a\ b\ e)(a\ b)(c\ d)(a\ e\ b) = (b\ e)(c\ d) \neq n \quad \lightning$$

Also gibt es keinen solchen Normalteiler N und $\mathbb{A}_5$ ist einfach. □

1.6.4 Definition: Auflösbar

Eine Gruppe G heißt auflösbar, wenn es eine Kette

$$\{e\} = G_k \subset G_{k-1} \subset \cdots \subset G_0 = G$$

gibt, so dass $G_i \subset G_{i-1}$ Normalteiler und G_{i-1}/G_i abelsch $\forall i = 1, ..., k$.

Eine solche Kette heißt Subnormalteilerkette mit abelschen Faktoren.

Beispiel:

1) Abelsche Gruppen G sind auflösbar mit $\{e\} \subset G$.

2) $\mathbb{S}_4$ ist auflösbar mit Subnormalteilerkette:

$$\{\mathrm{id}\} \subset K_4 \subset \mathbb{A}_4 \subset \mathbb{S}_4$$

   wobei K_4 die kleinsche Vierergruppe

$$K_4 = \{\mathrm{id}, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$$

   ist. Da $\left|\mathbb{S}_4/\mathbb{A}_4\right| = 2$, ist $\mathbb{A}_4$ in $\mathbb{S}_4$ Normalteiler. Dass K_4 in $\mathbb{A}_4$ Normalteiler ist lässt sich nachrechnen. (Es gilt sogar $K_4 \subset \mathbb{S}_4$ ist Normalteiler, man kann dies geometrisch begründen da $\mathbb{S}_4 = \mathrm{Sym}(\text{Tetraeder})$, und $K_4 = \mathrm{Ker}(\varphi)$ für

$$\varphi : \ \mathbb{S}_4 \to \mathbb{S}_3 = \mathbb{S}(\text{Kantenmittendiagonalen})$$

   Es gilt:

$$\mathbb{S}_4/\mathbb{A}_4 \cong \mathbb{Z}_2 \ \text{ ist abelsch} \qquad \mathbb{A}_4/K_4 \cong \mathbb{Z}_3 \ \text{ ist abelsch}$$

   K_4 ist auch abelsch.

3) $\mathbb{A}_5$ ist einfach, nicht abelsch, also auch nicht auflösbar.

1.6.5 Proposition:

Sei G endlich, $U \subset G$ Untergruppe, N Normalteiler.

1) G auflösbar $\Rightarrow$ U auflösbar.

2) G auflösbar $\Leftrightarrow$ N, G/N auflösbar.

Beweis:

1) Sei G auflösbar mit Subnormalteilerkette

$$\{e\} = G_k \subset G_{k-1} \subset \cdots \subset G_0 = G$$

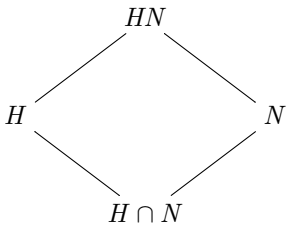
Setze $U_i := G_i \cap U$. Dann ist

$$\{e\} = U_k \subset U_{k-1} \subset \cdots \subset U_0 = U$$

eine Kette von Untergruppen in U. Dabei gilt:

$$U_i = G_i \cap U = G_i \cap G_{i-1} \cap U = G_i \cap U_{i-1}$$

Wegen 1.3.2 1) ($H \cap N$ Normalteiler in H) folgt $U_i = G_i \cap U_{i-1}$ ist Normalteiler in U_{i-1} (denn G_i ist Normalteiler in G_{i-1}).



Außerdem gilt:

$$U_{i-1}/U_i = U_{i-1}/G_i \cap U_{i-1} \cong G_i U_{i-1}/G_i \subset G_{i-1}/G_i$$

ist Untergruppe, denn $G_i U_{i-1} \subset G_{i-1}$ ist Untergruppe wegen 1.3.2.

Aber G_{i-1}/G_i ist abelsch, damit auch U_{i-1}/U_i.

2) " $\Rightarrow$ " N ist auflösbar wegen 1).
Sei

$$\{e\} = G_k \subset G_{k-1} \subset \cdots \subset G_0 = G$$

Subnormalteilerkette von G. Durch Multiplikation mit N erhalten wir wegen 1.3.2 eine Kette von Untergruppen

$$N = G_k N \subset G_{k-1} N \subset \cdots \subset G_0 N = G$$

Behauptung: $G_i N \subset G_{i-1} N$ ist Normalteiler.

Sei $g_1 n_1 \in G_i N$ und $g_2 n_2 \in G_{i-1} N$. Dann gilt

$$g_2 n_2 (g_1 n_1)(g_2 n_2)^{-1} = g_2 n_2 g_1 n_1 n_2^{-1} g_2^{-1}$$

Da N Normalteiler in G gilt

$$\begin{aligned} & g_1 n_1 g_1^{-1} \in N \\ \Rightarrow\ & \exists n_3 \in N : g_1 n_1 g_1^{-1} = n_3 \\ \Rightarrow\ & g_1 n_1 = n_3 g_1 \\ \Rightarrow\ & g_2 n_2 g_1 n_1 n_2^{-1} g_2^{-1} = g_2 n_2 n_3 g_1 n_2^{-1} g_2^{-1} \end{aligned}$$

Genauso $\exists n_3 \in N$:

$$\begin{aligned} & g_2 (n_2 n_3) g_2^{-1} = n_4 \\ \Rightarrow\ & g_2 n_2 n_3 = n_4 g_2 \\ \Rightarrow\ & g_2 n_2 n_3 g_1 n_2^{-1} g_2^{-1} = n_4 g_2 g_1 n_2^{-1} g_2^{-1} \end{aligned}$$

Da $G_i \subset G_{i-1}$ Normalteiler, $g_1 \in G_i$, $g_2 \in G_{i-1}$, $\exists g_3 \in G_i$:

$$
\begin{aligned}
& g_2 g_1 g_2^{-1} = g_3 \\
\Rightarrow\ & g_2 g_1 = g_3 g_2 \\
\Rightarrow\ & n_4 g_2 g_1 n_2^{-1} g_2^{-1} = n_4 g_3 g_2 n_2^{-1} g_2^{-1}
\end{aligned}
$$

Weiterhin $\exists\ n_5 \in N$:

$$
\begin{aligned}
& g_3^{-1} n_4 g_3 = n_5 \\
\Rightarrow\ & n_4 g_3 = g_3 n_5 \\
\Rightarrow\ & n_4 g_3 g_2 n_2^{-1} g_2^{-1} = g_3 n_5 \underbrace{g_2 n_2^{-1} g_2^{-1}}_{\in N} \in G_i N \quad \text{da } N \text{ Normalteiler ist}
\end{aligned}
$$

Mit dem 1. und 2. Isomorphiesatz (1.3.3,1.3.5) folgt:

$$
{G_{i-1}N}\big/{G_iN} = {G_{i-1}G_iN}\big/{G_iN} \overset{1.}{\cong} {G_i}\big/{G_{i-1} \cap G_iN} \overset{2.}{\cong} {G_{i-1}}\big/{G_i}\Big/{(G_{i-1} \cap G_iN)}\big/{G_i}
$$

$\Rightarrow {G_{i-1}N}\big/{G_iN}$ ist isomorph zu einer Faktorgruppe der abelschen Gruppe ${G_{i-1}}\big/{G_i}$ und damit selbst abelsch.

$\Rightarrow N = G_kN \subset G_{k-1}N \subset \cdots \subset G_0N = G$ ist Subnormalteilerreihe

$\Rightarrow \left\{e_{G/N}\right\} = {N}\big/{N} = {G_kN}\big/{N} \subset \cdots \subset {G_0N}\big/{N} \subset {G}\big/{N}$ ist Subnormalteilerkette mit abelschen Faktoren:

$$
{G_{i-1}N}\big/{N}\big/{G_iN}\big/{N} \overset{2.}{\cong} {G_{i-1}}\big/{G_iN}
$$

$\Rightarrow {G}\big/{N}$ ist auflösbar

" $\Leftarrow$ " Seien N und ${G}\big/{N}$ auflösbar mit

$$
\{e\} = N_k \subset N_{k-1} \subset \cdots \subset N_0 = N
$$

und

$$
\left\{e_{G/N}\right\} = {G_l}\big/{N} \subset {G_{l-1}}\big/{N} \subset \cdots \subset {G_0}\big/{N} = {G}\big/{N}
$$

Dann ist

$$
\{e\} = N_k \subset \cdots \subset N_0 = N = G_l \subset G_{l-1} \subset \cdots \subset G_0 = G
$$

eine Subnormalteilerkette mit abelschen Faktoren, denn

$$
{G_{i-1}}\big/{G_i} \overset{2.}{\cong} {G_{i-1}}\big/{N}\big/{G_i}\big/{N}
$$

□

1.6.6 Korollar:

Für $n \geq 5$ sind $\mathbb{S}_n, \mathbb{A}_n$ nicht auflösbar.

Beweis:

Da $\mathbb{A}_5 \subset \mathbb{A}_n \subset \mathbb{S}_n$ Untergruppe ist und $\mathbb{A}_5$ nicht auflösbar ist. □

1.6.7 Korollar:

Sei G eine p-Gruppe, dann ist G auflösbar.

Beweis:

Sei $|G| = p^n$, p Primzahl. Induktion nach n

$n = 0$ nichts zu zeigen

$n = 1$ G ist zyklisch und auflösbar

Sei $n > 0$. Nach 1.2.13 gilt $p \mid |Z(G)|$. $\Rightarrow \{e\} \subsetneq Z(G) \subset G$.

Falls $Z(G) = G \Rightarrow$ G ist abelsch $\Rightarrow$ G auflösbar.

Falls $Z(G) \subsetneq G$, so sind $Z(G)$ und $G/Z(G)$ selbst p-Gruppen, die nach Induktionsvorraussetzung auflösbar sind

$\Rightarrow$ G ist auflösbar. □

1.6.8 Definition: Kompositionsreihe

Sei G eine endliche Gruppe. Eine Kette

$$\{e\} \subset G_k \subset G_{k-1} \subset \cdots \subset G_0 = G$$

von Untergruppen, so dass $G_i \subset G_{i-1}$ Normalteiler ist und G_{i-1}/G_i zyklisch von Primzahlordnung, heißt Kompositionsreihe.

1.6.9 Satz:

Sei G endliche Gruppe.

$$G \text{ auflösbar} \quad \Leftrightarrow \quad G \text{ besitzt eine Kompositionsreihe}$$

Beweis:

„$\Leftarrow$“ klar.

„$\Rightarrow$ “ Wir müssen eine Subnormalteilerkette zu einer Kompositionsreihe verfeinern.

Falls G_{i-1}/G_i nicht Primzahlordnung hat, so ist G_{i-1}/G_i nach Lemma 1.6.2 nicht einfach, besitzt also einen echten Normalteiler, mit dem wir verfeinern können.

Die Ordnungen der Faktorgruppen werden dabei echt kleiner, nach endlich vielen Schritten erhalten wir also Faktorgruppen von Primzahlordnung.

□

Beispiel:

1) $\mathbb{S}_4$ hat die Kompositionsreihe

$$\{\mathrm{id}\} \subset \langle (1\ 2)(3\ 4) \rangle \subset K_4 \subset \mathbb{A}_4 \subset \mathbb{S}_4$$

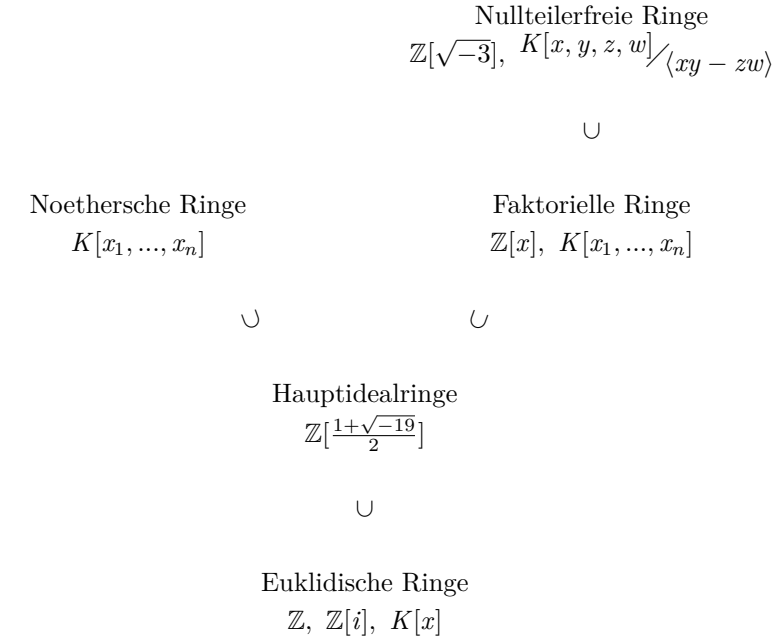
2) Gruppen der Ordnung pq mit p, q prim sind auflösbar:

Wie in Satz 1.5.16 folgt für $q < p$, dass es nur eine q-Sylowgruppe gibt, diese ist somit Normalteiler, und

$$\{e\} \subset Q \subset G$$

ist Kompositionsreihe, da $|Q| = q$ und $\left|G/Q\right| = \frac{pq}{q} = p$.

2 Ringe



Als bekannt vorausgesetzt werden:

- Polynomringe
- k-Algebra

Notation: R bezeichnet im Folgenden einen kommutativen Ring mit 1.

Euklidischer Ring:

Ein nullteilerfreier Ring heißt euklidisch wenn:

$$\exists\ \nu:\ R\backslash\{0\} \to \mathbb{N},\ \forall a, b \in R\backslash\{0\} \text{ mit } \nu(a) \geq \nu(b)\ \exists\ q, r \in R$$

mit

1) $a = qb + r$
2) $r = 0$ oder $\nu(r) < \nu(b)$

1) heißt dann Division mit Rest, ν heißt euklidische Norm.

Hauptideal Ring:

Ein nullteilerfreier Ring, in dem alle Ideale Hauptideale sind, heißt Hauptidealring.

Hauptideal:

Ein Ideal I das von einem Element erzeugt wird

$$\langle a \rangle = I$$

heißt Hauptideal.

Faktorieller Ring:

Ein nullteilerfreier Ring, in dem jedes $0 \neq a \in R\backslash R^*$ eine bis auf Vertauschung und Einheiten eindeutige Darstellung

$$a = p_1 \cdot \ \cdots\ \cdot p_r$$

mit p_i prim besitzt, heißt faktoriell.

Nullteilerfreier Ring:

Ein kommutativer Ring mit 1 ohne nicht-triviale Nullteiler heißt nullteilerfrei.

Nullteiler:

$a \in R$ heißt Nullteiler, falls

$$\exists\ b \neq 0,\ b \in R:\ ab = 0$$

Noetherscher Ring:

Ein kommutativer Ring mit 1, welcher eine der folgenden äquivalenten Eigenschaften erfüllt, heißt noethersch:

1) Jedes Ideal $I \subset R$ ist endlich erzeugt.
2) Jede aufsteigende Kette

$$I_1 \subset I_2 \subset I_3 \subset \cdots$$

von Idealen wird stationär, d.h. $\exists\ m$ mit

$$I_m = I_{m+1} = I_{m+2} = \cdots$$

3) Jede nicht-leere Menge von Idealen besitzt bezüglich der Inklusion ein maximales Element.

Einheit:

Sei R ein Ring. $a \in R$ heißt Einheit, falls $\exists b \in R: \ ab = 1$.

Einheitengruppe:

$(R^*, \cdot)$ ist die Einheitengruppe bestehend aus allen Einheiten in R.

Sei R nullteilerfrei. Sei $0 \neq a \in R\backslash\{0\}$

Irreduzibel:

a heißt irreduzibel falls $a = bc \ \Rightarrow \ b \in R^*$ oder $c \in R^*$

Prim:

a heißt prim falls $a \mid bc$ für $b, c \in R \ \Rightarrow \ a \mid b$ oder $a \mid c$

Satz:

$$a \in R \text{ ist prim } \Rightarrow \ a \text{ ist irreduzibel}$$

Quotientenkörper: $Quot(R)$

Sei R nullteilerfrei. Wir definieren auf $R \times R\backslash\{0\}$ eine Äquivalenzrelation:

$$(a, b) \sim (c, d) \ \Leftrightarrow \ ad = cb$$

Wir schreiben $\frac{a}{b}$ für die Äquivalenzklasse $[(a, b)]$und definieren auf der Menge der Äquivalenzklassen die Addition und Multiplikation

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$$
$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$$

Damit erhalten wir den Quotientenkörper $Quot(R)$. Es ist der kleinste Körper in den R eingebettet werden kann: (z.B. $\mathbb{Z} \subset \mathbb{Q}$.)

$$R \to Quot(R)$$
$$a \mapsto \frac{a}{1}$$

Ideal:

Sei R ein kommutativer Ring mit 1. Ein Ideal $I \subset R$ ist eine nicht leere Teilmenge wenn $\forall \ a, b \in I, \ r \in R$

1) $a + b \in I$
2) $r \cdot a \in I$

Erzeugnis:

Sei $A \subset R$ dann definiert man das Erzeugnis von A als:

$$\begin{aligned}\langle A \rangle &= \bigcap_{\substack{A \subset I \subset R \\ I \text{ Ideal}}} I \\ &= \left\{ \sum_{i=1}^{n} r_i a_i \ \middle| \ r_i \in R, \ a_i \in A, \ n \in \mathbb{N} \right\}\end{aligned}$$

Maximales Ideal:

Ein Ideal $m \subsetneq R$ heißt maximales Ideal, wenn für Ideale I mit $m \subsetneq I \subset R$ gilt $I = R$

Primideal:

Ein Ideal $P \subsetneq R$ heißt Primideal, wenn gilt: $\forall \ a, b \in R: \ a \cdot b \in P \ \Rightarrow \ a \in P$ oder $b \in P$

Summe von Idealen:

$$I_1 + I_2 = \{a + b \mid a \in I_1,\ b \in I_2\}$$

Produkt von Idealen:

$$I_1 \cdot I_2 = \langle a \cdot b \mid a \in I_1,\ b \in I_2 \rangle$$

Koprime Ideale:

Zwei Ideale I_1, I_2 heißen koprim genau dann wenn $I_1 + I_2 = \langle 1 \rangle$

Chinesischer Restsatz: Für Ringe

Sei R ein kommutativer Ring mit 1. Und seien $I_1, ..., I_r$ paarweise koprime Ideale. Dann ist

$$\begin{aligned} \varphi :\ R &\to {}^{R}\!/_{I_1} \times \cdots \times {}^{R}\!/_{I_r} \\ a &\mapsto ([a], ..., [a]) = (a + I_1, ..., a + I_r) \end{aligned}$$

surjektiv und mit

$$\mathrm{Ker}(\varphi) = I_1 \cap \cdots \cap I_r = I_1 \cdot \ \cdots \ \cdot I_r$$

Wenn man den Kern rausteilt wird die Abbildung also bijektiv das heißt

$${}^{R}\!/_{I_1 \cap \cdots \cap I_r} \cong {}^{R}\!/_{I_1} \times \cdots \times {}^{R}\!/_{I_r}$$

Satz: Quotientenring/Faktoring

Sei R ein Ring, I ein Ideal.
Dann ist ${}^{R}\!/_{I}$ mit den repräsentantenweise definierten Operationen ein Ring mit $[1] = 1 + I$ als Neutralem bzgl. $\cdot$, der Quotientenring/Faktorring

Primfaktorzerlegung bzw. Fundamentalsatz der Arithmetik:

Jede ganze Zahl $n \in \mathbb{Z} \setminus \{0, 1, -1\}$ hat eine eindeutige Darstellung

$$n = \pm 1 \cdot p_1^{r_1} \cdot \cdots \cdot p_s^{r_s}$$

mit Primzahlen $p_1 < \cdots < p_s$ und $r_i \in \mathbb{N}$. Die p_i heißen Primfaktoren von n und die Darstellung bezeichnen wir als die Primfaktorzerlegung von n.

ggT und kgV:

Sind $a_1, \ldots, a_t \in \mathbb{Z}$, dann heißt $d \in N$ größter gemeinsamer Teiler von $a_1, \ldots, a_t$

$$d = \mathrm{ggT}(a_1, \ldots, a_t),$$

wenn

(1) $d \mid a_j\ \forall\ j = 1, \ldots, t$, also d ist Teiler von allen a_j und

(2) ist $\tilde{d} \in \mathbb{Z}$ Teiler aller a_j, dann gilt $\tilde{d} \mid d$

Weiter heißt $m \in \mathbb{N}$ ein kleinstes gemeinsames Vielfaches von $a_1, \ldots, a_t$

$$m = \mathrm{kgV}(a_1, \ldots, a_t),$$

wenn

(1) $a_j \mid m\ \forall\ j = 1, \ldots, t$, also m ist Vielfaches aller a_j und

(2) ist $\tilde{m} \in \mathbb{Z}$ Vielfaches aller a_j, dann gilt $m \mid \tilde{m}$

Hier noch ein paar wichtige Sätze aus dem Algebraische Strukturen Skript

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

$$1)\ I \text{ Primideal } \Leftrightarrow {}^{R}\!/_{I} \text{ nullteilerfrei}$$
$$2)\ \ I \text{ maximal } \Leftrightarrow {}^{R}\!/_{I} \text{ Körper}$$

Korollar:

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

Korollar:

$$\langle 0 \rangle \subset R \text{ ist Primideal } \Leftrightarrow R \text{ nullteilerfrei}$$

Lemma:
Sei R nullteilerfrei, $0 \neq a \in R \setminus R^*$. Dann gilt:

$$\langle a \rangle \text{ ist Primideal} \Leftrightarrow a \text{ prim}$$

Lemma: Sei R nullteilerfrei, $0 \neq a \in R \setminus R^*$. Dann gilt:

$$\langle a \rangle \text{ maximal} \Rightarrow a \text{ irreduzibel}$$

Lemma: Sei R Hauptidealring, $a \in R \setminus (R^* \cup \{0\})$. Dann ist

$$\langle a \rangle \text{ maximal} \Leftrightarrow a \text{ irreduzibel}$$

Der Satz von Gauß und allgemeine Polynomringe

2.1 Satz von Gauß

2.1.1 Satz von Gauß

$$R \text{ faktoriell} \quad \Rightarrow \quad R[x] \text{ faktoriell}$$

2.1.2 Definition: Primitiv

Sei R nullteilerfrei

$$0 \neq f = \sum_{i=0}^{n} a_i x^i \in R[x]$$

ein Polynom. f heißt primitiv, falls $1 = \text{ggT}(a_0, ..., a_n)$.

2.1.3 Lemma:

Sei R faktoriell.

1) Ist $f \in R[x]$ primitiv und $c \in Quot(R)$ mit $c \cdot f \in R[x]$, so ist $c \in R$.
2) Für $f \in Quot(R)[x]$ $\exists\ 0 \neq c \in Quot(R)$ und $g \in R[x]$ primitiv mit $f = c \cdot g$

Beweis:

1) Sei $f = \sum_{i=0}^{n} a_i x^i$, $c = \frac{a}{b}$ mit $a, b \in R$ teilerfremd. Da $cf \in R[x] \ \Rightarrow\ \frac{aa_i}{b} \in R\ \forall i = 0, .., n$.
   Sei $p \in R$ prim mit $p|b$. Da $p \nmid a$ folgt aus $\frac{aa_i}{b} \in R$ $p|a_i\ \forall i = 0, ..., n$.
   $\Rightarrow\ p \mid \text{ggT}(a_0, ..., a_n)$
   $\Rightarrow\ \text{ggT}(a_0, ..., a_n) \neq 1$
   $\Rightarrow\ f$ nicht primitiv
   $\Rightarrow\ \nexists$ solches p
   $\Rightarrow\ b \in R^*$
   $\Rightarrow\ c = \frac{a}{b} \in R$

2) Sei $f = \sum_{i=0}^{n} \frac{a_i}{b_i} \cdot x_i$ mit $a_i \in R$, $b_i \in R \backslash \{0\}$
   $\Rightarrow b_0 \cdots b_n \cdot f \in R[x]$ und für $d = \text{ggT}(\text{Koeffizienten von } b_0 \cdots b_n f)$ gilt $g := \frac{b_0 \cdots b_n \cdot f}{d} \in R[x]$ ist primitiv und $c \cdot g = f$ mit $c = \frac{d}{b_0 \cdots b_n} \in Quot(R)$

□

Beispiel:

Sei $f = x^3 - 3x + \frac{1}{4} \in \mathbb{Q}[x]$ dann ist $g = 4x^3 - 12x + 1 \in \mathbb{Z}[x]$ primitiv und für $c = \frac{1}{4} \in Quot(\mathbb{Z}) = \mathbb{Q}$ gilt $c \cdot g = f$.

2.1.4 Lemma:

$$\text{Sei } R \text{ nullteilerfrei, } p \in R \text{ prim } \Rightarrow\ p \text{ ist prim in } R[x]$$

Beweis:

Seien $f = \sum_{i=0}^{n} a_i x^i$ und $g = \sum_{j=0}^{m} a_j x^j \in R[x]$ mit

$$p|f \cdot g = \sum_{k=0}^{m+n} c_k x^k \quad \text{mit} \quad c_k = \sum_{l=0}^{k} a_l b_{k-l} \quad \Rightarrow \quad p \mid c_k\ \forall k \qquad (*)$$

Angenommen $p \nmid f$ und $p \nmid g$. Dann $\exists i_0, j_0 :\ p \nmid a_{i_0}$ und $p \nmid b_{i_0}$. Wähle i_0, j_0 minimal. Dann gilt:

$$a_{i_0} b_{j_0} = c_{i_0+j_0} - \sum_{l=0}^{i_0-1} a_l b_{i_0+j_0-l} - \sum_{l=i_0+1}^{i_0+j_0} a_l b_{i_0+j_0-l}$$

und p teilt jeden Summanden auf der rechten Seite:

- $c_{i_0+j_0}$ wegen $(*)$
- $a_l b_{i_0+j_0-l}$ für $l < i_0 - 1$, da dann a_l von p geteilt wird, da i_0 minimal mit $p \nmid a_{i_0}$
- $a_l b_{i_0+j_0-l}$ für $l > i_0 + 1$, da dann $b_{i_0+j_0-l}$ von p geteilt wird da j_0 minimal mit $p \nmid b_{j_0}$

Es folgt:

$$p \mid a_{i_0} b_{j_0} \overset{p \text{ prim}}{\Rightarrow} p \mid a_{i_0} \text{ oder } p \mid b_{j_0} \quad \lightning$$

zu Wahl von a_{i_0}, b_{j_0}

2.1.5 Lemma:

Sei R faktoriell $f, g \in R[x]$ primitiv, dann ist auch $f \cdot g$ primitiv.

Beweis:

Angenommen $f \cdot g$ ist nicht primitiv
$\Rightarrow$ $\exists$ Primelement $p \in R$, das jeden Koeffizienten von $f \cdot g$ teilt
$\Rightarrow$ $p \mid f \cdot g$
$\Rightarrow$ $p \mid f$ oder $p \mid g$, da p auch in $R[x]$ prim ist $\lightning$

zu f, g primitiv. □

2.1.6 Lemma:

Sei R faktoriell, $f \in R[x]$ primitiv, f prim in $Quot(R)[x]$. Dann ist f prim in $R[x]$.

Beweis:

Da f primitiv ist, ist $f \neq 0$. Da $f \in Quot(R)[x]$ prim ist, ist $f \notin R^* = (R[x])^*$, also keine Einheit in $R[x]$.

Seien $g, h \in R[x]$ mit $f \mid g \cdot h$ in $R[x]$.

Dann gilt auch $f \mid g \cdot h$ in $Quot(R)[x]$, und da f dort prim ist, folgt ohne Einschränkung $f \mid g$ in $Quot(R)[x]$

$\Rightarrow$ $\exists\, q \in Quot(R)[x] : f \cdot g = g$.

Wie in 2.1.3 schreiben wir g als $g = c \cdot \tilde{g}$ mit $\tilde{g} \in R[x]$ primitiv und $c \in Quot(R)$.

Dann gilt $g = f \cdot g = c \cdot f \cdot \tilde{g}$.

Wegen $f, \tilde{g}$ primitiv in $R[x]$ folgt mit 2.1.5: $f \cdot \tilde{g}$ primitiv in $R[x]$.

Damit folgt aus 2.1.3: $c \in R \Rightarrow q \in R[x] \Rightarrow f \mid g$ in $R[x]$ □

Beweis von Satz von Gauß: 2.1.1

Sei $0 \neq f \in R[x]$, $f \notin (R[x])^* \cup \{0\}$.

Zu zeigen: f besitzt eine Darstellung als Produkt von Primelementen.

Ist $f \in R$, so folgt dies aus der tatsache, dass R faktoriell ist, und Lemma 2.1.4.

Sei $\deg(f) \geq 1$. Da $Quot(R)$ ein Lörper ist, ist $Quot(R)[x]$ euklidisch, daher Hauptidealring, daher faktoriell.

In $Quot(R)[x]$ können wir f also schreiben als

$$f = q_1 \cdots q_k \text{ mit } q_i \in Quot(R)[x] \text{ prim}$$

Wie in 2.1.3 2) schreiben wir

$$q_i = c_i \cdot p_i \text{ mit } c_i \in Quot(R) \text{ und } p_i \in R[x] \text{ primitiv}$$

p_i und q_i sind assoziiert in $Quot(R)[x]$ (da $c_i \in Quot(R)$ Einheit, da $c_i \neq 0$ und $Quot(R)$ Körper), also ist mit q_i auch p_i prim in $Quot(R)[x]$.

Wegen 2.1.6 ist p_i prim in $R[x]$. Wegen 2.1.5 ist

$$p := p_1 \cdots p_k \in R[x]$$

primitiv. Da $f = c \cdot p \in R[x]$ mit $c := c_1 \cdots c_k \in Quot(R)$ und p primitiv folgt aus 2.1.3 1) $c \in R$.

Da R faktoriell, können wir $c = b_1 \cdots b_l$ in Primfaktoren b_i zerlegen, die wegen 2.1.4 prim in $R[x]$ sind.

Damit ist $f = b_1 \cdots b_l \cdot p_1 \cdots p_k$ eine Zerlegung in Primfaktoren in $R[x]$.

Die Eindeutigkeit der Zerlegung bis auf Anordnung und Einheiten folgt per Induktion über die Anzahl der Faktoren und der definierenden Eigenschaft der Primelemente. □

Beispiel:

1) $\mathbb{Z}[x]$ ist faktoriell.

2) Ist K ein Körper, so ist $K[x_1, ..., x_n]$ faktoriell.

2.1.7 Definition:

Sei I eine beliebige Menge.

$$R[x_i \mid i \in I] = \left\{ \sum a_\alpha x_{i_1}^{\alpha_1} \cdots x_{i_k}^{\alpha_k} \;\middle|\; k \in \mathbb{N},\ \{i_1, ..., i_k\} \subset I,\ a_\alpha \in R,\ \text{nur endlich viele } a_\alpha \neq 0 \right\}$$

ist der Polynomring in den Variablen x_i mit $i \in I$.

Für $|I| < \infty$, ohne Einschränkung $I = \{1, ..., n\}$ ist es $R[x_1, ..., x_n]$.

Multiindexnotation:

Für $(i_1, ..., i_k)$ fest und $\alpha \in \mathbb{N}^k$ schreiben wir

$$x^\alpha = x_{i_1}^{\alpha_1} \cdots x_{i_k}^{\alpha_k}$$

Für $f \in R[x_i \mid i \in I]$ ist die Menge der vorkommenden Variablen (d.h. $ij:\ \exists \alpha:\ a_\alpha \neq 0,\ \alpha_j \neq 0$) $\{i_1, ..., i_k\}$ der Support von f, $supp(f)$.

Durch Hinzufügen von Nullen als Exponenten können wir ein Polynom immer bezüglich einer größeren Variablenmenge darstellen. Durch Hinzufügen von Nullen als Koeffizienten können wir auch die Exponentenmenge erweitern.

Für $f, g \in R[x_i \mid i \in I]$ schreiben wir f und g bezüglich derselben Variablenmenge $supp(f) \cup supp(g)$ sowie derselben Exponentenmenge

$$f = \sum_\alpha a_\alpha x^\alpha, \qquad g = \sum_\alpha b_\alpha x^\alpha$$

und definieren

$$f + g = \sum_\alpha (a_\alpha + b_\alpha) x^\alpha$$

$$f \cdot g = \sum_\beta \left(\sum_{\alpha + \alpha' = \beta} a_\alpha b_{\alpha'} \right) x^\beta$$

wobei die zweite Summe über alle β geht, die als Summen von Exponenten in f und g vorkommen.

Durch diese Verknüpfungen wird $R[x_i \mid i \in I]$ ein kommutativer Ring mit 1.

Beispiel zur Multiindexnotation:

Betrachte: $f = 2x_1x_2x_3^2 + 4x_1^2x_3 + 3x_2$
Die Variablenmengen $supp(f) = \{x_1, x_2, x_3\}$ und

$$\begin{aligned} \alpha_1 &= (1,1,2) \quad a_{\alpha_1} = 2 \\ \alpha_2 &= (2,0,1) \quad a_{\alpha_2} = 4 \\ \alpha_3 &= (0,1,0) \quad a_{\alpha_3} = 3 \end{aligned}$$

2.1.8 Lemma:

Sei R nullteilerfrei, I eine Menge, $J \subset I$ eine endliche Teilmenge.

1) $(R[x_i \mid i \in I])^* = R^*$
2) Sei $p \neq 0$, $p \in R[x_j \mid j \in J] \backslash R^*$

$$p \text{ prim in } R[x_j \mid j \in J] \quad \Leftrightarrow \quad p \text{ prim in } R[x_i \mid i \in I]$$

Beweis:

1) Sei $f \in (R[x_i \mid i \in I])^*$

   $\Rightarrow \exists\ g \in R[x_i \mid i \in I]:\ f \cdot g = 1$

   In f und g kommen nur endlich viele Variablen x_j mit $j \in J$ vor, daher gilt $f \cdot g = 1$ in $R[x_j \mid j \in J]$

   $\Rightarrow f \in R^*$

2)

„⇒ “ Sei p prim in $R[x_j \mid j \in J]$. Seien $f, g \in R[x_i \mid i \in I]$ mit $p \mid f \cdot g$.

Es gibt eine endliche Menge $J' \supset J$, die alle Variablen von p, f und g enthält.

$(J' = J \cup supp(f) \cup supp(g))$

$\Rightarrow$ $p \mid f \cdot g$ in $R[x_j \mid j \in J]$

Durch Induktion folgt mit 2.1.4, dass p prim in $R[x_j \mid j \in J']$ ist

$\Rightarrow$ Ohne Einschränkung: $p|f$

$\Rightarrow$ p prim in $R[x_i \mid i \in I]$

„⇐ “ Sei p prim in $R[x_i \mid i \in I]$ mit $p|f \cdot g$

$\Rightarrow$ $p|f \cdot g$ in $R[x_i \mid i \in I]$

$\Rightarrow$ Ohne Einschränkung $p \mid f \in R[x_i \mid i \in I]$ (da p prim ist)

$\Rightarrow$ $\exists q \in R[x_i \mid i \in I] : \ q \cdot p = f$

Da $p, f \in R[x_j \mid j \in J]$ kann q keine Variable x_i mit $i \notin J$ enthalten, also folgt $q \in R[x_j \mid j \in J]$

$\Rightarrow$ p prim in $R[x_j \mid j \in J]$

□

2.1.9 Proposition:

Sei I eine Menge, R faktoriell.

Dann ist $R[x_i \mid i \in I]$ ist faktoriell.

Beweis:

Sei $0 \neq f \in R[x_i \mid i \in I] \backslash R^*$.

Dann ist $J = supp(f)$ endlich und $f \in R[x_i \mid j \in J]$. In diesem Ring hat f durch Induktion und den Satz von Gauß eine eindeutige Primfaktorzerlegung, die wegen 2.1.8 eine Primfaktorzerlegung in $R[x_i \mid i \in I]$ ist. □

2.1.10 Satz: Universelle Eigenschaft von Polynomringen

Sei I eine Menge, A eine R-Algebra, $a_i \in A \ \forall i \in I$.

Dann $\exists!$ R-Algebrenhomomorphismus

$$\begin{aligned} \varphi : \ R[x_i \mid i \in I] &\to A \\ x_i &\mapsto a_i \end{aligned}$$

der Einsetzehomomorphismus.

Das Bild von φ heißt die von den a_i erzeugte Unteralgebra $\langle a_i \mid i \in I \rangle \subset A$.

Beweis:

Durch

$$\varphi \left(\sum_\alpha b_\alpha x_{i_1}^{\alpha_1} \cdots x_{i_k}^{\alpha_k} \right) = \sum_\alpha b_\alpha a_{i_1}^{\alpha_1} \cdots a_{i_k}^{\alpha_k}$$

ist der eindeutige Homomorphismus gegeben. □

3 Moduln und der Elementarteilersatz

3.1 Matrizen über Ringen und die Smith-Normalform

In Lineare Algebra 1 haben wir für $A \in \mathrm{Mat}(m \times n, K)$ wobei K ein Körper, mit Hilfe des Gauß-Algorithmus eine Normalform

$$SAT = \left(\begin{array}{c|c} \mathbb{1}_r & 0 \\ \hline 0 & 0 \end{array}\right)$$

erzielt, wobei $S \in \mathrm{Gl}(m, K),\ T \in \mathrm{Gl}(n, K),\ r = \mathrm{rang}(A)$.

Definition: Adjunkte

$$A^{\#} = (a_{ij}^{\#})_{ij},\ a_{ij}^{\#} = (-1)^{i+j}\det(A_{ji})$$

wobei $A_{ji} = A^t$ die Streichungsmatrix von A ist, bei der die j-te Zeile und die i-te Spalte gestrichen wird.

3.1.1 Satz:

Sei R ein kommutativer Ring mit 1, $A \in \mathrm{Mat}(n, R)$.

$$A^{\#} \cdot A = A \cdot A^{\#} = \det(A) \cdot \mathbb{1}_n$$

Beweis: Wie in Lineare Algebra 1, mit Verallgemeinerung. □

3.1.2 Korollar:

Es gilt:

$$A \in \mathrm{Mat}(n, R) \text{ invertierbar} \quad \Leftrightarrow \quad \det(A) \in R^*$$

Beweis:

„⇐“ $\det(A) \in R^* \Rightarrow \frac{1}{\det(A)} \cdot A^{\#}$ ist die Inverse von A.

„⇒“ $A^{-1} \cdot A = \mathbb{1}_n \Rightarrow \det(A)^{-1} \cdot \det(A) = 1 \Rightarrow \det(A) \in R^*$

□

Bemerkung:

Über Ringen gilt nicht: voller Rang ⇒ invertierbar.

z.B. $(2) \in \mathrm{Mat}(1, \mathbb{Z})$ hat vollen Rang, aber $\det(2) = 2 \notin \mathbb{Z}^*$. ⇒ (2) ist nicht invertierbar.

(Über $\mathbb{Q}$ wäre $\left(\frac{1}{2}\right)$ die inverse Matrix).

3.1.3 Satz: Smith-Normalform

Sei R ein euklidischer Ring, $A \in \mathrm{Mat}(m \times n, R)$. Dann $\exists S \in \mathrm{Gl}(m, R),\ T \in \mathrm{Gl}(n, R),\ r \leq \min\{m, n\}$ mit

$$SAT = D = \left(\begin{array}{ccc|c} d_1 & & & \\ & \ddots & & 0 \\ & & d_r & \\ \hline & 0 & & 0 \end{array}\right)$$

mit $d_i \mid d_{i+1}\ \forall i = 1, ..., r-1$.

Die d_i sind (bis auf Einheiten) durch A eindeutig bestimmt und heißen Elementarteiler von A.

D heißt Smith-Normalform von A.

Bemerkung:

Der Satz gilt allgemein für Hauptidealringe R, wir werden ihn jedoch nur für euklidische Ringe beweisen.

Der Beweis ist konstruktiv:

3.1.4 Algorithmus: Smith-Normalform

Sei R mit $\nu: R \to \mathbb{N}$ euklidischer Ring, $A \in \mathrm{Mat}(m \times n, R)$, $A \neq 0$.

1. Schritt: Zeile und Spaltenvertauschungen, so dass $a_{11} \neq 0$ und $\nu(a_{11}) \leq \nu(a_{ij})\ \forall a_{ij} \neq 0\ \forall (i,j) \neq (1,1)$
2. Schritt: Schreibe jedes a_{1j} und a_{j1}, das nicht durch a_{11} teilbar ist, als $a_{1j} = q \cdot a_{11} + r$ mit $\nu(r) \leq \nu(a_{11})$ und reduziere entsprechend mit der 1. Zeile bzw. Spalte.

   Zurück nach Schritt 1

   Da $\nu(a_{11})$ in jedem Schritt echt kleiner wird, terminiert der Prozess und wir enden mit einer Matrix, in der alle Einträge der 1. Zeile und Spalte durch a_{11} teilbar sind.
3. Schritt: Addiere Vielfache der 1. Zeile bzw. Spalte und erhalte

$$\left(\begin{array}{c|ccc} a_{11} & 0 & \cdots & 0 \\ \hline 0 & & & \\ \vdots & & A' & \\ 0 & & & \end{array}\right)$$

   Sind nicht alle Einträge von A' durch a_{11} teilbar, z.B. a_{ij} nicht teilbar, so addiere die i-te zur 1. Zeile und gehe wieder nach Schritt 2.

   Der nicht teilbare Eintrag ist jetzt in der 1. Zeile, wir verwenden wieder Division mit Rest und gehen zurück nach Schritt 1 usw. Da $\min\{\nu(a_{ij})\}$ bei jedem Durchlaufen von Schritt 2 echt kleiner wird, terminiert dieser Prozess und wir enden mit einem A', in dem alle Einträge durch a_{11} teilbar sind.

   Sind alle Eintäge von A' durch a_{11} teilbar, beginne mit A' bei Schritt 1.

Beweis:

Terminierung siehe Zwischenkommentare. Korrektheit: Rekursiv erhalten wir

$$P = \left(\begin{array}{c|c|cccc} a_{11} & 0 & \cdots & \cdots & 0 \\ \hline 0 & a_{22} & 0 & \cdots & 0 \\ \hline \vdots & 0 & a_{33} & & \\ \vdots & \vdots & & \ddots & \\ 0 & 0 & & & \ddots \end{array}\right)$$

Da alle Einträge von A' durch a_{11} teilbar sind, sind auch alle Einträge, die während des Prozesses auftauchen, durch a_{11} teilbar, insbesondere a_{22}. Die Korrektheit folgt per Induktion. Für den Induktionsanfang beachte, dass für $n = 1$ oder $m = 1$ der Algorithmus einfach Division mit Rest ist und den ggT der Einträge der Zeile bzw. Spalte produziert. □

Bemerkung:

Die Matrizen S, T erhält man durch Mitprotokollieren der Zeilen bzw. Spaltenoperationen.

Beispiel:

$$A = \begin{pmatrix} 6 & 9 & 6 \\ 6 & 6 & 7 \end{pmatrix} \in \mathrm{Mat}(2 \times 3, \mathbb{Z})$$

Die euklidische Norm ist

$$\begin{aligned} \nu : \ \mathbb{Z} &\to \mathbb{N} \\ a &\mapsto |a| \end{aligned}$$

1. Schritt: 6 hat schon kleinste Norm, weiter nach Schritt 2.
2. Schritt: $9 = 6 \cdot 1 + 3$, reduziere mit 1. Spalte

$$\left(\begin{array}{cc|ccc} 1 & 0 & 6 & 9 & 6 \\ 0 & 1 & 6 & 6 & 7 \\ \hline & & 1 & 0 & 0 \\ & & 0 & 1 & 0 \\ & & 0 & 0 & 1 \end{array}\right) \xrightarrow{\begin{array}{c}\text{Spalte} \\ II \mapsto II - I\end{array}} \left(\begin{array}{cc|ccc} 1 & 0 & 6 & 3 & 6 \\ 0 & 1 & 6 & 0 & 7 \\ \hline & & 1 & -1 & 0 \\ & & 0 & 1 & 0 \\ & & 0 & 0 & 1 \end{array}\right)$$

   Zurück nach Schritt 1, Spalten vertauschen:

$$\xrightarrow{\begin{array}{c}\text{Spalte} \\ I \leftrightarrow II\end{array}} \left(\begin{array}{cc|ccc} 1 & 0 & 3 & 6 & 6 \\ 0 & 1 & 0 & 6 & 7 \\ \hline & & -1 & 1 & 0 \\ & & 1 & 0 & 0 \\ & & 0 & 0 & 1 \end{array}\right)$$

   Jetzt sind alle in der 1. Zeile und Spalte durch 3 teilbar, reduziere mit Schritt 3:

$$\xrightarrow{\begin{array}{c}\text{Spalte} \\ II \mapsto II - 2I \\ III \mapsto III - 2I\end{array}} \left(\begin{array}{cc|ccc} 1 & 0 & 3 & 0 & 0 \\ 0 & 1 & 0 & 6 & 7 \\ \hline & & -1 & 3 & 2 \\ & & 1 & -2 & -2 \\ & & 0 & 0 & 1 \end{array}\right)$$

   $A' = (6\ 7)$, 7 ist nicht durch 3 teilbar, addiere 2. Zeile zu 1. und weiter mit Schritt 1

$$\xrightarrow{\begin{array}{c}\text{Zeile} \\ I \mapsto I + II\end{array}} \left(\begin{array}{cc|ccc} 1 & 1 & 3 & 6 & 7 \\ 0 & 1 & 0 & 6 & 7 \\ \hline & & -1 & 3 & 2 \\ & & 1 & -2 & -2 \\ & & 0 & 0 & 1 \end{array}\right)$$

   3 ist das kleinste, Schritt 2: $7 = 3 \cdot 2 + 1$ reduziere mit Spalte 1:

$$\xrightarrow{\begin{array}{c}\text{Spalte} \\ III \mapsto III - 2I\end{array}} \left(\begin{array}{cc|ccc} 1 & 1 & 3 & 6 & 1 \\ 0 & 1 & 0 & 6 & 7 \\ \hline & & -1 & 3 & 4 \\ & & 1 & -2 & -4 \\ & & 0 & 0 & 1 \end{array}\right)$$

   Schritt 1: vertausche III und I Spalte, damit 1 als kleinstes nach vorne kommt

$$\xrightarrow{\begin{array}{c}\text{Spalte} \\ III \leftrightarrow I\end{array}} \left(\begin{array}{cc|ccc} 1 & 1 & 1 & 6 & 3 \\ 0 & 1 & 7 & 6 & 0 \\ \hline & & 4 & 3 & -1 \\ & & -4 & -2 & 1 \\ & & 1 & 0 & 0 \end{array}\right)$$

   alle in 1. Zeile & Spalte teilbar durch 1. Also Schritt 3, reduziere:

$$\xrightarrow{\begin{array}{c}\text{Spalte} \\ II \mapsto II - 6I \\ III \mapsto III - 3I\end{array}} \left(\begin{array}{cc|ccc} 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 7 & -36 & -21 \\ \hline & & 4 & -21 & -13 \\ & & -4 & 22 & 13 \\ & & 1 & -6 & -3 \end{array}\right)$$

$$\xrightarrow[II \mapsto II - 7I]{\text{Zeile}} \left(\begin{array}{cc|ccc} 1 & 1 & 1 & 0 & 0 \\ -7 & -6 & 0 & -36 & -21 \\ \hline & & 4 & -21 & -13 \\ & & -4 & 22 & 13 \\ & & 1 & -6 & -3 \end{array}\right)$$

$A' = (-36 \ -21)$ alle Einträge durch 1 teilbar weiter mit A' nach Schritt 1. $\nu(-21) = 21$ ist das kleinste. Tausche Spalten:

$$\xrightarrow[II \leftrightarrow III]{\text{Spalte}} \left(\begin{array}{cc|ccc} 1 & 1 & 1 & 0 & 0 \\ -7 & -6 & 0 & -21 & -36 \\ \hline & & 4 & -13 & -21 \\ & & -4 & 13 & 22 \\ & & 1 & -3 & -6 \end{array}\right)$$

Schritt 2: Division mit Rest $-36 = -21 - 15$

$$\xrightarrow[III \mapsto III - II]{\text{Spalte}} \left(\begin{array}{cc|ccc} 1 & 1 & 1 & 0 & 0 \\ -7 & -6 & 0 & -21 & -15 \\ \hline & & 4 & -13 & -8 \\ & & -4 & 13 & 9 \\ & & 1 & -3 & -3 \end{array}\right)$$

Schritt 1: Tausche Spalten

$$\xrightarrow[II \leftrightarrow III]{\text{Spalte}} \left(\begin{array}{cc|ccc} 1 & 1 & 1 & 0 & 0 \\ -7 & -6 & 0 & -15 & -21 \\ \hline & & 4 & -8 & -13 \\ & & -4 & 9 & 13 \\ & & 1 & -3 & -3 \end{array}\right)$$

Schritt 2: Division mit Rest $-21 = -15 - 6$ reduziere

$$\xrightarrow[III \mapsto III - II]{\text{Spalte}} \left(\begin{array}{cc|ccc} 1 & 1 & 1 & 0 & 0 \\ -7 & -6 & 0 & -15 & -6 \\ \hline & & 4 & -8 & -5 \\ & & -4 & 9 & 4 \\ & & 1 & -3 & 0 \end{array}\right)$$

Schritt 1: Tausche Spalten

$$\xrightarrow[III \leftrightarrow II]{\text{Spalte}} \left(\begin{array}{cc|ccc} 1 & 1 & 1 & 0 & 0 \\ -7 & -6 & 0 & -6 & -15 \\ \hline & & 4 & -5 & -8 \\ & & -4 & 4 & 9 \\ & & 1 & 0 & -3 \end{array}\right)$$

Schritt 2: Division mit Rest $-15 = 2 \cdot (-6) - 3$

$$\xrightarrow[III \mapsto III - 2II]{\text{Spalte}} \left(\begin{array}{cc|ccc} 1 & 1 & 1 & 0 & 0 \\ -7 & -6 & 0 & -6 & -3 \\ \hline & & 4 & -5 & 2 \\ & & -4 & 4 & 1 \\ & & 1 & 0 & -3 \end{array}\right)$$

Schritt 1: Spalten tauschen

$$\xrightarrow[II \leftrightarrow III]{\text{Spalte}} \left(\begin{array}{cc|ccc} 1 & 1 & 1 & 0 & 0 \\ -7 & -6 & 0 & -3 & -6 \\ \hline & & 4 & 2 & -5 \\ & & -4 & 1 & 4 \\ & & 1 & -3 & 0 \end{array}\right)$$

alle Einträge durch -3 teilbar, reduzieren mit Schritt 3:

$$\xrightarrow[III \mapsto III - 2II]{\text{Spalte}} \left(\begin{array}{cc|ccc} 1 & 1 & 1 & 0 & 0 \\ -7 & -6 & 0 & -3 & 0 \\ \hline & & 4 & 2 & -9 \\ & & -4 & 1 & 2 \\ & & 1 & -3 & 6 \end{array}\right)$$

Die Elementarteiler sind 1, 3 (bis auf Einheiten in $\mathbb{Z}$, also bis auf Vorzeichen).

Es gilt:

$$\begin{pmatrix} 1 & 1 \\ -7 & -6 \end{pmatrix} \cdot \begin{pmatrix} 6 & 9 & 6 \\ 6 & 6 & 7 \end{pmatrix} \cdot \begin{pmatrix} 4 & 2 & -9 \\ -4 & 1 & 2 \\ 1 & -3 & 6 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -3 & 0 \end{pmatrix}$$

Zur Eindeutigkeit der Elementarteiler:

3.1.5 Satz:

Sei $A \in \mathrm{Mat}(m \times n, R)$. Für $I \subset \{1, ..., m\}$, $J \subset \{1, ..., n\}$. Sei $A_{I,J}$ die Streichungsmatrix mit den Zeilen in I und Spalten in J.
Die Menge

$$\{\det(A_{I,J}) \mid |I| = |J| = i\}$$

ist die Menge aller $i \times i$-Minoren von A. Seien $d_1, ..., d_r$ die Elementarteiler von A. Dann gilt:

$$d_1 \cdots d_i = \mathrm{ggT}(\det(A_{I,J}) \mid |I| = |J| = i) =: D_i$$

Insbesondere sind die Elementarteiler bis auf Einheiten eindeutig, und

$$d_1 = D_1 = \mathrm{ggt}(\text{aller Einträge von } A)$$

Beweisidee: (benötigt äußere Algebra, LA2)

Die Einträge der i-ten äußeren Potenz $\bigwedge^i A$ sind genau die $i \times i$-Minoren von A (bei geeigneter Basiswahl).
Es gilt

$$\bigwedge^i S \cdot \bigwedge^i A = \bigwedge^i (S \cdot A)$$

Behauptung:

$$\mathrm{ggT}\left(\text{Einträge von } \bigwedge^i (S \cdot A)\right) = \mathrm{ggT}\left(\text{Einträge } \bigwedge^i (A)\right) \text{ für } S \text{ invertierbar}$$

Jeder Eintrag von $\bigwedge^i (S \cdot A) = \bigwedge^i S \cdot \bigwedge^i A$ ist eine Linearkombination von Einträgen von

$$\bigwedge^i A \;\Rightarrow\; \mathrm{ggT}\left(\bigwedge^i A\right) \mid \mathrm{ggT}\left(\bigwedge^i (S \cdot A)\right)$$

Da S invertierbar ist, gilt $A = S^{-1}(S \cdot A)$ und wir können mit demselben Argument folgen, dass

$$\mathrm{ggT}\left(\bigwedge^i (S \cdot A)\right) \mid \mathrm{ggT}\left(\bigwedge^i A\right)$$

Analog gilt

$$\mathrm{ggT}\left(\bigwedge^i A\right) = \mathrm{ggT}\left(\bigwedge^i (A \cdot T)\right)$$

für T invertierbar. Damit folgt für $SAT = D = \begin{pmatrix} d_1 & & \\ & \ddots & \\ & & d_r \end{pmatrix}$ mit $d_i \mid d_{i+1}$, $i = 1, ..., r-1$:

$$\mathrm{ggT}\left(\bigwedge^i A\right) = \mathrm{ggT}\left(\bigwedge^i (SAT)\right) = \mathrm{ggT}\left(\bigwedge^i D\right) = \mathrm{ggT}(d_{j_1} \cdots d_{j_i} \mid 1 \le j_1 < \cdots < j_i \le r) = d_1 \cdots d_i$$

denn $d_j \mid d_k$ für $j \le k$. □

Beispiel:

$$A = \begin{pmatrix} 6 & 9 & 6 \\ 6 & 6 & 7 \end{pmatrix}, \quad d_1 = \mathrm{ggT}(\text{aller Einträge}) = 1$$

Die 2×2-Minoren sind:

$$\det \begin{pmatrix} 6 & 9 \\ 6 & 6 \end{pmatrix} = -18,\ \det \begin{pmatrix} 6 & 6 \\ 6 & 7 \end{pmatrix} = 6,\ \det \begin{pmatrix} 9 & 6 \\ 6 & 7 \end{pmatrix} = 27,\ \mathrm{ggT}(-18, 6, 27) = d_1 \cdot d_2 = 3 \;\Rightarrow\; d_2 = 3$$

3.2 Moduln

3.2.1 Definition: R-Modul

Sei R ein Ring. Ein $\underline{R}$-Modul $(M, +, \cdot)$ ist eine Menge M mit zwei Verknüpfungen

$$\begin{aligned} + &: M \times M \to M \\ \cdot &: R \times M \to M \end{aligned}$$

sodass

1) $(M, +)$ ist abelsche Gruppe
2) $r \cdot (m_1 + m_2) = r \cdot m_1 + r \cdot m_2$ (Distributivität)
   $(r_1 + r_2) \cdot m = r_1 \cdot m + r_2 \cdot m$
3) $(r_1 \cdot r_2) \cdot m = r_1 \cdot (r_2 \cdot m)$ (Assoziativität)
4) $1 \cdot m = m$

3.2.2 Beispiel:

1) Sei $R = K$ ein Körper, dann ist jeder K-Vektorraum ein K-Modul.
2) $\{\text{abelsche Gruppen}\} \overset{1:1}{\leftrightarrow} \{\mathbb{Z} - \text{Moduln}\}$

   Sei $(G, +)$ abelsche Gruppe. Setze

$$\begin{aligned} \mathbb{Z} \times G &\to G \\ (n, g) &\mapsto \underbrace{g + \cdots + g}_{n-\text{mal}} \quad \text{für } n \geq 0 \\ (-1) \cdot g &\mapsto -g \end{aligned}$$

   Dann gilt die Distributivität:

$$\begin{aligned} n(g_1 + g_2) &= g_1 + g_2 + \cdots + g_1 + g_2 \\ &= g_1 + \cdots + g_1 + g_2 + \cdots + g_2 \quad \text{da abelsch} \\ &= ng_1 + ng_2 \end{aligned}$$

   und

$$\begin{aligned} (n_1 + n_2)g &= \underbrace{g + \cdots + g}_{n_1 + n_2} \\ &= \underbrace{g + \cdots g}_{n_1} + \underbrace{g + \cdots g}_{n_2} \\ &= n_1 g + n_2 g \end{aligned}$$

   Assoziativität:

$$\begin{aligned} (n_1 \cdot n_2) \cdot g &= \underbrace{g + \cdots + g}_{n_1 \cdot n_2} \\ &= \underbrace{\underbrace{g + \cdots g}_{n_2} + \cdots + \underbrace{g + \cdots + g}_{n_2}}_{n_1} \\ &= n_1 \cdot (n_2 \cdot g) \end{aligned}$$

   und $1 \cdot g = g \;\Rightarrow\; G$ ist ein $\mathbb{Z}-$Modul
3) Sei R ein Ring, $I \subset R$ ist ein Ideal $\Leftrightarrow$ I ist $R-$Modul

   " $\Rightarrow$ " $(I, +)$ ist abelsche Gruppe, Distributivität, Assoziativität und $1 \cdot m = m$ gelten, da dies Rechnungen in R sind.

   " $\Leftarrow$ " Die Abgeschlossenheit bezüglich der $R-$Skalarmultiplikation folgt aus der Definition.

   Insbesondere ist R selbst ein $R-$Modul.

4) Sei I ein Ideal, dann ist R/I ein $R-$Modul.

5) Seien M_1, M_2 $R-$Moduln, dann ist $M_1 \times M_2$ mit komponentenweise definierter Addition und Skalarmultiplikation ein Modul. Insbesondere ist $R^n = R \times \cdots \times R$ ein $R-$Modul.

6) Sei $\varphi : R \to S$ ein Ringhomomorphismus, dann ist S mit der Addition und mit der Skalarmultiplikation definiert durch $r \cdot s := \varphi(r) \cdot s$ ein $R-$Modul, denn $(S, +)$ ist abelsche Gruppe. Distributivität:

$$\begin{aligned} r \cdot (s_1 + s_2) &= \varphi(r) \cdot (s_1 + s_2) \\ &= \varphi(r) \cdot s_1 + \varphi(r) \cdot s_2 \end{aligned}$$

und

$$\begin{aligned} (r_1 + r_2) \cdot s &= \varphi(r_1 + r_2) \cdot s \\ &= (\varphi(r_1) + \varphi(r_2)) \cdot s \\ &= \varphi(r_1) \cdot s + \varphi(r_2) \cdot s \end{aligned}$$

Assoziativität:

$$\begin{aligned} (r_1 \cdot r_2) \cdot s &= \varphi(r_1 \cdot r_2) \cdot s \\ &= \varphi(r_1 \cdot \varphi(r_2) \cdot s \\ &= r_1 \cdot (r_2 \cdot s) \end{aligned}$$

und $1 \cdot s = \varphi(1) \cdot s = 1 \cdot s = s$. Insbesondere sind $\mathbb{Q}$ und $\mathbb{R}$ $\mathbb{Z}-$Moduln.

7) Sei $R = K[x]$, V ein $K-$Vektorraum und $\varphi : V \to V$ ein Endomorphismus. Wir definieren:

$$x \cdot v := \varphi(v) \in V \quad \text{für } v \in V$$

und erhalten einen $K[x]-$Modul V: $(V, +)$ ist abelsche Gruppe. Distributivität:

$$\begin{aligned} f(x) \cdot (v_1 + v_2) &= (a_n x^n + \cdots + a_0) \cdot (v_1 + v_2) \\ &= (a_n x \cdots x + \cdots + a_0) \cdot (v_1 + v_2) \\ &= a_n \cdot (x \cdots x) \cdot (v_1 + v_2) + \cdots + a_0(v_1 + v_2) \\ &= a_n \varphi^n(v_1 + v_2) + \cdots + a_0(v_1 + v_2) \\ &= a_n \left(\varphi^n(v_1) + \varphi^n(v_2)\right) + \cdots + a_0(v_1 + v_2) \\ &= a_n \varphi^n(v_1) + a_n \varphi^n(v_2) + \cdots + a_0 v_1 + a_0 v_2 \\ &= a_n \varphi^n(v_1) + \cdots + a_0 v_1 + a_n \varphi^n(v_2) + \cdots a_0 v_2 \\ &= f(x) \cdot v_1 + f(x) \cdot v_2 \end{aligned}$$

und

$$(f(x) + g(x)) \cdot v = f(x) \cdot v + g(x) \cdot v$$

Assoziativität:

$$(f(x) \cdot g(x)) \cdot v = f(x) \cdot (g(x) \cdot v)$$

analog wie oben, $1 \cdot v = v$.

Umgekehrt: Gegeben ein $K[x]-$Modul V, so erhalten wir durch die Einschränkung der Skalarmultiplikation auf K einen $K-$Vektorraum V, und durch

$$\begin{aligned} \varphi : \ & V \to V \\ & v \mapsto x \cdot v \end{aligned}$$

einen Endomorphismus, denn

$$\begin{aligned} \varphi(v + w) &= x \cdot (v + w) \\ &= x \cdot v + x \cdot w \\ &= \varphi(v) + \varphi(w) \end{aligned}$$

und

$$\begin{aligned} \varphi(\lambda \cdot v) &= x \cdot \lambda \cdot v \\ &= \lambda \cdot x \cdot v \\ &= \lambda \cdot \varphi(v) \end{aligned}$$

Man erhält:

$$\{\text{Tupel } (V, \varphi) \text{ mit } V \ K\text{-Vektorraum}, \varphi : V \to V \text{ Endomorphismus}\} \overset{1:1}{\leftrightarrow} \{K[x]\text{-Moduln } V\}$$

3.2.3 Lemma:

Sei M ein R-Modul, $m \in M$. Es gilt:

$$0_R \cdot m = 0_M$$
$$(-1_R) \cdot m = -m$$

Beweis:

$$0 \cdot m = (0+0) \cdot m = 0 \cdot m + 0 \cdot m \quad \Rightarrow \quad 0 \cdot m = 0$$

und

$$0 = 0 \cdot m = (1-1) \cdot m = 1 \cdot m + (-1) \cdot m = m + (-1) \cdot m \quad \Rightarrow -m = (-1) \cdot m$$

□

3.2.4 Definition: Untermodul

Ein Untermodul $U \subset M$ ist eine Teilmenge, die selbst wieder ein Modul ist.

3.2.5 Lemma: Untermodulkriterium

Sei $U \subset M$ eine Teilmenge. Es gilt:

U ist Untermodul $\Leftrightarrow$
- $U \neq \varnothing$
- $m_1 + m_2 \in U \ \forall m_1, m_2 \in U$
- $r \cdot m \in U \ \forall r \in R, \ m \in U$

Beweis:

„$\Rightarrow$“ Da

$$+ : \ U \times U \to U$$
$$\cdot : \ R \times U \to U$$

„$\Leftarrow$“ Aus dem Untergruppenkriterium folgt, dass $(U, +)$ eine Untergruppe bezüglich $+$ ist, denn $m_1 + m_2 \in U$ und $-m = (-1) \cdot m \in U$.

Distributivität, Assoziativität und $1 \cdot m = m \ \forall m \in U$ gelten, da sie in M gelten. □

3.2.6 Lemma:

Sei $U \subset M$ Untermodul, dann ist M/U mit $r \cdot [m] = [r \cdot m]$ ein R-Modul.

Beweis:

$\left(M/U, +\right)$ ist abelsche Gruppe. Die Skalarmultiplikation ist wohldefiniert, denn falls

$$\begin{aligned} [m_1] = [m_2] \quad &\Rightarrow \quad m_1 - m_2 \in U \\ &\Rightarrow \quad r \cdot (m_1 - m_2) \in U \\ &\Rightarrow \quad rm_1 - rm_2 \in U \\ &\Rightarrow \quad [rm_1] = [rm_2] \end{aligned}$$

Die Rechenregeln werden vererbt. □

3.2.7 Definition:

Ein R-Modul-Homomorphismus $f : M \to N$ ist ein R-linearer Gruppenhomomorphismus, d.h.

$$f(m_1 + m_2) = f(m_1) + f(m_2) \ \forall m_1, m_2 \in M$$
$$f(r \cdot m) = r \cdot f(m) \ \forall r \in R, \ m \in M$$

3.2.8 Satz: Homomorphiesatz

Sei $f:\ M \to N$ ein R-Modulhomomorphismus. $\mathrm{Ker}(f)$, $\mathrm{Im}(f)$ sind Untermoduln von M bzw. N und es gilt

$$\begin{aligned} \tilde{f}:\ {}^{M}\!/_{\mathrm{Ker}(f)} &\cong \mathrm{Im}(f) \\ [m] &\mapsto f(m) \end{aligned}$$

Beweis:

Folgt aus dem Homomorphiesatz für Gruppen, nur die Verträglichkeit mit der Skalarmultiplikation ist zu prüfen:

$$\begin{aligned} \tilde{f}\,(r \cdot [m]) &= \tilde{f}\,([r \cdot m]) \\ &= f(r \cdot m) \\ &= r \cdot f(m) \\ &= r \cdot \tilde{f}([m]) \end{aligned}$$

□

3.2.9 Definition: Endlich erzeugt

$$M \text{ heißt } \underline{\text{endlich erzeugt}} \quad \Leftrightarrow \quad \exists\, f:\ R^n \to M \text{ (surjektiver Modulhomomorphismus)}$$

3.2.10 Bemerkung:

Seien $e_1, ..., e_n$ die Standard-Einheits-Vektoren von R^n, setze $m_i := f(e_i)$.

f surjektiv $\Leftrightarrow$ Jedes Element von M lässt sich in der Form:
$f(r) = f(r_1 e_1 + \cdots + r_n e_n) = r_1 f(e_1) + \cdots + r_n f(e_n) = r_1 m_1 + \cdots + r_n m_n$
schreiben, also als R-Linearkombination der m_i

$\Leftrightarrow$ Die m_i erzeugen M als R-Modul: $M = \langle m_1, ..., m_n \rangle_R$

Die m_i müssen keine Basis bilden, die Darstellung als R-Linearkombination der m_i muss nicht eindeutig sein:

Beispiel:

$\mathbb{Z}_3$ ist ein $\mathbb{Z}$-Modul, und endlich erzeugt, denn $\mathbb{Z} \to {}^{\mathbb{Z}}\!/_{3\mathbb{Z}} = \mathbb{Z}_3$ ist ein surjektiver $\mathbb{Z}$-Modulhomomorphismus.

Aber $[0] = 3 \cdot [1] = 0 \cdot [1]$ hat keine eindeutige Darstellung als $\mathbb{Z}$-Linearkombination des Erzeugers $[1]$.

3.2.11 Definition: Freier Modul

$$\text{Ein endlich erzeugter } R\text{-Modul } M \text{ heißt } \underline{\text{frei}} \quad \Leftrightarrow \quad \exists \text{ Isomorphismus } M \cong R^n$$

Insbesondere bilden die Bilder m_i der e_i dann eine Basis von M, d.h. jedes Element von M lässt sich eindeutig als R-Linearkombination der m_i darstellen.

Beispiel:

1) $\mathbb{Q}$ als $\mathbb{Z}$-Modul ist nicht endlich erzeugt: Angenommen, $\mathbb{Q}$ wäre von $r_1, ..., r_n$ erzeugt. Wähle d teilerfremd zu den Nennern der r_i. Sei $a \in \langle r_1, ...r_n \rangle_{\mathbb{Z}} \ \Rightarrow\ a = a_1 r_1 + \cdots + a_n r_n$ mit $a_i \in \mathbb{Z}$. Sei

$$r_i = \frac{p_i}{q_i} \ \Rightarrow\ a = a_1 \frac{p_1}{q_1} + \cdots + a_n \frac{p_n}{q_n} = \frac{\cdots}{\mathrm{kgV}(q_1, ..., q_n)} \neq \frac{1}{d}$$
$$\Rightarrow\ \frac{1}{d} \notin \langle r_1, ..., r_n \rangle_{\mathbb{Z}}$$

2) Ein K-Vektorraum ist ein freier K-Modul.

3) Sei $R = K[x_i \mid i \in \mathbb{N}]$ der Polynomring in abzählbar vielen Variablen. R als R-Modul ist endlich erzeugt, sogar frei mit Basis 1.

   Betrachte $U = \{f \in R \mid f(0) = 0\}$ die Polynome ohne konstanten Koeffizienten. Da $0 \in U$ ist $U \neq \varnothing$.

Es gilt:

$$f, g \in U \Rightarrow (f+g)(0) = f(0) + g(0) = 0 + 0 = 0$$
$$\Rightarrow f + g \in U$$

und

$$f \in U \text{ und } r \in R \Rightarrow r \cdot f(0) = r \cdot 0 = 0$$
$$\Rightarrow r \cdot f \in U$$

Nach dem Untermodulkriterium 3.2.5 ist U ein Untermodul.

Behauptung:

U ist nicht endlich erzeugt ($U = \langle x_i | i \in \mathbb{N} \rangle_R$).

Angenommen, $U = \langle f_1, ..., f_k \rangle_R$. In jedem f_i gibt es nur endlich viele Variablen, seien ohne Einschränkung $x_1, ..., x_n$ die Variablen, die in allen f_i vorkommen. Betrachte eine R-Linearkombination $r_1 f_1 + \cdots r_k f_k$ mit $r_i \in R$.

Die f_i haben keinen konstanten Anteil, d.h. jeder Term eines f_i enthält ein x_j, $j = 1, ..., n$.

Aber $x_{n+1} \in U$ und x_{n+1} lässt sich nicht als Summe von Termen darstellen, von denen jeder ein x_j, $j = 1, ..., n$ enthält.

$\Rightarrow U \neq \langle f_1, ..., f_n \rangle_R$. U ist also nicht endlich erzeugt.

Insbesondere können Untermoduln von endlich erzeugten Moduln selbst nicht endlich erzeugt sein.

3.2.12 Definition: Exakte Sequenzen

Eine Sequenz von R-Moduln und R-Modulhomomorphismen:

$$\cdots \; M_{i-1} \xrightarrow{\varphi_{i-1}} M_i \xrightarrow{\varphi_i} M_{i+1} \xrightarrow{\varphi_{i+1}} \; \cdots$$

heißt <u>exakt</u> bei $M_i :\Leftrightarrow \operatorname{Ker}(\varphi_i) = \operatorname{Im}(\varphi_{i-1})$

Eine Sequenz heißt exakt, wenn sie exakt bei jedem inneren Eintrag ist.

Beispiel:

1) $N \xrightarrow{\varphi} M \longrightarrow 0$ ist exakt $\Leftrightarrow$ Ker(Nullabbildung) $= M = \operatorname{Im}(\varphi) \Leftrightarrow \varphi$ surjektiv

2) $0 \longrightarrow N \xrightarrow{\varphi} M$ ist exakt $\Leftrightarrow$ Bild(Inklusion der 0) $= \{0\} = \operatorname{Ker}(\varphi) \Leftrightarrow \varphi$ injektiv

3.3 Endlich präsentierte Moduln

3.3.1 Definiton: Endlich präsentiert

M heißt endlich präsentiert wenn M durch φ erzeugt wird, also $\varphi: R^m \to M$ surjektiv ist, und $\mathrm{Kern}(\varphi)$ selbst wieder endlich erzeugt wird.

3.3.2 Lemma:

$$M \text{ endlich präsentiert} \quad \Leftrightarrow \quad \exists \text{ exakte Sequenz } R^n \xrightarrow{f} R^m \longrightarrow M \longrightarrow 0$$

Beweis:

„⇒ “ M ist endlich erzeugt durch $\varphi : R^m \to M$

φ ist surjektiv $\Rightarrow$ $R^m \xrightarrow{\varphi} M \longrightarrow 0$ ist exakt

$\Rightarrow$ $0 \to \mathrm{Ker}(\varphi) \to R^m \to M \to 0$ ist exakt

Da $\mathrm{Kern}(\varphi)$ endlich erzeugt, $\exists\ R^n \twoheadrightarrow \mathrm{Kern}(\varphi)$

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathrm{Kern}(\varphi) & \longrightarrow & R^m & \longrightarrow & M & \longrightarrow & 0 \\ & & \uparrow & \nearrow_{f} & & & & & \\ & & R^n & & & & & & \end{array}$$

Damit existiert

$$R^n \xrightarrow{f} R^m \xrightarrow{\varphi} M \longrightarrow 0$$

und ist exakt.

„⇐“ Sei $R^n \xrightarrow{f} R^m \xrightarrow{\varphi} M \longrightarrow 0$ exakt.

$\Rightarrow$ φ ist surjektiv

$\Rightarrow$ M ist endlich erzeugt.

Außerdem gilt $\mathrm{Kern}(f) = \mathrm{Im}(f)$

$\Rightarrow$ $R^n \xrightarrow{f} \mathrm{Im}(f)$ zeigt, dass $\mathrm{Kern}(\varphi)$ selbst endlich erzeugt ist.

$\Rightarrow$ M ist endlich präsentiert. □

3.3.3 Definition: Präsentationsmatrix

Die Abbildung

$$R^n \xrightarrow{f} R^m$$

ist ein Morphismus freier Moduln und daher durch die Bilder $f(e_1), ..., f(e_n)$ festgelegt. Diese Bilder schreiben wir in der Basis $e_1, ..., e_m$ (ähnlich wie bei der darstellenden Matrix aus Lina 1) und erhalten so eine $m \times n$ Matrix $A \in \mathrm{Mat}(m \times n, R)$ die Präsentationsmatrix von M.

Es gilt:

$$M = \mathrm{Im}(\varphi) \cong R^m/\mathrm{Kern}(\varphi) = R^m/\mathrm{Im}(f) = R^m/\mathrm{Im}(A)$$

das heißt, M ist durch A vollständig beschrieben. $\mathrm{Im}(A)$ liefert alle Relationen zwischen Erzeugern $\varphi(e_i)$ von M, d.h. für alle Gleichungen $r_1\varphi(e_1) + \cdots + r_m\varphi(e_m) = 0$, die die Erzeuger $\varphi(e_i)$ erfüllen, gilt

$$\begin{pmatrix} r_1 \\ \vdots \\ r_m \end{pmatrix} \in \mathrm{Im}(A)$$

3.3.4 Satz:

M sei ein R-Modul. Äquivalent sind:

1) Jede ansteigende Kette von Untermoduln wird stationär
2) Jeder Untermodul von M ist endlich erzeugt
3) Jede Teilmenge von Untermoduln enthält ein maximales Element

Beweis wie bei Ringen.

3.3.5 Definition: Noetherscher Modul

Ein Modul, der die Eigenschaften aus 3.3.4 erfüllt, heißt noethersch.

3.3.6 Proposition:

Sei

$$0 \longrightarrow M' \xrightarrow{i} M \xrightarrow{\pi} M'' \longrightarrow 0$$

eine exakte Sequenz von R-Moduln.

$$M \text{ noethersch} \quad \Leftrightarrow \quad M',\ M'' \text{ noethersch}$$

Beweis:

- **Behauptung:**

$$N_1,\ N_2 \subset M \text{ Untermoduln mit } N_1 \subset N_2,\ \pi(N_1) = \pi(N_2),\ i(M') \cap N_1 = i(M') \cap N_2 \quad \Rightarrow \quad N_1 = N_2$$

Beweis:

$$\begin{aligned}
x \in N_2 \ &\Rightarrow\ \pi(x) \in \pi(N_2) = \pi(N_1) \\
&\Rightarrow\ \exists x' \in N_1 :\ \pi(x) = \pi(x') \\
&\Rightarrow\ \pi(x - x') = 0 \\
&\Rightarrow\ x - x' \in \mathrm{Kern}(\pi) = \mathrm{Im}(i) = i(M') \\
&\quad\ \text{Da } x' \in N_1 \subset N_2,\ x \in N_2 \\
&\Rightarrow\ x - x' \in N_2 \\
&\Rightarrow\ x - x' \in N_2 \cap i(M') = N_1 \cap i(M') \\
&\Rightarrow\ x - x' \in N_1, \text{ da } x' \in N_1 \\
&\Rightarrow\ x \in N_1
\end{aligned}$$

„⇐ “ Seien M', M'' noethersch.

$$\begin{aligned}
&\Rightarrow\ M_1 \subset M_2 \subset \cdots && \text{ist eine Kette von Untermoduln in } M \\
&\Rightarrow\ \pi(M_1) \subset \pi(M_2) \subset \cdots && \text{ist eine Kette in } M'' \\
&\Rightarrow\ i(M') \cap M_1 \subset i(M') \cap M_2 \subset \cdots && \text{ist eine Kette in } M'
\end{aligned}$$

Da beide noethersch, stabilisieren beide Ketten.

Wähle n groß genug, dass beide stabil sind

$$\begin{aligned}
&\Rightarrow \pi(M_N) = \pi(M_n)\ \forall N \geq n \\
&\quad\ i(M') \cap M_N = i(M') \cap M_n\ \forall N \geq n \\
&\overset{\text{Beh}}{\Rightarrow} M_N = M_n\ \forall N \geq n \\
&\Rightarrow \text{Die Kette wird stationär} \\
&\Rightarrow M \text{ ist noethersch}
\end{aligned}$$

” ⇒ ” Sei M noethersch.

Jede Kette in M' oder M'' induziert eine Kette in M via i bzw. π^{-1}, die stationär wird, die ursprüngliche deshalb auch. □

3.3.7 Lemma:

$$R \text{ noethersch } \Rightarrow R^n \text{ noethersch}$$

Beweis: Induktion über n

$n = 1$ klar. Sei R^{n-1} noethersch. Betrachte:

$$R^{n-1} \xrightarrow{i} R^n \xrightarrow{\pi} R$$

$$\begin{pmatrix} x_1 \\ \vdots \\ x_{n-1} \end{pmatrix} \mapsto \begin{pmatrix} x_1 \\ \vdots \\ x_{n-1} \\ 0 \end{pmatrix} \begin{pmatrix} v_1 \\ \vdots \\ \vdots \\ v_n \end{pmatrix} \mapsto v_n$$

i ist injektiv, π ist surjektiv

$$\text{Kern}(\pi) = \text{Im}(i) \Rightarrow 0 \to R^{n-1} \to R^n \to R \to 0 \text{ ist exakt}$$

da R^{n-1}, R noethersch folgt mit Proposition 3.3.6 R^n noethersch. □

3.3.8 Satz:

Endlich erzeugte Moduln über noetherschen Ringen sind schon endlich präsentiert.

Beweis:

$$M \text{ endlich erzeugt } \Rightarrow \exists R^m \overset{\varphi}{\twoheadrightarrow} M$$

Dann ist

$$0 \to \text{Kern}(\varphi) \to R^m \to M \to 0$$

exakt, R^m ist noethersch wegen 3.3.7.

$\overset{3.3.6}{\Rightarrow}$ Kern(φ) noethersch

$\overset{3.3.4}{\Rightarrow}$ Kern(φ) endlich erzeugt

$\Rightarrow$ M endlich präsentiert

□

3.3.9 Korollar:

Endlich erzeugte Moduln über noetherschen Ringen sind noethersch.

Beweis:

Mit derselben exakten Sequenz

$$0 \to \text{Kern}(\varphi) \to R^m \to M \to 0$$

folgt auch M ist noethersch. □

3.4 Der Elementarteilersatz

3.4.1 Beispiel:

Eine endlich erzeugte abelsche Gruppe (d.h. ein endlich erzeugter $\mathbb{Z}$-Modul, siehe Beispiel 3.2.2 2)) lässt sich durch eine Präsentationsmatrix beschreiben (Satz 3.3.8), z.B.:

$$0 \longrightarrow \mathbb{Z}^3 \xrightarrow{A} \mathbb{Z}^4 \xrightarrow{\varphi} G \longrightarrow 0$$

Sei die Matrix:

$$A = \begin{pmatrix} 1 & 1 & 1 \\ -3 & 1 & 1 \\ 1 & -3 & 1 \\ 1 & 1 & -3 \end{pmatrix} \qquad \text{dann ist} \qquad G \cong {}^{\mathbb{Z}^4}\!/_{\mathrm{Kern}(\varphi)} = {}^{\mathbb{Z}^4}\!/_{\mathrm{Im}(A)}$$

Bestimme die Smith-Normalform von A, und die Basiswechsel:

$$\left(\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & -3 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & -3 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & -3 \\ \hline & & & & 1 & 0 & 0 \\ & & & & 0 & 1 & 0 \\ & & & & 0 & 0 & 1 \end{array}\right) \quad \begin{array}{c} \text{Zeilen} \\ II \mapsto II + 3I \\ III \mapsto III - I \\ IV \mapsto IV - I \\ \longrightarrow \end{array} \quad \left(\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 3 & 1 & 0 & 0 & 0 & 4 & 4 \\ -1 & 0 & 1 & 0 & 0 & -4 & 0 \\ -1 & 0 & 0 & 1 & 0 & 0 & -4 \\ \hline & & & & 1 & 0 & 0 \\ & & & & 0 & 1 & 0 \\ & & & & 0 & 0 & 1 \end{array}\right)$$

$$\begin{array}{c} \text{Spalten} \\ II \mapsto II - I \\ III \mapsto III - I \\ \longrightarrow \end{array} \quad \left(\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 3 & 1 & 0 & 0 & 0 & 4 & 4 \\ -1 & 0 & 1 & 0 & 0 & -4 & 0 \\ -1 & 0 & 0 & 1 & 0 & 0 & -4 \\ \hline & & & & 1 & -1 & -1 \\ & & & & 0 & 1 & 0 \\ & & & & 0 & 0 & 1 \end{array}\right) \quad \text{Weiter mit } A' = \begin{pmatrix} 4 & 4 \\ -4 & 0 \\ 0 & -4 \end{pmatrix}$$

$$\begin{array}{c} \text{Zeile} \\ III \mapsto III + II \\ \longrightarrow \end{array} \quad \left(\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 3 & 1 & 0 & 0 & 0 & 4 & 4 \\ 2 & 1 & 1 & 0 & 0 & 0 & 4 \\ -1 & 0 & 0 & 1 & 0 & 0 & -4 \\ \hline & & & & 1 & -1 & -1 \\ & & & & 0 & 1 & 0 \\ & & & & 0 & 0 & 1 \end{array}\right)$$

$$\begin{array}{c} \text{Spalte} \\ III \mapsto III - II \\ \longrightarrow \end{array} \quad \left(\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 3 & 1 & 0 & 0 & 0 & 4 & 0 \\ 2 & 1 & 1 & 0 & 0 & 0 & 4 \\ -1 & 0 & 0 & 1 & 0 & 0 & -4 \\ \hline & & & & 1 & -1 & 0 \\ & & & & 0 & 1 & -1 \\ & & & & 0 & 0 & 1 \end{array}\right) \quad \text{Weiter mit } A' = \begin{pmatrix} 4 \\ -4 \end{pmatrix}$$

$$\begin{array}{c} \text{Zeile} \\ IV \mapsto IV + III \\ \longrightarrow \end{array} \quad \left(\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 3 & 1 & 0 & 0 & 0 & 4 & 0 \\ 2 & 1 & 1 & 0 & 0 & 0 & 4 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ \hline & & & & 1 & -1 & 0 \\ & & & & 0 & 1 & -1 \\ & & & & 0 & 0 & 1 \end{array}\right)$$

Man erhält:

$$\underbrace{\begin{pmatrix} 1 & 0 & 0 & 0 \\ 3 & 1 & 0 & 0 \\ 2 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{pmatrix}}_{S} \underbrace{\begin{pmatrix} 1 & 1 & 1 \\ -3 & 1 & 1 \\ 1 & -3 & 1 \\ 1 & 1 & -3 \end{pmatrix}}_{A} \underbrace{\begin{pmatrix} 1 & -1 & 0 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix}}_{T} = \underbrace{\begin{pmatrix} 1 & 0 & 0 \\ 0 & 4 & 0 \\ 0 & 0 & 4 \\ 0 & 0 & 0 \end{pmatrix}}_{D}$$

Die Elementarteiler sind 1, 4, 4.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbb{Z}^3 & \xrightarrow{A} & \mathbb{Z}^4 & \longrightarrow & G & \longrightarrow & 0 \\ & & \cong\uparrow T & & \cong\downarrow S & & \cong & & \\ 0 & \longrightarrow & \mathbb{Z}^3 & \xrightarrow{D} & \mathbb{Z}^4 & \longrightarrow & G' & \longrightarrow & 0 \end{array}$$

$$G' \cong {}^{\mathbb{Z}^4}\!/_{\mathrm{Im}(D)} = {}^{\mathbb{Z}^4}\!/_{\left\langle \begin{pmatrix}1\\0\\0\\0\end{pmatrix}, \begin{pmatrix}0\\4\\0\\0\end{pmatrix}, \begin{pmatrix}0\\0\\4\\0\end{pmatrix} \right\rangle_{\mathbb{Z}}} \cong {}^{\mathbb{Z}}\!/_{4\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{4\mathbb{Z}} \times \mathbb{Z}$$

das heißt, die Erzeuger $e_1, ..., e_4$ von G' gegeben durch die kanonische Basis von $\mathbb{Z}^4$ erfüllen $e_1 = 0$, $4 \cdot e_2 = 0$, $4 \cdot e_3 = 0$.

$$G \cong {}^{\mathbb{Z}^4}\!/_{\mathrm{Im}(A)} = {}^{Z^4}\!/_{\mathrm{Im}(AT)} = {}^{Z^4}\!/_{\mathrm{Im}(S^{-1}D)} \cong {}^{\mathbb{Z}^4}\!/_{\mathrm{Im}(D)} \cong G'$$

Verwende die Spalten von S^{-1} als Basis

$$S^{-1} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ -3 & 1 & 0 & 0 \\ 1 & -1 & 1 & 0 \\ 1 & 0 & -1 & 1 \end{pmatrix}$$

und setze

$$v_1 = \begin{pmatrix} 1 \\ -3 \\ 1 \\ 1 \end{pmatrix},\ v_2 = \begin{pmatrix} 0 \\ 1 \\ -1 \\ 0 \end{pmatrix},\ v_3 = \begin{pmatrix} 0 \\ 0 \\ 1 \\ -1 \end{pmatrix},\ v_4 = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

Dann gilt $v_1,\ 4 \cdot v_2,\ 4 \cdot v_3 \in \mathrm{Im}(A)$, denn

$e_1,\ 4 \cdot e_2,\ 4 \cdot e_3 \in \mathrm{Im}(D)$
$\Rightarrow \exists w_1, w_2, w_3 \in \mathbb{Z}^3 :\ D \cdot w_1 = e_1,\ D \cdot w_2 = 4 \cdot e_2,\ D \cdot w_3 = 4 \cdot e_3$
$\Rightarrow SATw_1 = e_1,\ SATw_2 = 4e_2,\ SATw_3 = 4e_3$
$\Rightarrow A(Tw_1) = S^{-1}e_1 = v_1,\ A(Tw_2) = 4v_2,\ A(Tw_3) = 4v_3$

3.4.2 Bemerkung:

Allgemein: Sei R euklidischer Ring (bzw. allgemeiner: Hauptidealring), M endlich erzeugter R-Modul.
Wegen Satz 3.3.8 ist M dann schon endlich präsentiert

$$R^n \xrightarrow{A} R^m \xrightarrow{\pi} M \longrightarrow 0 \qquad \text{mit } A \in \mathrm{Mat}(m \times n, R)$$

Der Satz über die Smith-Normalform 3.1.3 liefert $S \in \mathrm{Gl}(m, R),\ T \in \mathrm{Gl}(n, R)$ mit

$$\begin{array}{ccccccc} R^n & \xrightarrow{A} & R^m & \longrightarrow & M & \longrightarrow & 0 \\ \cong\uparrow & T & \cong\downarrow & S & \cong & & \\ R^n & \xrightarrow{D} & R^m & \longrightarrow & M' & \longrightarrow & 0 \end{array} \qquad \text{mit } D = \begin{pmatrix} d_1 & & \\ & \ddots & \\ & & d_r \end{pmatrix}$$

Dann sind die $v_i = \pi(S^{-1} \cdot e_i)$ Erzeuger von M mit Relationen $d_1 v_1 = 0, \cdots, d_r v_r = 0$.

Ist d_i eine Einheit, so folgt aus $d_i v_i = 0$ schon $v_i = 0$ und wir können den Erzeuger v_i streichen.

3.4.3 Definition:

1) Sei M ein Modul, $U_i \subset M$ Untermoduln, wir schreiben $M = U_1 \oplus \cdots \oplus U_n$ falls sich jedes Element in M als Summe von Elementen in den U_i schreiben lässt und falls aus $U_1 + \cdots + U_m = 0$ mit $u_i \in U_i$ folgt $u_i = 0\ \forall i$.

2) M heißt zyklisch, wenn er von einem Element erzeugt wird.

3) $T = \{m \in M \mid \exists r \in R,\ r \neq 0 \text{ mit } r \cdot m = 0\} \subset M$ heißt Torsionsuntermodul.

3.4.4 Elementarteilersatz

Sei R ein euklidischer Ring (bzw. allgemeiner: Hauptidealring), sei M ein endlich erzeugter Modul.

1) $\exists v_1, ..., v_m$ Erzeuger von M und $d_1, ..., d_r \in R$ (die (nicht Einheiten) Elementarteiler),
$r \leq m,\ d_i \notin R^*,\ d_i \mid d_{i+1}\ i = 1, ..., r-1$, so dass M durch die Relationen $d_i \cdot v_i = 0$ beschrieben wird.

2) $M = U_1 \oplus \cdots \oplus U_m$ ist direkte Summe zyklischer Untermoduln U_i und

$$U_i \cong \begin{cases} R/d_i R & i \leq r \\ R & i > r \end{cases}$$

Anders gesagt

$$M \cong R/\langle d_1 \rangle \times \cdots \times R/\langle d_r \rangle \times R^{m-r}$$

Der Rang $m - r$ und die Elementarteiler sind durch M eindeutig bestimmt.

Beweis:

Konstruktiv, wie in Bemerkung 3.4.2 mit dem Smith-Normalform-Algorithmus (3.1.3):

$$M = R^m/\mathrm{Im}(A) \cong M' = R^m/\mathrm{Im}(D) \overset{*}{=} R^m/\langle d_1 \cdot e_1, ..., d_r e_r \rangle \quad * \text{ wobei Einheiten schon weggelassen werden}$$

Für die Basiswechsel S, T mit $SAT = D$ gilt $v_i = \pi(S^{-1} e_i)$ sind Erzeuger von M, die $d_i \cdot v_i = 0$ erfüllen, also

$$\begin{aligned} M &= R^m/\langle d_1 v_1, ..., d_r v_r \rangle \\ &= \langle v_1 \rangle \oplus \cdots \oplus \langle v_m \rangle / \langle d_1 v_1, ..., d_r v_r \rangle \\ &= \langle v_1 \rangle / \langle d_1 v_1 \rangle \oplus \cdots \oplus \langle v_r \rangle / \langle d_r v_r \rangle \oplus \langle v_{r+1} \rangle \oplus \cdots \oplus \langle v_m \rangle \\ &\cong R/d_1 R \times \cdots \times R/d_r R \times R^{m-r} \end{aligned}$$

□

3.4.5 Korollar:

Sei R euklidischer Ring (Hauptidealring), M endlich erzeugter Modul. Sei T der Torsionsmodul von M, dann $\exists$ freier Untermodul $F \subset M$ mit $M = T \oplus F$.

Beweis:

Mit dem Elementarteilersatz 3.4.4 gilt

$$T = U_1 \oplus \cdots \oplus U_r \cong {}^{R}\!/_{d_1 R} \times \cdots \times {}^{R}\!/_{d_r R}$$

und

$$F = U_{r+1} \oplus \cdots \oplus U_m \cong R^{m-r}$$

□

Beispiel: (Siehe Beispiel 3.4.1)

$$A = \begin{pmatrix} 1 & 1 & 1 \\ -3 & 1 & 1 \\ 1 & -3 & 1 \\ 1 & 1 & -3 \end{pmatrix}, \quad G = {}^{\mathbb{Z}^4}\!/_{\mathrm{Im}(A)}$$

G wird erzeugt von

$$v_2 = \begin{pmatrix} 0 \\ 1 \\ -1 \\ 0 \end{pmatrix}, \quad v_3 = \begin{pmatrix} 0 \\ 0 \\ 1 \\ -1 \end{pmatrix}, \quad v_4 = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

mit $4 \cdot v_2 = 0$, $4 \cdot v_3 = 0$

$\Rightarrow G = \langle v_2 \rangle \oplus \langle v_3 \rangle \oplus \langle v_4 \rangle$

Der Torsionsmodul T ist $T = \langle v_2, v_3 \rangle$, $T \cong \mathbb{Z}_4 \times \mathbb{Z}_4$, $\langle v_4 \rangle$ ist frei. Statt v_4 kann man als freie Erzeuger auch e_2 oder e_3 wählen z.B. T ist eindeutig.

3.4.6 Definition: Torsionsfrei/Torsionsmodul

M heißt torsionsfrei, wenn $T = \{0\}$ und Torsionsmodul, wenn $M = T$.

3.4.7 Korollar:

Sei R euklidischer Ring (Hauptidealring), M endlich erzeugter Modul.

$$M \text{ frei} \quad \Leftrightarrow \quad M \text{ torsionsfrei}$$

3.4.8 Korollar:

Sei R euklidischer Ring (Hauptidealring). Jeder Untermodul eines freien R-Moduls ist wieder frei.

Beweis:

M frei $\Rightarrow M$ torsionsfrei
$\Rightarrow U \subset M$ enthält auch keine Torsionselemente
$\Rightarrow U$ frei

□

Wir können die Zerlegung

$$M \cong {}^{R}\!/_{\langle d_1 \rangle} \times \cdots \times {}^{R}\!/_{\langle d_r \rangle} \times R^{m-r}$$

aus dem Elementarteilersatz 3.4.4 noch weiter verfeinern mit dem chinesischen Restsatz:

Ist $d \in R$ und $d = p_1^{r_1} \cdots p_l^{r_l}$ eine Primfaktorzerlegung mit $r_i > 0$, dann folgt mit dem chinesischem Restsatz

$${}^{R}\!/_{\langle d \rangle} \cong {}^{R}\!/_{\langle p_1^{r_1} \rangle} \times \cdots \times {}^{R}\!/_{\langle p_l^{r_l} \rangle}$$

da die Ideale $\langle p_i^{r_i} \rangle$ coprim sind. Daher folgt folgender Satz direkt aus dem Elementarteilersatz und dem chinesischen Restsatz:

3.4.9 Satz:

Sei R euklidisch (bzw. allgemeiner: Hauptidealring), sei M endlich erzeugter R-Modul. Dann $\exists\ t \in \mathbb{N}_{\geq 0}$ und Primelemente $p_1, ..., p_k \in R,\ r_1, ..., r_k \in \mathbb{N}_{\geq 0}$ mit

$$M \cong {}^{R}\!/_{\langle p_1^{r_1} \rangle} \times \cdots \times {}^{R}\!/_{\langle p_k^{r_k} \rangle} \times R^t$$

und diese Darstellung ist eindeutig bis auf Reihenfolge der Faktoren.

Da $\mathbb{Z}$-Moduln abelsche Gruppen sind (Beispiel 3.2.2 2)) folgt insbesondere:

3.4.10 Satz: Klassifikation der endlich erzeugten abelschen Gruppen

Sei G eine endlich erzeugte abelsche Gruppe

1) G ist direkte Summe von zyklischen Untergruppen
2) $\exists\ 0 \leq r \leq m,\ d_1, ..., d_r \geq 2,\ d_i \mid d_{i+1}\ \forall i = 1, ..., r-1$ mit:
$$G \cong \mathbb{Z}_{d_1} \times \cdots \times \mathbb{Z}_{d_r} \times \mathbb{Z}^{m-r}$$
3) $\exists$ Primzahlen $p_1, ..., p_k$ und $r_1, ..., r_k > 0$ mit:
$$G \cong \mathbb{Z}_{p_1^{r_1}} \times \cdots \times \mathbb{Z}_{p_k^{r_k}} \times \mathbb{Z}^{m-r}$$

Dabei sind r, m, d_i, p_i, r_i bis auf Reihenfolge (und Einheiten) eindeutig bestimmt.

Beispiel: Sei G gegeben durch die Präsentationsmatrix

$$\begin{pmatrix} 2 & & & \\ & 3 & & \\ & & 4 & \\ & & & 18 \end{pmatrix} \in \mathrm{Mat}(4, 2)$$

$$\begin{aligned}
&\text{ggT(Einträge)} = 1 \quad \Rightarrow\ d_1 = 1 \\
&\text{ggT}(2 \times 2\text{-Minoren}) = \text{ggt}(6, 8, 36, 12, 54, 72) \\
&\qquad\qquad\qquad\quad = 2 \ \Rightarrow\ d_2 = 2 \\
&\text{ggT}(3 \times 3\text{-Minoren}) = \text{ggT}(24, 108, 144, 216) \\
&\qquad\qquad\qquad\quad = 12 \ \Rightarrow\ d_3 = 6 \\
&\det = 2 \cdot 3 \cdot 4 \cdot 18 \quad \Rightarrow\ d_4 = 2 \cdot 18 = 36
\end{aligned}$$

Man erhält:

$$\Rightarrow D = \begin{pmatrix} 1 & & & \\ & 2 & & \\ & & 6 & \\ & & & 36 \end{pmatrix}$$

$$\begin{aligned}
&\Rightarrow G \cong \mathbb{Z}_2 \times \mathbb{Z}_6 \times \mathbb{Z}_{36} \\
&\quad 6 = 2 \cdot 3,\ 36 = 2^2 \cdot 3^2 \\
&\Rightarrow G \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_4 \times \mathbb{Z}_9
\end{aligned}$$

3.5 Die Jordannormalform

Beispiel 3.2.2:

$$\{\text{Tupel } (V,\varphi) \text{ mit } V \ K\text{-Vektorraum}, \varphi : V \to V \text{ Endomorphismus}\} \overset{1:1}{\leftrightarrow} \{K[x]\text{-Moduln } V\}$$

wobei die Modulstruktur durch $x \cdot v = \varphi(v)$ gegeben ist. Sei $V = K^n$ und φ durch die Matrix A gegeben. Für $f \in K[x]$ gilt dann $f \cdot v = f(A) \cdot v$.

3.5.1 Lemma:

Sei K^n mittels $A \in \mathrm{Mat}(n,K)$ ein $K[x]$-Modul. Ein Unterraum $U \subset K^n$ ist $K[x]$-Untermodul
$\Leftrightarrow \ A \cdot U \subset U$

Beweis:

" $\Leftarrow$ " Summen sind in U, da es ein Unterraum ist.

$K[x]$-Vielfache $f \cdot v = f(A) \cdot v$ sind in U, da $A \cdot U \subset U$.

" $\Rightarrow$ " $x \cdot u \in U \ \forall u \in U \Rightarrow A \cdot u \in U \ \forall u \in U \Rightarrow A \cdot U \subset U$ □

3.5.2 Lemma:

Sei K^n ein $K[x]$-Modul mittels A. Dann ist:

$$K[x]^n \xrightarrow{x \cdot \mathbb{1}_n - A} K[x]^n \longrightarrow K^n \longrightarrow 0$$

eine endliche Präsentation von K^n.

Beweis:

$e_1, ..., e_n \in K^n$ erzeugen K^n als $K[x]$-Modul, denn $\forall v \in K^n \ \exists \lambda_i \in K \subset K[x] : \ v = \lambda_1 e_1 + \cdots + \lambda_n e_n$

$$K[x]^n \overset{\pi}{\to} K^n$$
$$\begin{pmatrix} f_1(x) \\ \vdots \\ f_n(x) \end{pmatrix} \mapsto f_1(x) \cdot e_1 + \cdots + f_n(x) \cdot e_n = f_1(A) \cdot e_1 + \cdots + f_n(A) \cdot e_n$$

Behauptung:

$\mathrm{Kern}(\pi)$ wird von $x_j \cdot e_j - A \cdot e_j$ erzeugt. Dies folgt, da wir jeden Vektor $\begin{pmatrix} f_1(x) \\ \vdots \\ f_n(x) \end{pmatrix}$ durch ersetzen in einen Vektor $\begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix} K^n$ überführen können. Damit:

$$\begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix} = 0 \quad \Leftrightarrow \quad \begin{pmatrix} f_1(x) \\ \vdots \\ f_n(x) \end{pmatrix} \in \mathrm{Kern}(\pi) \quad \Leftrightarrow \quad \begin{pmatrix} f_1(x) \\ \vdots \\ f_n(x) \end{pmatrix} = \sum \lambda_j (x \cdot e_j - A \cdot e_j)$$

Damit gilt $\mathrm{Im}(x \cdot \mathbb{A}_n - A) = \mathrm{Kern}(\pi)$, die Sequenz ist also exakt und liefert eine endliche Präsentation. □

Beispiel:

Sei $n = 3$, $A = (a_{ij})$. Betrachte den Vektor

$$\begin{pmatrix} x^2 \\ 2x+1 \\ 2 \end{pmatrix} \in K[x]^3$$

Wir wollen ihn durch Ersetzungen $xe_j = Ae_j$ in einen Vektor in K^3 überführen. Dazu:

$$\begin{aligned}
x^2 \cdot e_1 + (2x+1) \cdot e_2 + 2 \cdot e_3 &= x \cdot (x \cdot e_1) + 2 \cdot (x \cdot e_2) + e_2 + 2 \cdot e_3 \\
&= x \cdot (a_{11}e_1 + a_{21}e_2 + a_{31}e_3) + 2(a_{12}e_1 + a_{22}e_2 + a_{32}e_3) + e_2 + 2e_3 \\
&= a_{11} \cdot (x \cdot e_1) + a_{21}(xe_2) + a_{31}(xe_3) + 2a_{12}e_1 + (2a_{22}+1)e_2 + (2a_{32}+2)e_3 \\
&= a_{11}(a_{11}e_1 + a_{21}e_2 + a_{31}e_3) + a_{21}(a_{12}e_1 + a_{22}e_2 + a_{31}e_3) + a_{31}(a_{13}e_1 + a_{23}e_2 + a_{33}e_3) \\
&\quad + 2a_{12}e_1 + (2a_{22}+1)e_2 + (2a_{32}+2)e_3 \\
&= (a_{11}^2 + a_{21}a_{12} + a_{31}a_{13} + 2a_{12})e_1 + (a_{11}a_{21} + a_{21}a_{22} + a_{31}a_{23} + 2a_{22} + 1)e_2 \\
&\quad + (a_{11}a_{31} + a_{21}a_{32} + a_{31}a_{33} + 2a_{32} + 2)e_3 \\
&= \begin{pmatrix} a_{11}^2 + a_{21}a_{12} + a_{31}a_{13} + 2a_{12} \\ a_{11}a_{21} + a_{21}a_{22} + a_{31}a_{23} + 2a_{22} + 1 \\ a_{11}a_{31} + a_{21}a_{32} + a_{31}a_{33} + 2a_{32} + 2 \end{pmatrix} \in K^3
\end{aligned}$$

3.5.3 Lemma:

Das $K[x]$-Modul K^n (mittels A) ist ein Torsionsmodul.

Beweis:

Nach dem Satz von Cayley-Hamilton gilt $\chi_A(A) = 0$ für das charakteristische Polynom $\chi_A = \det(x \cdot \mathbb{1}_n - A)$.

$\Rightarrow \chi_A \cdot v = \chi_A(A) \cdot v = 0 \cdot v = 0 \ \forall v \in V$
$\Rightarrow v$ ist Torsionselement $\forall v \in V$ □

Bemerkung:

Der Kern des Einsetzhomomorphismus

$$\begin{aligned} \varphi_A : \ K[x] &\to \mathrm{Mat}(n, K) \\ f &\mapsto f(A) \end{aligned}$$

ist ein Hauptideal, erzeugt vom Minimalpolynom p_A.

Es gilt auch $p_A \cdot v = 0 \ \forall v \in V$, $p_A \mid \chi_A$ folgt aus dem Satz von Cayley-Hamilton.

3.5.4 Lemma:

χ_A zerfalle in Linearfaktoren. Dann ist K^n als $K[x]$-Modul mittels A eine direkte Summe.
$K^n = U_1 \oplus \cdots \oplus U_k$ zyklischer Untermoduln U_i mit

$$U_i \cong {}^{K[x]}\!/_{\langle (x - \lambda_i)^{r_i} \rangle}$$

wobei $\chi_A = \prod_i (x - \lambda_i)^{r_i}$.

Beweis:

Bestimme die Smith-Normalform von $x \cdot \mathbb{1}_n - A$ 3.1.4,

$$D = \begin{pmatrix} d_1 & & \\ & \ddots & \\ & & d_n \end{pmatrix}$$

wobei $d_i \neq 0$ gelten muss, da K^n Torsionsmodul ist (Elementarteilersatz 3.4.4,3.4.5)

Wir zerlegen weiter mit dem chinesischen Restsatz (3.4.9) und erhalten

$$K^n = U_1 \oplus \cdots \oplus U_k$$

mit $U_i \cong {}^{K[x]}\!/_{\langle p_i^{r_i} \rangle}$ mit Primelementen $p_i \in K[x]$.

Es gilt:

$$\prod p_i^{r_i} = d_1 \cdots d_r = \det(D) = \det(x\mathbb{1}_n - A) = \chi_A$$

Da χ_A zerfällt, müssen die p_i von der Form $p_i = x - \lambda_i$ sein. □

3.5.5 Satz: Jordannormalform

Sei $A \in \mathrm{Mat}(n, K)$, χ_A zerfalle in Linearfaktoren über K. Dann $\exists$ Basis B bezüglich der A die Form

$$\begin{pmatrix} J(\lambda_1, r_1) & & \\ & \ddots & \\ & & J(\lambda_k, r_k) \end{pmatrix}$$

hat, wobei die $J(\lambda_1, r_i)$ Jordankästchen der Größe r_i sind,

$$J(\lambda_i, r_i) = \begin{pmatrix} \lambda_i & & & \\ 1 & \ddots & & \\ & \ddots & \ddots & \\ & & 1 & \lambda_i \end{pmatrix}$$

die λ_i nicht notwendiger verschieben. Bis auf Reihenfolge ist die Darstellung eindeutig.

Beweis:

Wir betrachten die Zerlegung $K^n = U_1 \oplus \cdots U_k$ aus Lemma 3.5.4 mit $U \overset{\varphi}{\cong} {K[x]}/{\langle (x-\lambda_i)^{r_i} \rangle}$.
Betrachte ${K[x]}/{\langle (x-\lambda_i)^{r_i} \rangle}$ als K-Vektorraum eine Basis ist $1, x-\lambda_i, (x-\lambda_i)^2, ..., (x-\lambda_i)^{r_i-1}$.
Die Bilder dieser Basis unter dem Isomorphismus φ_i nennen wir $v_{ij} \in U_i$, $j = 0, ..., r_i - 1$.

$$\begin{aligned} (A - \lambda_i \mathbb{1}_n) \cdot v_{ij} &= (x - \lambda_i) \cdot \varphi_i((x-\lambda_i)^j) \\ &= \varphi((x-\lambda_i)^{j+1}) \quad (\varphi_i \text{ ist } K[x]\text{-linear}) \\ &= \begin{cases} v_{i(j+1)} & j = 1, ..., r_i - 2 \\ 0 & j = r = r_i - 1 \end{cases} \end{aligned}$$

Man erhält

$$A \cdot v_{ij} = \begin{cases} \lambda_i \cdot v_{ij} + v_{ij+1} & j = 0, ..., r_i - 2 \\ 0 & \text{sonst} \end{cases}$$

Bezüglich der Basis $\{v_{ij}\}$ hat $A|_{U_i}$ also die Form

$$\begin{pmatrix} \lambda_i & & & \\ 1 & \ddots & & \\ & \ddots & \ddots & \\ & & 1 & \lambda_i \end{pmatrix}$$

und insgesamt hat A die gewünschte Form. $\square$

4 Körper und Konstruierbarkeit

Als bekannt vorausgesetzt:

- Definition Körper

Charakteristik

Die Charakteristik eines Körpers K, geschrieben $\text{char}(K)$, ist die kleinste Zahl $n \in \mathbb{N}_{>0}$ sodass

$$\underbrace{1+1+\cdots+1}_{n-\text{mal}} = 0$$

Falls keine solche Zahl existiert setze $\text{char}(K) = 0$.

4.1 Konstruierbarkeit

4.1.1 Definition: Körpererweiterung / Grad

Sei L ein Körper und $K \subset L$ mit den Verknüpfungen von L ein Körper, so ist K Unterkörper und $K \subset L$ eine Körpererweiterung, L ein Oberkörper.

L ist ein K-Vektorraum mit Skalarmultiplikation

$$\begin{aligned} K \times L &\to L \\ (k, l) &\mapsto kl \end{aligned}$$

Man nennt

$$[L : K] := \dim_K L$$

den Grad der Körpererweiterung.

Man schreibt L/K.

4.1.2 Beispiel:

1) $\mathbb{R} \subset \mathbb{C}$, $[\mathbb{C} : \mathbb{R}] = 2$
2) $\mathbb{Q} \subset \mathbb{R}$, $[\mathbb{R} : \mathbb{Q}] = \infty$
3) $\mathbb{Q}\left[\sqrt{2}\right] = \left\{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\right\}$

   $\mathbb{Q}\left[\sqrt{2}\right]$ ist das Bild des Einsetzhomomorphismus:

$$\begin{aligned} \varphi : \ \mathbb{Q}[x] &\to \mathbb{R} \\ x &\mapsto \sqrt{2} \end{aligned}$$

   Behauptung:

   $\text{Kern}(\varphi) = \langle x^2 - 2 \rangle$

   Angenommen $x^2 - 2$ wäre zerlegbar über $\mathbb{Q}$, dann existieren $a, b, c, d \in \mathbb{Q}$ mit

$$\begin{aligned} (x^2 - 2) &= (ax + b)(cx + d) \\ &= acx^2 + (ad + bc)x + bd \end{aligned}$$

Es folgt:

$\Rightarrow c = \frac{1}{a},\ d = \frac{-2}{b}$ und $\frac{-2a}{b} + \frac{b}{a} = 0$

$\Rightarrow \frac{-2a^2 + b^2}{ab} = 0$

$\Rightarrow -2a^2 + b^2 = 0$

$\Rightarrow 2a^2 = b^2$

$\Rightarrow 2 = \frac{b^2}{a^2}$

$\Rightarrow \sqrt{2} = \frac{b}{a} \in \mathbb{Q}$ ↯

$\Rightarrow x^2 - 2$ ist irreduzibel

$\Rightarrow \langle x^2 - 2 \rangle$ ist maximal

Es gilt $x^2 - 2 \in \text{Kern}(\varphi)$

$\Rightarrow \langle x^2 - 2 \rangle \subset \text{Kern}(\varphi)$

$\Rightarrow \langle x^2 - 2 \rangle = \text{Kern}(\varphi)$

$\Rightarrow {}^{\mathbb{Q}[x]}\!/_{\langle x^2 - 2 \rangle} \cong \mathbb{Q}\left[\sqrt{2}\right]$ ist ein Körper

$[\mathbb{Q} : \mathbb{Q}\left[\sqrt{2}\right]] = 2$ denn eine $\mathbb{Q}$-Basis von ${}^{\mathbb{Q}[x]}\!/_{\langle x^2 - 2 \rangle}$ ist $1,\ x - 2$. Die Tatsache, dass $\mathbb{Q}\left[\sqrt{2}\right]$ ein Körper ist, kann man auch direkt sehen: Die Ringstruktur wird von $\mathbb{Q}[x]$ geerbt, zu zeigen ist die Existenz von Inversen.

$$\frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{a^2 - 2b^2} = \frac{a}{a^2 - 2b^2} - \frac{b}{a^2 - 2b^2}\sqrt{2} \in \mathbb{Q}\left[\sqrt{2}\right]$$

denn $a^2 - 2b^2 \neq 0$, da $\sqrt{2}$ irrational.

4.1.3 Turmsatz

Seien $K \subset L \subset M$ Körpererweiterungen (L ist Zwischenkörper). Dann gilt:

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

Beweis:

Sei $\{v_i\}$ eine L-Vektorraumbasis von M, $\{w_j\}$ ein K-Vektorraumbasis von L.

Sei $m \in M \ \Rightarrow m = \sum l_i v_i,\ l_i \in L$.

Für $l_i \in L$ gilt $l_i = \sum k_{ij} w_j$ mit $k_{ij} \in K \ \Rightarrow \ m = \sum_{i,j} k_{ij} w_j v_i$

$\Rightarrow$ Die $\{w_j v_i\}$ erzeugen M als K-Vektorraum.

$$\begin{aligned}
\sum k_{ij} w_j v_i = 0 \ &\Rightarrow \ \sum_i \left(\sum_j k_{ij} w_j \right) v_i = 0 \\
&\Rightarrow \ \sum_j k_{ij} w_j = 0 \ \forall i \\
&\Rightarrow \ k_{ij} = 0 \ \forall i, j \\
&\Rightarrow \ \{w_j v_i\} \text{ linear unabhängig}
\end{aligned}$$

$\{w_j v_i\}$ ist also eine Basis.

$$|\{w_j v_i\}| = |\{v_i\}| \cdot |\{w_j\}| \ \Rightarrow \ [M : K] = [M : L] \cdot [L : K]$$

□

4.1.4 Korollar:

Ist $[L : K]$ eine Primzahl, so hat $K \subset L$ keine echten Zwischenkörper.

Beweis: Turmsatz.

Bemerkung:

- $K \subset L \Rightarrow \text{char}(K) = \text{char}(L)$, denn $1_K = 1_L$

- Ist $|K| < \infty \Rightarrow \text{char}(K)$ prim.
- Ist $\text{char}(K) = 0 \Rightarrow |K| = \infty$
- Es gibt unendlich viele Körper der Charakteristik p, z.B. Quot $(\mathbb{Z}_p[x])$.

4.1.5 Definition: Primkörper

$$K \text{ heißt } \underline{\text{Primkörper}} \Leftrightarrow K \text{ besitzt keine echten Unterkörper}$$

Sei K ein Körper

$$P(K) := \bigcap_{\substack{U \subset K \\ U \text{ Unterkörper}}} U$$

ist $\underline{\text{Primkörper von } K}$

4.1.6 Satz:

$$\text{char}(K) = 0 \Leftrightarrow P(K) \cong \mathbb{Q}$$
$$\text{char}(K) = p \Leftrightarrow P(K) \cong \mathbb{Z}_p$$

Beweis:

$\mathbb{Q}$ ist ein Primkörper, $\mathbb{Z}_p$ auch. Die charakte ristische Abbildung:

$$\mathbb{Z} \to K$$
$$n \mapsto n \cdot 1_k$$

liefert uns diese als Unterkörper von K. □

4.1.7 Lemma:

Sei $K \subset L$, $\alpha_1, .., \alpha_n \in L$, der Einsetzhomomorphismus:

$$\varphi : \ K[x_1, ..., x_n] \to L$$
$$x_i \mapsto \alpha_i$$

mit $\text{Im}(\varphi) =: K[\alpha_1, ..., \alpha_n]$. $K[\alpha_1, ..., \alpha_n]$ ist der Durchschnitt aller Unterringe von L, die K und die α_i enthalten.

Beweis:

$K[\alpha_1, ..., \alpha_n]$ ist in jedem Unterring von L, der K und α_i enthält, enthalten, außerdem ist er selbst ein solcher Unterring. □

4.1.8 Definition:

Sei $K \subset L$, $\alpha_1, ..., \alpha_n \in L$

$$K(\alpha_1, ..., \alpha_n) := \bigcap_{\substack{U \subset L \text{ Unterkörper} \\ K \subset U \\ \alpha_1, ..., \alpha_n \in U}} U$$

der kleinste Körper, der K und α_i enthält.

4.1.9 Lemma:

$$K(\alpha_1, ..., \alpha_n) = \text{Quot}\,(K[\alpha_1, ..., \alpha_n])$$

Beweis:

$K[\alpha_1, ..., \alpha_n]$ ist Unterring von L und daher nullteilerfrei. Die Inklusion

$$K[\alpha_1, ..., \alpha_n] \hookrightarrow K(\alpha_1, ..., \alpha)$$

können wir auf Quot $(K[\alpha_1, ..., \alpha_n])$ fortsetzen und erhalten

$$\text{Quot}(K[\alpha_1, ..., \alpha_n]) \subset K(\alpha_1, ..., \alpha_n)$$

Andererseits ist Quot $(K[\alpha_1, ..., \alpha_n])$ ein Unterkörper, der K und α_i enthält, also gilt auch

$$K(\alpha_1, ..., \alpha_n) \subset \text{Quot}(K[\alpha_1, ..., \alpha_n])$$

□

4.1.10 Satz:

Sei $K \subset L$ und $\alpha \in L$. Dann sind äquivalent:

1) $\exists g \in K[x] \backslash \{0\}$ mit $g(\alpha) = 0$
2) Kern $(\varphi_\alpha : \ K[x] \to K[\alpha] : \ x \mapsto \alpha) \neq \{0\}$
3) $K[\alpha] = K(\alpha)$
4) $K[\alpha]$ ist Körper

Falls $1) - 4)$ gilt, folgt dass der normierte Erzeuger von Kern(φ_α), m_α, irreduzibel ist.
Außerdem gilt $[K[\alpha] : K] = \deg(m_\alpha)$, $\{1, \alpha, ..., \alpha^{\deg(m_\alpha)-1}\}$ ist eine K-Vektorraumbasis von $K[\alpha]$.

4.1.11 Definition:

- m_α heißt das Minimalpolynom von α
- $\deg(m_\alpha)$ der Grad von α
- α heißt algebraisch$/_K$
- Elemente $\alpha \in L$, die nicht algebraisch$/_K$ sind, heißen transzendent$/_K$

Beweis: von 4.1.10

1) $\Rightarrow$ 2) : $g \in \mathrm{Kern}(\varphi_\alpha)$
2) $\Rightarrow$ 1) : $\exists g \neq 0,\ g \in \mathrm{Kern}(\varphi_\alpha),$ mit $g(\alpha) = 0$

Behauptung:

Falls 2) gilt, so ist m_α irreduzibel.

Sei $m_\alpha = g_1 \cdot g_2$ $\Rightarrow 0 = m_\alpha(\alpha) = g_1(\alpha) \cdot g_2(\alpha) \in L$
$\Rightarrow$ Ohne Einschränkung: $g_1(\alpha) = 0$
$\Rightarrow g_1 \in \mathrm{Kern}(\varphi_\alpha) = \langle m_\alpha \rangle$
$\Rightarrow m_\alpha \mid g_1$
$\Rightarrow \exists\, h :\ h \cdot m_\alpha = g_1$
$\Rightarrow m_\alpha = h \cdot m_\alpha \cdot g_2$
$\Rightarrow h \cdot g_2 = 1$
$\Rightarrow g_2$ ist Einheit

Wir Vervollständigen den Beweis:

2) $\Rightarrow$ 4) $K[\alpha] = \mathrm{Im}(\varphi_\alpha) \cong K[x]/\mathrm{Ker}(\varphi_\alpha) = K[x]/\langle m_\alpha \rangle$
und $\langle m_\alpha \rangle$ ist maximal, da m_α irreduzibel
$\Rightarrow K[x]/\langle m_\alpha \rangle$ ist Körper
$\Rightarrow K[\alpha]$ ist Körper

4) $\Rightarrow$ 2) Sei $\mathrm{Ker}(\varphi_\alpha) = \{0\}$
$\Rightarrow K[\alpha] = \mathrm{Im}(\varphi_\alpha) = K[x]/\mathrm{Ker}(\varphi_\alpha) = K[x]/\{0\}$
ist kein Körper

4) $\Rightarrow$ 3) nach Definiton

3) $\Rightarrow$ 4) klar

In $K[x]/\langle m_\alpha \rangle$ bilden die Klassen von $1, x, x^2, ..., x^{\deg(m_\alpha)-1}$ eine K-Vektorraumbasis, also entsprechend $1, \alpha, ..., \alpha^{\deg(\alpha)-1}$ in $K[\alpha]$. □

4.1.12 Beispiel:

1) $\sqrt{2} \in \mathbb{R}$ ist algebraisch$/_{\mathbb{Q}}$
2) $i \in \mathbb{C}$ ist algebraisch$/_{\mathbb{R}}$, $\deg(i) = 2$
3) π ist transzendent über $\mathbb{Q}$. (ohne Beweis)

4.1.13 Definition:

$$K \subset L \text{ heißt algebraisch } \Leftrightarrow \forall \alpha \in L :\ \alpha \text{ ist algebraisch}/_K$$

Falls $K \subset L$ nicht algebraisch, so heißt $K \subset L$ transzendent.

Beispiel:

$K \subset K(x) = \mathrm{Quot}\,(K[x])$ ist transzendent, denn die Potenzen von x erfüllen keine K-lineare Relation.

4.1.14 Satz:

Sei $K \subset L$. Dann sind äquivalent:

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

2) $K \subset L$ ist algebraisch und $\exists\ \alpha_1, .., \alpha_n \in L :\ K(\alpha_1, ..., \alpha_n) = L$

3) $\exists\ \alpha_1, ..., \alpha_n \in L$ algebraisch mit $L = K(\alpha_1, ..., \alpha_n)$

4.1.15 Definition:

Eine Körpererweiterung, die 4.1.14 $1) - 3)$ erfüllt, heißt endlich.

Insbesondere gilt: Endliche Körpererweiterungen sind algebraisch.

Beweis: von 4.1.14

$1) \Rightarrow 2)$ Sei $[L : K] = n,\ \alpha \in L$

$\Rightarrow\ 1, \alpha, ..., \alpha^n$ sind linear abhängig$/_K$

$\Rightarrow\ \exists\ \lambda_i \in K :\ \sum_{i=0}^{n} \lambda_i \alpha^i = 0$

Setze $g = \sum_{i=0}^{n} \lambda_i x^i,$ dann gilt $g(\alpha) = 0\ \Rightarrow\ \alpha$ ist algebraisch

Sei $\alpha_1, ..., \alpha_n$ eine K-Vektorraumbasis von L, dann ist $K(\alpha_1, ..., \alpha_n) \subset L$

und per Definition: $L \subset K(\alpha_1, ..., \alpha_n)$ da $l \in L$ sich schreiben lässt als $\sum \lambda_i \alpha_i = l$ mit $\lambda_i \in K$

$\Rightarrow\ L = K(\alpha_1, ..., \alpha_n)$

$2) \Rightarrow 3)$ klar

$3) \Rightarrow 1)$ $[L : K] = [K(\alpha_1, ..., \alpha_n) : K] \overset{4.1.3}{=} [K(\alpha_1, ..., \alpha_n) : K(\alpha_1, ..., \alpha_{n-1})] \cdot\ \cdots\ \cdot [K(\alpha_1) : K]$

und jeder Faktor ist $< \infty,$ da jedes α_i algebraisch$/_K$ ist. □

4.1.16 Lemma:

Ist $K \subset L$, $N \subset L$ eine Teilmenge von Elementen, die algebraisch über K sind, so ist $K(N) = K[N]$ und die Körpererweiterung $K(N)/_K$ ist algebraisch.

(Der Fall: $|N| < \infty$ folgt aus 4.1.10 per Induktion)

Beweis:

Wr zeigen, dass $K[N]$ ein Körper ist. Dazu müssen wir ein Inverses für jedes $g \in K[N]$, $g \neq 0$ finden.

g ist ein Polynom in endlich vielen $\alpha_1, ..., \alpha_n \in N$ mit Koeffizienten in K, und die α_i sind algebraisch$/_K$.

$\Rightarrow g \in K[\alpha_1, ..., \alpha_n] = K(\alpha_1, ..., \alpha_n)$

$\Rightarrow \exists\ g^{-1} \in K[\alpha_1, ..., \alpha_n] \subset K[N]$

Da $K(\alpha_1, ..., \alpha_n)$ algebraisch ist, ist g algebraisch$/_K$ und damit $K[N]$ algebraisch$/_K$. □

4.2 Zerfällungskörper und algebraischer Abschluß

4.2.1 Satz: Kronecker

Sei K ein Körper, $f \in K[x]$, $f = g \cdot h$, g irreduzibel, $L = {}^{K[x]}\!/_{\langle g \rangle}$.

Dann hat f in L eine Nullstelle α (es existiert also ein $\alpha \in L$ sodass $f(\alpha) = 0$), mit

$$\alpha = [x] = x + \langle g \rangle \in L, L \cong K[\alpha]$$

Beweis:

$$f(\alpha) = f([x]) = [f(x)] \in L = {}^{K[x]}\!/_{\langle g \rangle}$$
$$[f(x)] = [g \cdot h] = [g] \cdot [h] = 0 \quad (\text{da } g = 0)$$

Das Minimalpolynom von α teilt g, da beide irreduzibel sind, sind sie bis auf konstanten Faktor gleich und damit $L \cong K[\alpha]$. □

4.2.2 Korollar:

Sei K ein Körper, $f \in K[x]$, $d = \deg(f) > 0$

1) $\exists\ K \subset L$, so dass ${}^{f}\!/_{L}$ in Linearfaktoren zerfällt. (Das bedeutet $\exists c, a_1, \ldots, a_n \in L : f = c(x - a_1) \cdots (x - a_n)$).
2) Sind $\alpha_1, ..., \alpha_d \in L$ Nullstellen von f, dann ist $K[\alpha_1, ..., \alpha_d]$ der kleinste solche Körper.
3) K [Nullstellen] ist bis auf Isomorphie eindeutig und heißt Zerfällungskörper von f.

Beweis:

1) Satz von Kronecker 4.2.1 und Induktion.
2) Seien $\alpha_1, ..., \alpha_d \in L$ Nullstellen

   $\Rightarrow f = c(x - \alpha_1) \cdots (x - \alpha_d) \in K[\alpha_1, ..., \alpha_d][x]$

   Nach Definition ist $K(\alpha_1, ..., \alpha_n)$ der kleinste Körper, der K und die α_i enthält.

   Wegen 4.1.10 (mit Induktion) gilt $K[\alpha_1, ..., \alpha_n] = K(\alpha_1, ..., \alpha_n)$ da jedes α_i als Nullstelle eines Polynoms in $K[x]$ per Definition algebraisch ist.
3) f zerfalle über $L' \supset K$, das heißt, in L' hat f d Nullstellen $\alpha'_1, ..., \alpha'_d$.

   Dann ist wegen 2) $K[\alpha'_1, ..., \alpha'_d]$ ein Körper (der kleinste in L', über dem f zerfällt).

   Zu zeigen: $K[\alpha'_1, ..., \alpha'_d] \cong K[\alpha_1, ..., \alpha_d]$.

   Sei $f = g \cdot h,\ g, h \in K[x]$, g irreduzibel und normiert, dann hat wegen des Satzes von Kronecker 4.2.1 f eine Nullstelle α_1 in ${}^{K[x]}\!/_{\langle g \rangle} \cong K[\alpha_1]$.

   Als Faktor von f zerfällt auch g über L' in Linearfaktoren und die Nullstellen von g in L' sind auch Nullstellen von f in L'.

   $\Rightarrow$ Ohne Einschränkung α'_1 ist eine Nullstelle von g in L'.

   Das Minimalpolynom von α'_1 über K ist, da $g(\alpha'_1) = 0$, ein Faktor von g und da g irreduzibel und normiert, gleich g.

   $\Rightarrow K[\alpha'_1] \cong {}^{K[x]}\!/_{\langle g \rangle} \cong K[\alpha_1]$

   f hat in $K[\alpha_1][x]$ und $K[\alpha'_1][x]$ den Linearfaktor $(x - \alpha_1)$ bzw. $(x - \alpha'_1)$, $f = (x - \alpha_1) \cdot f_1$, $f = (x - \alpha'_1) \cdot f'_1$.

   Der Isomorphismus $K[\alpha_1] \cong K[\alpha'_1]$ induziert einen Ringhomomorphismus

   $$K[\alpha_1][x] \overset{\cong}{\to} K[\alpha'_1][x]$$

   der f festhält (da der Isomorphismus $K[\alpha_1] \cong K[\alpha'_1]$ K festhält).

   Da außerdem $x - \alpha_1 \mapsto x - \alpha'_1$ muss auch f_1 auf f'_1 überführt werden.

   Wir führen Induktion über den Grad von f und können daher per Induktionsvorraussetzung annehmen, dass der Zerfällungskörper von $f_1 \in K[\alpha_1][x]$ (bzw. $f'_1 \in K[\alpha'_1][x]$) eindeutig ist, damit ist auch der Zerfällungskörper von f eindeutig. □

4.2.3 Korollar:

Sei $f \in K[x]$, $deg_K f = d$, der Zerfällungskörper L von f hat höchstens Grad

$$[L : K] \leq d!$$

über K.

Beweis:

Folgt durch sukzessives Adjungieren von Nullstellen aus 4.1.10 und 4.2.1. □

Beispiel:

1) Der Zerfällungskörper von $x^2 + 1 \in \mathbb{R}[x]$ ist $\mathbb{C}$

2) Sei $f = x^d - 1 \in \mathbb{Q}[x]$. Über $\mathbb{C}$ zerfällt f, die Nullstellen sind

$$\alpha_j = e^{\frac{2\pi i}{d} \cdot j} \quad j = 0, ..., d-1$$

die d-ten Einheitswurzeln. Die $\{a_j\} \subset \mathbb{C}^*$ sind eine zyklische Untergruppe, erzeugt von beliebigen α_j mit $\text{ggT}(j, d) = 1$, z.B. von α_1.

Daher ist der Zerfällungskörper von f gleich

$$\mathbb{Q}[\alpha_1, ..., \alpha_{d-1}] = \mathbb{Q}[\alpha_j] \ \ \forall\, j$$

mit $\text{ggT}(j, d) = 1$.

3) Sei $f = x^3 - 2 \in \mathbb{Q}[x]$. $\mathbb{Q}\left[\sqrt[3]{2}\right]$ ist nicht der Zerfällungskörper von f, denn die Nullstellen von f in $\mathbb{C}$ sind

$$\alpha_1 = \sqrt[3]{2},\ \alpha_2 = \sqrt[3]{2} \cdot e^{\frac{2\pi i}{3}},\ \alpha_3 = \sqrt[3]{2} \cdot e^{\frac{4\pi i}{3}}$$

Der Zerfällungskörper ist $\mathbb{Q}[\alpha_1, \alpha_2, \alpha_3]$ ($\neq \mathbb{Q}[\alpha_i]$ für jedes i).

Bemerkung:

Für ein Polynom $x^d - n$ sind die Nullstellen von der Form $\sqrt[d]{n} \cdot e^{\frac{2\pi i}{d} \cdot j}$ mit $j = 0, 1, \ldots, d-1$

4.2.4 Lemma:

Sei K ein Körper. Dann sind äquivalent:

1) $\forall\, f \in K[x]$, $\deg(f) \geq 1$ gilt: f hat eine Nullstelle in K.

2) $f \in K[x]$ ist irreduzibel $\Leftrightarrow \deg(f) = 1$

3) $\forall\, K \subset L$ algebraisch $\Rightarrow K = L$

4.2.5 Definition: Algebraisch abgeschlossen

Ein K, dass 4.2.4 1)-3) erfüllt, heißt algebraisch abgeschlossen.

Beweis: von 4.2.4

1) $\Rightarrow$ 2) „$\Rightarrow$ “
   Sei $\deg(f) > 1$, wegen 1) hat f eine Nullstelle α in K, der Linearfaktor $(x - \alpha)$ spaltet ab
   $\Rightarrow$ f ist nicht irreduzibel
   „$\Leftarrow$ “
   Sei $\deg(f) = 1$, $f = g \cdot h$
   $\Rightarrow$ Ohne Einschränkung $\deg(g) = 1$, $\deg(h) = 0$ $\Rightarrow$ h Einheit $\Rightarrow$ f irreduzibel

2) $\Rightarrow$ 3) Sei $K \subset L$ algebraisch, $\alpha \in L$.
   Das Minimalpolynom m_α ist irreduzibel 4.1.10 $\Rightarrow$ $\deg(m_\alpha) = 1$ $\Rightarrow$ $m_\alpha = x - \alpha$
   Da $m_\alpha \in K[x]$ folgt $\alpha \in K$ $\Rightarrow$ $L \subset K$ $\Rightarrow$ $K = L$

3) $\Rightarrow$ 1) Wegen des Satzes von Kronecker 4.2.1 gibt es für jedes $f \in K[x]$ mit $\deg(f) \geq 1$ eine Nullstelle in
   $L = K[\alpha] \cong {}^{K[x]}\!/_{\langle g \rangle}$
   (wobei g ein irreduzibler Faktor von f ist), und $K \subset L$ ist algebraisch
   $\Rightarrow$ $K = L$ $\Rightarrow$ $\alpha \in K$ $\Rightarrow$ f hat eine Nullstelle in K. □

Beispiel:

$\mathbb{Q}$, $\mathbb{R}$ sind nicht algebraisch abgeschlossen, da $x^2 + 1$ keine Nullstelle hat.

4.2.6 Fundamentalsatz der Algebra

$\mathbb{C}$ ist algebraisch abgeschlossen.

Beweis: in Funktionentheorie, bzw. später

Für K wollen wir die Existenz des algebraischen Abschluss $\overline{K}$ zeigen. Zur Vorbereitung:

4.2.7 Lemma: Zornsches Lemma

Sei $(M, \leq)$, $M \neq \varnothing$, partiell geordnet. Besitzt jede Kette in M eine obere Schranke, so besitzt M ein maximales Element.

Das Zornsche Lemma ist äquivalent zum Auswahlaxiom und zum Wohlordnungssatz (Lineare Algebra).

4.2.8 Proposition:

Sei R ein Ring und $I \subsetneq R$ ein Ideal. Dann $\exists$ maximales Ideal m mit $I \subset m \subsetneq R$

Beweis:

Sei $M = \{J \subsetneq R \text{ Ideal}, \ I \subset J\}$, $M \neq \varnothing$, da $I \in M$. M ist bezüglich $\subset$ partiell geordnet. Sei K eine nicht-leere Kette in M, setze $S = \bigcup_{J \in K} J$

Behauptung: $S \in M$

Da die Kette nicht-leer ist, gibt es $J \in K$ und $I \subset J \subset S$. Seien $x, x' \in S$, $r \in R$. Dann $\exists J, J' \in K$ mit $x \in J$, $x' \in J'$, ohne Einschränkung $J \subset J'$, da K total geordnet.

$\Rightarrow x + x' \in J' \subset S$. Außerdem $r \cdot x \in J \subset S$

$\Rightarrow S$ ist ein Ideal.

Wäre $S = R$, so gäbe es ein $J \in K$ mit $1 \in J$ $\lightning$

$\Rightarrow \ S \subsetneq R \ \Rightarrow \ S \in M$.

Damit besitzt K eine obere Schranke. $S \in M \ \Rightarrow \ M$ besitzt ein maximales Element m.

Es gilt $I \subset m$, da $m \in M$. Wäre m kein maximales Ideal, so gäbe es ein Element in M echt größer m $\lightning$ zur Maximalität von m in M

$\Rightarrow \ m$ ist ein maximales Ideal, das I enthält. $\square$

4.2.9 Proposition: Artin

Sei K ein Körper. Dann $\exists$ algebraische Körpererweiterung $L \supset K$, so dass jedes nicht-konstante Polynom $f \in K[x]$ eine Nullstelle in L hat.

Beweis:

Sei $\Lambda = {}^{K[x]}\!/_{K}$ die Menge aller nicht-konstanten Polynome. Betrachte

$$R = K[x_f \mid f \in \Lambda]$$

den Polynomring mit Variablen für jedes $f \in \Lambda$. Betrachte:

$$I = \langle f(x_f) \mid f \in \Lambda \rangle \subset R$$

$f(x_f)$ entsteht aus $f(x) \in \Lambda$, indem wir die Variable umbenennen als x_f.

Die Erzeuger von I hängen also von verschiedenen Variablen ab. Angenommen, $I = R$. Dann $\exists \ f_1, ..., f_k \in \Lambda$, $g_1, ..., g_k \in R$:

$$\Lambda = \sum_{i=1}^{k} g_i f_i(x_{f_i}) \quad (*)$$

Im Zerfällungskörper L' von $f = f_1 \cdots f_k \in K[x]$ wählen wir für jedes f_i eine Nullstelle α_i.

Wir wenden den Einsetzhomomorphismus

$$\begin{aligned}\varphi:\ R &\to\ L'\\ x_{f_i} &\mapsto \alpha_i\\ x_f &\mapsto 0\ \ f \neq f_i\end{aligned}$$

auf $(*)$ an und erhalten

$$\Lambda = \sum_{i=1}^{k} \varphi(g_i) f_i(\varphi(x_{f_i})) = \sum_{i=1}^{k} \varphi(g_i) f_i(\alpha_i) = \sum_{i=1}^{k} \varphi(g_i) \cdot 0 = 0 \quad \lightning$$

$\Rightarrow I \subsetneq R$. Wegen 4.2.8 $\exists$ ein maximales Ideal $I \subset m \subsetneq R$. Setze $L = {}^{R}\!/_{m}$, dann ist L ein Körper mit $K \subset L$.

Für $f \in {}^{K[x]}\!/_{K}$ $\exists$ eine Nullstelle in L, da $f(x_f) \in I \subset m \ \Rightarrow\ [f(x_f)] = [0] \ \Rightarrow\ f([x_f]) = 0 \ \Rightarrow\ [x_f]$ ist Nullstelle.

Noch zu zeigen: L ist algebraisch.

Da $f([x_f]) = 0$ ist $[x_f]$ algebraisch. Aus 4.1.16 folgt dann, dass $L = {}^{K[x_f]}\!/_{m} = K[[x_f]]$ algebraisch ist. □

4.2.10 Satz:

Jeder Körper besitzt einen algebraischen Abschluss $\overline{K}$.

Beweis:

Setze $K_0 = K$ und konstruiere mit 4.2.9 $K_0 \subset K_1$, so dass jedes Polynom in ${}^{K_0[x]}\!/_{K_0}$ in K_1 eine Nullstelle hat.

Konstruiere rekursiv:

$$K_0 \subset K_1 \subset K_2 \subset \cdots$$

und setze $\overline{K} := \bigcup_{i=0}^{\infty} K_i$.

Behauptung: $\overline{K}$ ist der algebraische Abschluss von K.

Sei $\alpha, \beta, \gamma \in \overline{K}$, dann $\exists\ K_i$ mit $\alpha, \beta, \gamma \in K_i$, da die K_i eine Kette bilden.

Die Körperaxiome für α, β, γ ($(\alpha+\beta)\gamma = \alpha\gamma + \beta\gamma$ usw.) gelten also, da sie in K_i gelten.

$\Rightarrow \overline{K}$ ist ein Körper, es gilt $K \subset \overline{K}$.

Ist $\alpha \in \overline{K}$ $\exists\ K_i:\ \alpha \in K_i \ \Rightarrow\ \alpha$ algebraisch ${}/_{K}$ $\Rightarrow$ $\overline{K}$ algebraisch ${}/_{K}$

Sei $f \in {}^{\overline{K}[x]}\!/_{\overline{K}}$.

f hat endlich viele Koeffizienten $\Rightarrow \exists\ K_i:\ f \in {}^{K_i[x]}\!/_{K_i}$ Dann hat f nach Konstruktion eine Nullstelle in $K_{i+1} \subset \overline{K}$.

$\Rightarrow \overline{K}$ ist algebraisch abgeschlossen. □

4.3 Konstruktion mit Zirkel und Lineal

4.3.1 Definition:

Wir identifizieren $\mathbb{R}^2 \cong \mathbb{C}$.

$k(a, r)$ bezeichne den Kreis um a mit Radius r. $a \in \mathbb{C},\ r \in \mathbb{R}$
$g(p, q)$ bezeichne die Gerade durch p und $q \in \mathbb{C}$

4.3.2 Definition: Konstruierbare Punkte

Sei $M \subset \mathbb{C}$, $0, 1 \in M$.

$G(M) :=$ Menge aller Geraden durch 2 Punkte von M
$K(M) :=$ Menge der Kreise mit Mittelpunkt aus M und Radius := Entfernung zweier Punkte von M
$A(M) :=$ Menge der Schnittpunkte zweier Geraden
$= \{z \in \mathbb{C} \mid \exists\ g_1, g_2 \in G(M),\ g_1 \neq g_2,\ z \in g_1 \cap g_2\}$
$B(M) :=$ Menge der Schnittpunkte einer Geraden mit einem Kreis
$= \{z \in \mathbb{C} \mid \exists\ g \in G(M),\ k \in K(M),\ z \in g \cap k\}$
$C(M) :=$ Menge der Schnittpunkte zweier Kreise
$= \{z \in \mathbb{C} \mid \exists\ k_1, k_2 \in K(M),\ k_1 \neq k_2,\ z \in k_1 \cap k_2\}$

Wir definieren weiter:

$$M' = A(M) \cup B(M) \cup C(M)$$

und rekursiv:

$$M_0 := M,\ M_1 = M',\ M_2 = M_1', \cdots$$

Wobei

$$M_0 \subset M_1 \subset \ldots$$

Man definiert

$$\tilde{M} = \bigcup_{n \geq 0} M_n$$

$\tilde{M}$ ist die Menge der aus M konstruierbaren Punkte.

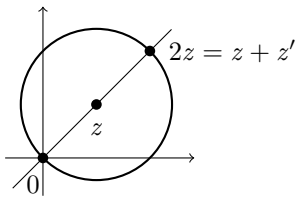
4.3.3 Satz:

$\tilde{M}$ ist ein Unterkörper von $\mathbb{C}$.

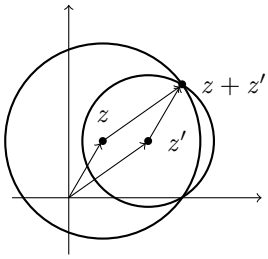
Beweis:

Behauptung: $(\tilde{M}, +)$ ist eine Untergruppe von $(\mathbb{C}, +)$.

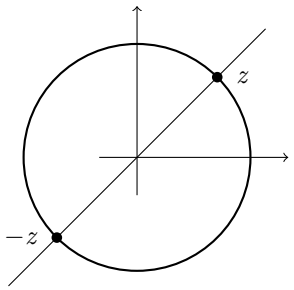
$\tilde{M} \neq \varnothing$. Seien $z, z' \in \tilde{M}$. Falls $z = z' \ \Rightarrow\ z + z' \in k(z, |z|) \cap g(0, z) \subset \tilde{M}$



Falls $z \neq z' \quad \Rightarrow \quad z + z' \in k(z, |z'|) \cap k(z', |z|) \subset \tilde{M}$



$-z \in k(0, |z|) \cap g(0, z) \subset \tilde{M}$



Behauptung: $(\tilde{M}\backslash\{0\}, \cdot)$ ist Untergruppe von $(\mathbb{C}\backslash\{0\}, \cdot)$

Dazu:

1) $z, z' \in \tilde{M}\backslash\{0\} \cap \mathbb{R}_{>0} \;\Rightarrow\; zz' \in \tilde{M}\backslash\{0\}$
2) $z \in \tilde{M}\backslash\{0\} \cap \mathbb{R}_{>0} \;\Rightarrow\; \frac{1}{z} \in \tilde{M}\backslash\{0\}$
3) $z \in \tilde{M}\backslash\{0\} \cap \mathbb{R}_{>0} \;\Rightarrow\; i \cdot z \in \tilde{M}\backslash\{0\}$
4) $z \in \tilde{M}\backslash\{0\} \;\Rightarrow\; |z|, \overline{z}, \mathrm{Re}(z), \mathrm{Im}(z) \in \tilde{M}$
5) $\lambda \in \mathbb{R}_{>0},\; z \in \tilde{M}\backslash\{0\} \;\Rightarrow\; \lambda z \in \tilde{M}\backslash\{0\}$

Dann folgt:

- $\tilde{M}\backslash\{0\}$

  Gilt, da $1 \in \tilde{M}\backslash\{0\}$

- $z \cdot z' \in \tilde{M}\backslash\{0\}$

  Sei $z, z' \in \tilde{M}\backslash\{0\}$ beliebig:

  $z \cdot z' = \mathrm{Re}(z) \cdot \mathrm{Re}(z') - \mathrm{Im}(z) \cdot \mathrm{Im}(z') + i$
  $(\mathrm{Im}(z') \cdot \mathrm{Re}(z) + \mathrm{Re}(z') \cdot \mathrm{Im}(z)$

  Da Produkte aus $|\mathrm{Re}(z)|$, $|\mathrm{Re}(z')|$, $|\mathrm{Im}(z)|$, $|\mathrm{Im}(z')|$ wegen 1) in $\tilde{M}\backslash\{0\}$ sind und Negative da $(\tilde{M}, +)$ Untergruppe von $(\mathbb{C}, +)$ ist, und ein Produkt von o mit einer Zahl aus $\tilde{M}\backslash\{0\}$ in $\tilde{M}\backslash\{0\}$ ist wegen 3) folgt $z \cdot z' \in \tilde{M}\backslash\{0\}$.

- $\frac{1}{z} \in \tilde{M}\backslash\{0\}$

  $$\frac{1}{z} = \frac{1}{|z|^2} \cdot \overline{z} \in \tilde{M}\backslash\{0\}$$

  denn $\frac{1}{|z|} \in \tilde{M}\backslash\{0\}$ wegen 2)

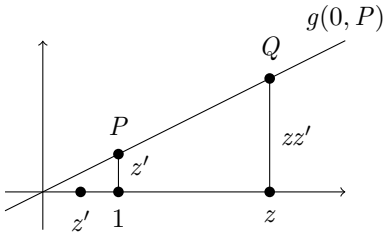
  $\frac{1}{|z|} \cdot \frac{1}{|z|}$ wegen 1)

  $\overline{z} \in \tilde{M}\backslash\{0\}$ wegen 4)

  und reelles Vielfaches einer Zahl in $\tilde{M}\backslash\{0\}$ wegen 5). □

1) • Lot fällen auf 1, z' abtragen liefert P
• Lot fällen auf z
• Schnittpunkt von $g(0,P)$ mit Lot auf z sei Q

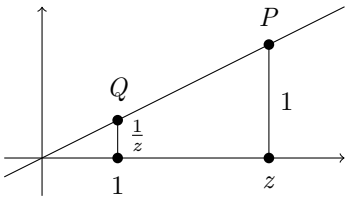
Dann gilt $|zQ| = zz'$ wegen Strahlensatz.



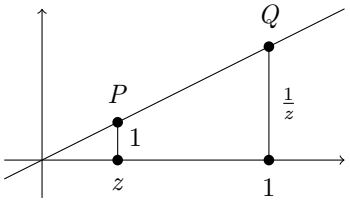
2) • Lot fällen auf z, 1 abtragen liefert P
• Lot fällen auf 1
• Schnittpunkt von $g(0,P)$ mit Lot auf 1 liefert Q.

Dann gilt $|1Q| = \frac{1}{z}'$ wegen Strahlensatz.

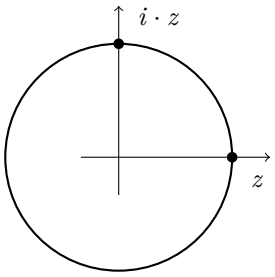
Falls $z > 1$



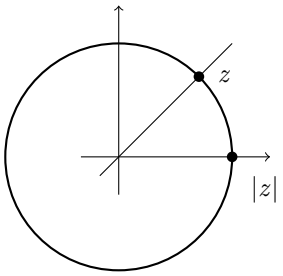
Falls $z < 1$



3) • $i \cdot z \in g(0,i) \cap k(0,|z|) \subset \tilde{M} \backslash \{0\}$



4) • $|z| \in k(0,|z|) \cap g(0,1) \in \tilde{M}\backslash\{0\}$
• $\mathrm{Re}(z)$ = Lot von z auf $g(0,1)$
• $\mathrm{Im}(z)$ = Lot von z auf $g(0,i)$
($i \in \tilde{M}\backslash\{0\}$ wegen 3))
• $\overline{z}$ = Spiegelung von z an $g(0,1)$



5) • $|\lambda \cdot z| = \lambda \cdot |z| \in \tilde{M}\backslash\{0\}$ wegen 1), 4)
• $\lambda \cdot z \in k(0, \lambda \cdot |z|) \cap g(0,z)$

□

Bemerkung: $\mathbb{Q} \subset \tilde{M}$, da man über die Strahlensätze jedes bekommt.

4.3.4 Definition:

1) Eine Körpererweiterung $K \subset L$ heißt quadratisch abgeschlossen in L
$:\Leftrightarrow \forall\ \alpha \in L$ mit $\alpha^2 \in K$ gilt $\alpha \in K$

2) $K \subset L$ heißt Quadratwurzelerweiterung
$:\Leftrightarrow \exists\ \alpha_1, ..., \alpha_n \in L$ mit $L = K(\alpha_1, ..., \alpha_n)$, $\alpha_i^2 \in K(\alpha_1, ..., \alpha_{i-1})$, $\alpha_i \notin K(\alpha_1, ..., \alpha_{i-1})$

Bemerkung:

Der Grad einer Quadratwurzelerweiterung ist eine Zweierpotenz.

Beispiel:

$\mathbb{R} \subset \mathbb{C}$ ist nicht quadratisch abgeschlossen, denn $i^2 = -1 \in \mathbb{R}$, $i \notin \mathbb{R}$.

$\mathbb{R} \subset \mathbb{C}$, $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2})$ sind Quadratwurzelerweiterung.

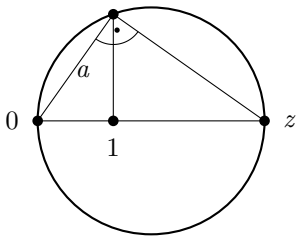
4.3.5 Satz:

$\tilde{M}$ ist quadratisch abgeschlossen in $\mathbb{C}$.

Beweis:

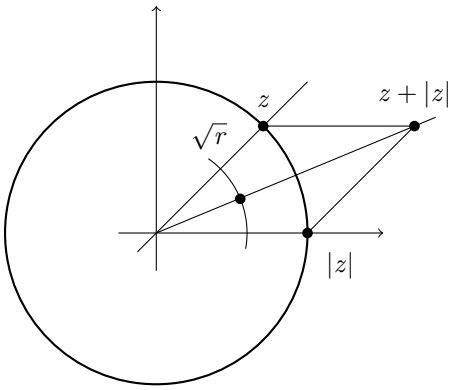
Sei $z \in \tilde{M} \cap \mathbb{R}_{>0}$, $z > 1$:

Konstruiere mit dem Kathetensatz a mit $1 \cdot z = a^2 \ \Rightarrow\ \sqrt{z} = a \in \tilde{M}$:



Sei $z \in \tilde{M} \cap \mathbb{R}_{>0}$, $z < 1 \Rightarrow \frac{1}{z} > 1 \Rightarrow \sqrt{\frac{1}{z}} \in \tilde{M} \Rightarrow \sqrt{z} = \frac{1}{\sqrt{\frac{1}{z}}} \in \tilde{M}$

Sei $z = r \cdot e^{i\cdot\varphi} \in \tilde{M} \Rightarrow \pm\sqrt{r} \cdot e^{i\frac{\varphi}{2}} \in \tilde{M}$, denn $\sqrt{r} \cdot e^{i\frac{\varphi}{2}} \in k(0,\sqrt{r}) \cap g(0, z+|z|) \subset \tilde{M}$



□

4.3.6 Satz:

$z \in \tilde{M} \Leftrightarrow \exists\, \mathbb{Q}(M \cup \tilde{M}) \subset L \subset \mathbb{C}$ mit $z \in L$ und $K = \mathbb{Q}(M \cup \overline{M}) \subset L$ ist Quadratwurzelerweiterung

Wobei $\overline{M}$ = Menge der komplex konjugierten Elemente von M.

Insbesondere:

$$z \in \tilde{M} \Rightarrow [\mathbb{Q}(z) : \mathbb{Q}] = 2^r \text{ ist Zweierpotenz}$$

Beweis:

„⇒ “ Sei $\mathbb{Q}(M \cup \overline{M}) \subset L \subset \mathbb{C}$ mit $z \in L$ und $K = \mathbb{Q}(M \cup \overline{M}) \subset L$ sei Quadratwurzelerweiterung.
$\Rightarrow L = K(\alpha_1, ..., \alpha_n)$, $\alpha_i^2 \in K(\alpha_1, ..., \alpha_{i-1})$.

Induktion über n:

$n = 0$: $L = K \subset \tilde{M}$

$n-1 \to n$: Nach Induktionsvorraussetzung gilt: $K(\alpha_1, ..., \alpha_{n-1}) \subset \tilde{M}$
$\alpha_n^2 \in K(\alpha_1, ..., \alpha_{n-1})$
$\Rightarrow \alpha_n^2 \in \tilde{M}$
$\Rightarrow \alpha_n \in \tilde{M}$, da $\tilde{M}$ quadratisch abgeschlossen
$\Rightarrow L \subset \tilde{M}$
$\Rightarrow z \in \tilde{M}$

„⇐ “ Wir verfolgen die Konstruktionsschritte, um z zu erreichen und adjungieren die neuen Elemente schrittweise zu $K = \mathbb{Q}(M \cup \overline{M})$ dazu, $K = K_0 \subset K_1 \subset \cdots$
Schneiden wir zwei Geraden, so erhalten wir die Koordinaten $(\mathrm{Re}(z), \mathrm{Im}(z))$ des Schnittpunkt z durch ein lineares Gleichungssystem über K.
Dies lässt sich über K schon lösen und wir müssen nichts dazu adjungieren.

Schneiden wir eine Gerade mit der Gleichung $y = mx+b$ mit einem Kreis mit der Gleichung $(x-a_1)^2+(y-a_2)^2 = r^2$, so erfüllt x die quadratische Gleichung:

$$f = (x - a_1)^2 + (mx + b - a_2)^2 - r^2 = 0$$

Falls f irreduzibel $/_{K_i}$ adjungieren wir eine Nullstelle dazu und erhalten :

$$K_{i+1} = K_i[x]/_{\langle f \rangle} \text{ mit } [K_{i+1} : K_i] = 2$$

Falls f reduzibel $/_{K_i}$ ist, ist $K_{i+1} = K_i$. Schneiden wir zwei Kreise mit den Gleichungen:

$$(x - a_1)^2 + (y - b_1)^2 = r_1^2$$
$$(x - a_2)^2 + (y - b_2)^2 = r_2^2$$

ersetzen wir zunächst die zweite Gleichung durch die Differenz beider:

$$2(a_1 - a_2)x + 2(b_1 - b_2)y = -r_1^2 + r_2^2 + a_1^2 + b_1^2 - a_2^2 - b_2^2$$

Dies ist eine Geradengleichung. Wir haben also wie vorher jetzt eine Kreis und eine Geradengleichung und verfahren wie im Fall vorher.

Wir erhalten schließlich L im letzten Konstruktionsschritt als Quadratwurzelerweiterung von K mit $z \in L$. $\square$

4.3.7 Korollar:

Würfelverdopplung (also die Konstruktion eines Würfels mit Volumen 2 ist durch Konstruktion nicht möglich.

Beweis:

Um einen Würfel des Volumens 2 zu konstruieren, müssen wir die Kantenlänge $\alpha = \sqrt[3]{2}$ konstruieren.

Behauptung: $m_\alpha = x^3 - 2 \in \mathbb{Q}[x]$ ist Minimalpolynom

Wäre m_α reduzibel, $m_\alpha = g \cdot h$ mit $\deg(g) > 0$, $\deg(h) > 0$, dann folgt, da $\deg(g) + \deg(h) = \deg(m_\alpha) = 3$.

Ohne Einschränkung sei $\deg(g) = 1$

$\Rightarrow$ g ist ein Linearfaktor

$\Rightarrow$ Die Nullstelle von g (die auch Nullstelle von m_α ist) muss in $\mathbb{Q}$ sein.

Aber die Nullstellen von m_α sind:

$$\sqrt[3]{2},\ \sqrt[3]{2} \cdot e^{\frac{2\pi i}{3}},\ \sqrt[3]{2} \cdot e^{\frac{4\pi i}{3}}$$

und keine davon ist in $\mathbb{Q}$.

Damit gilt $\mathbb{Q}(\sqrt[3]{2}) \cong {}^{\mathbb{Q}[x]}\!/_{\langle x^3 - 2 \rangle}$ und $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$.

Wäre α konstuierbar, also $\alpha \in \tilde{M}$, so gäbe es nach 4.3.6 eine Quadratwurzelerweiterung $\mathbb{Q} \subset L$ mit $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2}) \subset L$, aber $[L : \mathbb{Q}] = 2^r$. $\lightning$ da $3 \nmid 2$. $\square$

4.3.8 Bemerkung:

π ist transzendent ${}^{}\!/_{K_i}$ (Beispiel 4.1.12 3)). damit auch $\sqrt{\pi}$.

$\Rightarrow$ Ein Quadrat der Fläche π = Kreisfläche eines Kreises von Radius 1 ist nicht konstruierbar

$\Rightarrow$ Die Quadratur des Kreises ist nicht möglich.

In Korollar 4.3.7 war es wichtig die Irreduzibilität von $x^3 - 2$ zeigen zu können. Für weitere Aussagen dieser Art:

4.3.9 Satz: Eisenstein-Kriterium

Sei R faktoriell, $f \in R[x] \setminus R$ primitiv.

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

$\exists\ p \in R$ prim mit $p \mid a_0, ..., a_{n-1}$ $p^2 \nmid a_0 \Rightarrow f$ irreduzibel in $R[x]$.

Beweis:

Sei $f = g \cdot h$,

$$g = \sum_{i=0}^{k} b_i x^i, \quad h = \sum_{j=0}^{l} c_j x^j$$

Falls $k = 0$, so ist $g \in R$, $g \mid a_i\ \forall i$.

$\Rightarrow$ $g \in R^*$, da f primitiv.

Genauso folgt $h \in R^*$ falls $l = 0$.

Sei $k, l > 0$. Da $f = g \cdot h$ gilt

$$a_k = \sum_{i+j=k} b_i c_j \text{ für } k = 0, ..., n$$

$p \mid a_0 = b_0 c_0$, da p prim folgt ohne Einschränkung $p \mid b_0$. Da $p^2 \nmid a_0$ folgt $p \nmid c_0$.

Behauptung: $p \mid b_i\ \forall i = 0, ..., k$

Per Induktion, $p \mid b_0$ gilt. Es gelte $p \mid b_0, ..., b_{i-1}$. Da

$$\begin{aligned} a_i &= b_0 c_i + b_1 c_{i-1} + \cdots + b_i c_0 \\ \Rightarrow b_i c_0 &= a_i - b_o c_i - \cdots - b_{i-1} c_1 \end{aligned}$$

und alle Summanden rechts werden von p geteilt.

$\Rightarrow p \mid b_i c_0$, da p prim und $p \nmid c_0$ folgt $p \mid b_i$.

Damit folgt $p \mid a_n = b_k c_l$.

$\Rightarrow p \mid a_0, ..., a_n \lightning$ zu f primitiv. □

Beispiel:

$f = x^5 - 4x + 2 \in \mathbb{Z}[x] \setminus \mathbb{Z}$ ist primitiv, $2 \mid a_0, ..., a_{n-1}$, $2^2 \nmid a_0 \Rightarrow f$ ist irreduzibel.

4.3.10 Satz:

Sei R faktoriell, $f \in R[x] \setminus R$.

$$f \text{ ist irreduzibel in } R[x] \Leftrightarrow f \text{ primitiv in } R[x] \text{ und irreduzibel in } \mathrm{Quot}(R)[x]$$

Beweis:

Wegen des Satzes von Gauß (2.1.1) ist $R[x]$ faktoriell, $\mathrm{Quot}(R)[x]$ ist auch faktoriell, daher sind irreduzibel und prim äquivalent.

Sei f primitiv in $R[x]$ und irreduzibel in $\mathrm{Quot}(R)[x]$

$\overset{2.1.6}{\Rightarrow} f$ irreduzibel in $R[x]$.

Sei f irreduzibel in $R[x]$, $f = g \cdot h$ mit $g, h \in \mathrm{Quot}(R)[x]$. Wie in Lemma 2.1.3 2) schreiben wir g und h als

$$g = c \cdot p, \quad h = d \cdot p$$

mit $p, q \in R[x]$ primitiv und $c, d \in \mathrm{Quot}(R)$.

Wegen Lemma 2.1.5 ist $p \cdot q$ primitiv.

$\Rightarrow f = (c \cdot d) \cdot p \cdot q \overset{2.1.3}{\Rightarrow} (c \cdot d) \in R$

Diese Gleichung ist also in $R[x]$, und f ist irreduzibel in $R[x]$

$\Rightarrow$ Zwei der drei Faktoren $(cd), p, q$ sind Einheiten.

Dann folgt ohne Einschränkung $g = c \cdot p$ ist Einheit in $\mathrm{Quot}(R)[x]$.

$\Rightarrow f$ ist irreduzibel.

f muss primitiv sein, da für einen Teiler $e \in R \setminus R^*$ aller Koeffizienten $f = e \cdot \frac{f}{e}$ sonst eine Zerlegung in Nichteinheiten wäre. □

Beispiel:

$x^5 - 4x + 2 \in \mathbb{Q}[x]$ ist irreduzibel .

4.3.11 Satz:

Sei $e^{i\varphi}$ transzendent $/_{\mathbb{Q}}$, dann ist die 3-Teilung des Winkels φ nicht möglich.

Beweis:

Sei $z = e^{i\varphi}$. Das Bild des Einsetzehomomorphismus

$$\begin{aligned} \varphi : \ \mathbb{Q}[x] &\to \mathbb{Q} \\ x &\mapsto z \end{aligned}$$

ist isomorph zu $\mathbb{Q}[x]$, da n.V. z transzendent, also keine algebraische Gleichung erfüllt, also $\mathrm{Ker}(\varphi) = \{0\}$.

$\Rightarrow \mathbb{Q}[z]$ ist faktoriell und $z \in \mathbb{Q}[z]$ ist prim.

Betrachte $f = x^3 - z \in \mathbb{Q}[z][x]$ f ist primitiv, z teilt alle Koeffizienten außer a_n, $z^2 \nmid a_0$

$\overset{4.3.9}{\Rightarrow} f$ ist irreduzibel in $\mathbb{Q}[z][x]$

$\overset{4.3.10}{\Rightarrow} f$ ist irreduzibel in $\mathrm{Qout}(\mathbb{Q}[z])[x] = \mathrm{Quot}(z)[x]$

$\Rightarrow x^3 - z$ ist Minimalpolynom von $e^{\frac{i\varphi}{3}}$ und $\left[\mathbb{Q}(z)\left(e^{\frac{i\varphi}{3}}\right) : \mathbb{Q}(z)\right] = 3. \lightning$ zu 4.3.6 (Quadratwurzelerweiterung). □

4.3.12 Beispiel:

Das regelmäßige 5-Eck ist konstruierbar.

Zunächst: Für $z = e^{\frac{2\pi i}{5}}$ und $f = \frac{x^5-1}{x-1} = x^4 + x^3 + x^2 + x + 1$ gilt $f(z) = 0$. Für

$$\begin{aligned} \varphi : \ \mathbb{Z}[x] &\xrightarrow{\cong} \mathbb{Z}[x] \\ x &\mapsto x + 1 \end{aligned}$$

gilt

$$\begin{aligned} \varphi(f) = \varphi(x+1) = \frac{(x+1)^5 - 1}{x+1-1} &= \frac{\sum_{i=0}^{5} \binom{5}{i} x^i - 1}{x} \\ &= \frac{1 + 5x + 10x^2 + 10x^3 + 5x^4 + x^5 - 1}{x} \\ &= 5 + 10x + 10x^2 + 5x^3 + x^4 \end{aligned}$$

Da φ Isomorphismus gilt f irreduzibel $\Leftrightarrow$ $\varphi(f)$ irreduzibel.

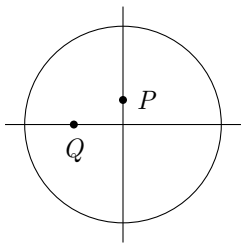
Da $5 \mid$ alle Koeffizienten außer a_n, $5^2 \nmid a_0$ folgt mit Eisenstein (4.3.9) $\varphi(f)$ irreduzibel.

$\Rightarrow f$ irreduzibel

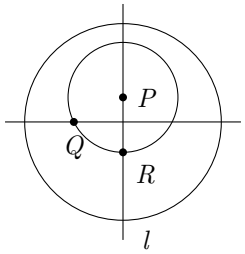
$\Rightarrow$ Das Minimalpolynom von z ist f und hat Grad 4.

Wir können also keinen Widerspruch zu Satz 4.3.6 erzeugen. Um die Konstruierbarkeit zu zeigen, müssen wir ein Konstruktionsverfahren angeben:

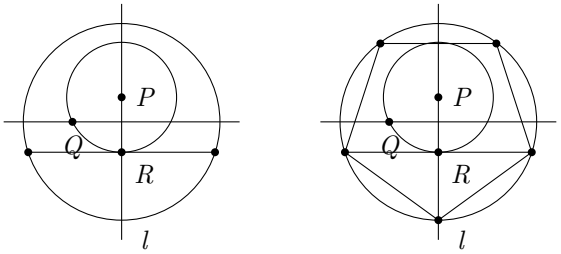
- Zwei aufeinander senkrechte Geraden durch den Mittelpunkt eines Kreises.
- Halbiere Radius erhalte Q
- Viertele Radius erhalte P



- Kreis mit Mittelpunkt P durch Q schneidet Gerade l in Punkt R

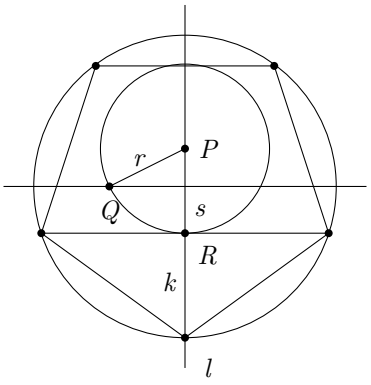


- Die Strecke durch R orthogonal zu l ist die Diagonale eines regelmäßigen 5-Ecks, trage ihre Länge 5 mal ab



Behauptung: Die Konstruktion funktioniert

Wir konstruieren die Längen:



$$r^2 = \left(\frac{1}{2}\right)^2 + \left(\frac{1}{4}\right)^2 = \frac{5}{16}$$

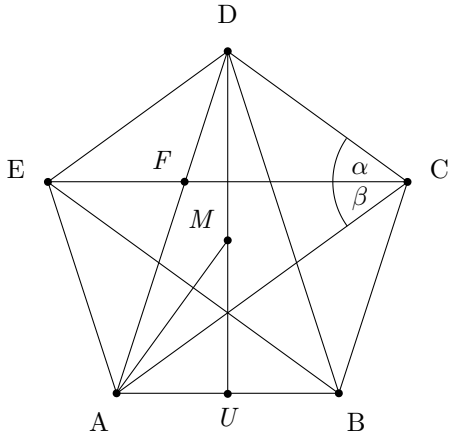
Man erhält

$$r = \frac{\sqrt{5}}{4}, \quad s = \frac{\sqrt{5}}{4} - \frac{1}{4}, \quad k = 1 - s = \frac{5}{4} - \frac{\sqrt{5}}{4}$$

In einem regelmäßigen 5-Eck gilt:

Innenwinkel $= \frac{360°}{5} = 72°$, Außenwinkel $= 180° - 72° = 108°$.

Sei a die Seitenlänge, d die Diagonalenlänge.



Wir erhalten für die Winkel:

$$\alpha = \frac{180° - 108°}{2} = 36°$$
$$\beta = 108° - 2 \cdot 36° = 36°$$

$\Rightarrow \triangle ABD$, $\triangle CDF$, $\triangle AEF$ sind ähnlich.

$\Rightarrow \overline{CF} = a$, $\frac{d}{a} = \frac{\overline{AD}}{\overline{AB}} = \frac{\overline{AE}}{\overline{EF}} = \frac{a}{d-a}$

Durch Lösen dieser quadratischen Gleichung für d in a erhalten wir

$$d = \frac{a}{2}\left(1 + \sqrt{5}\right)$$

Für die Höhe $h = \overline{DU}$ gilt dann

$$h^2 = d^2 - \frac{a^2}{4} = \frac{a^2}{4}\left(1 + \sqrt{5}\right)^2 - \frac{a^2}{4} = a^2\left(\frac{1}{4}\left(1 + 5\sqrt{5} + 5 - 1\right)\right) = a^2 \cdot \frac{1}{4}\left(5 + 2\sqrt{5}\right)$$

Weiter gilt $\overline{MU} = h - 1$ und in $\triangle AUM$:

$$\begin{aligned} 1 = \frac{a^2}{4} + (h-1)^2 &= \frac{a^2}{4} + h^2 - 2h + 1 \\ &= \frac{a^2}{4} + \frac{a^2}{4}\left(5 + 2\sqrt{5}\right) - a\sqrt{5 + 2\sqrt{5}} + 1 \\ &= \frac{a^2}{4}\left(6 + 2\sqrt{5}\right) - a\sqrt{5 + 2\sqrt{5}} + 1 \end{aligned}$$

Daraus folgt:

$$\Rightarrow \ \frac{a^2}{4}\left(6 + 2\sqrt{5}\right) - a\sqrt{5 + 2\sqrt{5}} = 0$$

$$\Rightarrow \ a \cdot \frac{3 + \sqrt{5}}{2} - \sqrt{5 + 2\sqrt{5}} = 0$$

$$\Rightarrow \ a \cdot \frac{3 + \sqrt{5}}{2} = \sqrt{5 + 2\sqrt{5}}$$

$$\Rightarrow \ a = \frac{2\sqrt{5 + 2\sqrt{5}}}{3 + \sqrt{5}} = \frac{2\sqrt{5 + 2\sqrt{5}}(3 - \sqrt{5})}{4} = \frac{1}{2}\sqrt{(5 + 2\sqrt{5})(14 - 6\sqrt{5})} = \frac{1}{2}\sqrt{10 - 2\sqrt{5}} = \sqrt{\frac{10 - 2\sqrt{5}}{4}} = \sqrt{\frac{5 - \sqrt{5}}{2}}$$

Für k gilt damit:

$$\begin{aligned} k^2 = a^2 - \frac{d^2}{4} = a^2 - \frac{a^2}{16}(6 + 2\sqrt{5}) &= a^2\left(\frac{10 - 2\sqrt{5}}{16}\right) \\ &= \frac{5 - \sqrt{5}}{2} \cdot \frac{10 - 2\sqrt{5}}{16} \\ &= \frac{60 - 20\sqrt{5}}{2 \cdot 16} \\ &= \frac{30 - 10\sqrt{5}}{16} \\ &= \frac{25 - 10\sqrt{5} + 5}{16} \\ &= \left(\frac{5 - \sqrt{5}}{4}\right)^2 \end{aligned}$$

also haben wir für k die richtige Länge konstruiert.

4.3.13 Satz:

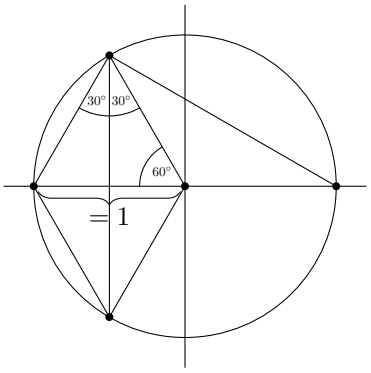
Das regelmäßige 9-Eck ist nicht konstruierbar.

Beweis:

Angenommen $e^{\frac{2\pi i}{9}} \in \tilde{M}$ (für $M = \{0, 1\}$).

$$\Rightarrow \ a = e^{\frac{2\pi i}{9}} + e^{\frac{-2\pi i}{9}} = 2 \cdot \mathrm{Re}\left(e^{\frac{2\pi i}{9}}\right) \in \tilde{M}$$

Man erhält:



$$a^3 = e^{\frac{2\pi i}{3}} + 3e^{\frac{2\pi i}{9}} + 3e^{\frac{-2\pi i}{9}} + e^{\frac{-2\pi i}{3}} = 3a + \underbrace{e^{\frac{2\pi i}{3}} + e^{\frac{-2\pi i}{3}}}_{=-1} = 3a - 1$$

Sei $f = x^3 - 3x + 1 \in \mathbb{Z}[x] \Rightarrow f(a) = 0$

Behauptung: f irreduzibel

Wäre $f = g \cdot h = (c_1 x + c_0)(d_2 x^2 + d_1 x + d_0)$

$\Rightarrow$ $c_0 d_0 = 1 \Rightarrow c_0 \in \mathbb{Z}^* = \{\pm 1\}$

und $c_1 d_2 = 1 \Rightarrow c_1 \in \mathbb{Z}^* = \{\pm 1\}$

$\Rightarrow$ Die möglichen Linearfaktoren sind $\pm(x \pm 1)$, aber ± 1 sind nicht Nullstellen von f $\lightning$

Mit 4.3.10 folgt $f \in \mathbb{Q}[x]$ ist irreduzibel.

$\Rightarrow f$ ist Minimalpolynom von a

$\Rightarrow [\mathbb{Q}(a) : \mathbb{Q}] = 3$ $\lightning$

wegen Satz 4.3.6. $\square$

4.4 Die Galoisgruppe

4.4.1 Definition:

Sei $K \subset L$ eine Körpererweiterung. Ein K-Automorphismus ist $\varphi: L \to L$ mit $\varphi|_K = \mathrm{id}_K$.

Beispiel:

Sei $\mathbb{R} \subset \mathbb{C}$, dann ist die komplexe Konjugation ein $\mathbb{R}$-Automorphismus von $\mathbb{C}$.

4.4.2 Bemerkung:

Jeder Automorphismus von K ist ein $P(K)$-Automorphismus für den Primkörper $P(K)$, denn

$$\varphi(1) = 1 \Rightarrow \varphi(a \cdot 1) = a \cdot 1 = a \;\forall\; a \in \mathbb{Z}$$

falls $P(K) = \mathbb{Q}$ außerdem

$$\varphi\left(\frac{p}{q}\right) = \frac{\varphi(p)}{\varphi(q)} = \frac{p}{q}$$

□

4.4.3 Lemma:

Sei $K \subset L$, φ ein K-Automorphismus. Dann ist φ ein K-Vektorraumhomomorphismus.

Falls $[L:K] < \infty$, ist φ K-Vektorraumisomorphismus.

Beweis:

$\varphi(l_1 + l_2) = \varphi(l_1) + \varphi(l_2)$ für $l_i \in L$, da φ Körperautomorphismus. Sei $\lambda \in K$, $l \in L$, dann gilt

$$\varphi(\lambda l) \overset{*}{=} \varphi(\lambda)\varphi(l) = \lambda \cdot \varphi(l)$$

(* Da φ Körperautomorphismus). Da $\varphi|_K = \mathrm{id}_K$. Als Körperautomorphismus ist φ injektiv.

Falls $[L:K] < \infty \Rightarrow \dim_K(L) < \infty$ folgt damit, dass φ Isomorphimus ist. □

4.4.4 Definition: Galoisgruppe

Sei $K \subset L$ eine Körpererweiterung.

$$\mathrm{Aut}_K(L) = \{\varphi \in \mathrm{Aut}(L) \mid \varphi|_K = \mathrm{id}_K\}$$

heißt die Gruppe der K-Automorphismen von L oder die Galoisgruppe von $K \subset L$.

Beispiel:

Für $\mathbb{R} \subset \mathbb{C}$ gilt

$$\mathrm{Aut}_{\mathbb{R}}(\mathbb{C}) = \{\mathrm{id},\ \mathrm{konj}\} \cong \mathbb{Z}_2$$

denn für $\varphi \in \mathrm{Aut}_{\mathbb{R}}(\mathbb{C})$ gilt

$$\begin{aligned} -1 = \varphi(-1) = \varphi(i^2) = \varphi(i) \cdot \varphi(i) = \varphi(i)^2 \\ \Rightarrow \varphi(i) \in \{\pm i\} \end{aligned}$$

4.4.5 Definition: Fixkörper und Fixgruppe

Sei $K \subset L$ eine Körpererweiterung und $U \subset \mathrm{Aut}_K(L)$ eine Untergruppe. Dann ist

$$\mathrm{Fix}(U) := \{a \in L \mid \varphi(a) = a \;\forall\; \varphi \in U\}$$

der Fixkörper von U, $K \subset \mathrm{Fix}(U) \subset L$.

Für einen Zwischenkörper M, $K \subset M \subset L$ ist

$$\mathrm{Aut}_M(L) \subset \mathrm{Aut}_K(L)$$

die Fixgruppe von M.

Beispiel: $\mathbb{R} \subset \mathbb{C}$

$U = \{\mathrm{id}\} \subset \mathbb{Z}_2$, $\mathrm{Fix}(U) = \mathbb{C}$, $\mathrm{Fix}(\mathbb{Z}_2) = \mathbb{R}$

4.4.6 Proposition:

Sei $K \subset L$, $f \in K[x]$, $\varphi \in \mathrm{Aut}_K(L)$.

Dann bildet φ die Nullstellen von f auf die Nullstellen von f ab.

Beweis:

Sei $f = a_n x^n + \cdots + a_0 \in K[x]$, seien $\alpha_1, ..., \alpha_n$ die Nullstellen von f. Es folgt:

$$0 = \varphi(0) = \varphi(f(\alpha_i)) = \varphi(a_n \alpha_i^n + \cdots + a_0) = a_n \varphi(\alpha_i)^n + \cdots + a_0 = f(\varphi(\alpha_i))$$

□

4.4.7 Lemma:

Sei $K \subset K[\alpha_1, ..., \alpha_r]$ algebraisch. $\varphi \in \mathrm{Aut}_K(K[\alpha_1, ..., \alpha_r])$ ist eindeutig durch die Bilder $\varphi(\alpha_1), ..., \varphi(\alpha_r)$ festgelegt.

Beweis:

Für $r = 0$ ist $\varphi = \mathrm{id}_K$. Induktion nach r.

Sei $l \in K[\alpha_1, ..., \alpha_r]$, dann lässt sich l schreiben als

$$l = c_d \alpha_r^d + \cdots + c_1 \alpha_r + c_0$$

mit $c_i \in K[\alpha_1, ..., \alpha_{r-1}]$.

$$\Rightarrow \ \varphi(l) = \varphi(c_d)\varphi(\alpha_r)^d + \cdots + \varphi(c_1)\varphi(\alpha_r) + \varphi(c_0)$$

ist eindeutig bestimmt durch die $\varphi(\alpha_i)$, da die $\varphi(c_i)$ durch $\varphi(\alpha_1), ..., \varphi(\alpha_{r-1})$ nach Induktionsvorraussetzung eindeutig bestimmt sind. □

4.4.8 Proposition:

Sei $f \in K[x]$ mit Zerfällungskörper L. Seien $\alpha_1, ..., \alpha_n$ die Nullstellen von f. Dann ist $\mathrm{Aut}_K(L) \subset \mathbb{S}_n = \mathbb{S}(\{\alpha_1, ..., \alpha_n\})$. Die Operation:

$$\begin{gathered} \bullet : \mathrm{Aut}_K(L) \times \{\alpha_1, ..., \alpha_n\} \to \{\alpha_1, ..., \alpha_n\} \\ \varphi \bullet \alpha_i = (\varphi, \alpha_i) \mapsto \varphi(\alpha_i) \end{gathered}$$

ist treu.

Beweis:

Nach 4.4.6 gilt $\varphi(\alpha_i) = \alpha_j$, wir können φ also mit einer Permutation der α_i identifizieren.

Nach 4.4.7 ist φ durch die Permutation eindeutig.

Gibt es ein α_i so dass $\forall \varphi$ gilt

$$\varphi(\alpha_i) = \alpha_i$$

so folgt $\varphi = \mathrm{id}$. Also ist die Gruppenbildung treu. □

Beispiel:

Sei $f = x^3 - 2 \in \mathbb{Q}[x]$, $L = \mathbb{Q}[\alpha_1, \alpha_2, \alpha_3]$ mit $\alpha_j = \sqrt[3]{2} \cdot e^{\frac{2\pi i}{3} \cdot j}$.

Es gilt $[L : \mathbb{Q}] = 6$, denn $\mathbb{Q} \subset \mathbb{Q}\left(\sqrt[3]{2}\right) \subset L$, $\left[\mathbb{Q}\left(\sqrt[3]{2}\right) : \mathbb{Q}\right] = 3$, $\mathbb{Q}\left(\sqrt[3]{2}\right) \neq L$,

$f \big/ x - \sqrt[3]{2} \in \mathbb{Q}\left(\sqrt[3]{2}\right)[x]$ ist Minimalpolynom von $\alpha_2 \in L$.

$\mathrm{Aut}_{\mathbb{Q}}(L) \cong \mathbb{S}_3$, da f keine mehrfache Nullstellen hat.

4.4.9 Proposition:

Ist $K \subset L$ endlich, so gilt

$$|\mathrm{Aut}_K(L)| \leq [L:K]$$

Beweis:

Sei $L = K[\alpha_1, ..., \alpha_n]$, sei f_j das Minimalpolynom von α_j über $K[\alpha_1, ..., \alpha_{j-1}]$.

Die Inklusion $\varphi_0 : \ K \hookrightarrow \ L$ ist der einzige Körperhomomorphismus $K \to L$, der K festhält.

Sei $\varphi_{j-1} : \ K[\alpha_1, ..., \alpha_{j-1}] \to L$ ein Körperhomomorphismus, der K festhält.

Behauptung:

$\exists$ höchstens $\deg(f_j)$ Körperhomomorphismen

$$\varphi_j : \ K[\alpha_1, ..., \alpha_j] \to L$$

mit

$$\varphi_j\big|_{K[\alpha_1,...,\alpha_{j-1}]} = \varphi_{j-1}$$

Wie in 4.4.7 ist φ_j durch das Bild $\varphi_j(\alpha_j)$ festgelegt, und $\varphi_j(\alpha_j)$ muss eine Nullstelle von $\varphi_{j-1}(f_j)$ sein, denn für

$$f_j = c_r x^r + \cdots + c_0$$

mit $c_i \in K[\alpha_1, ..., \alpha_{j-1}]$ gilt:

$$\begin{aligned}\varphi_{j-1}(f_j)(\varphi_j(\alpha_j)) &= \varphi_{j-1}(c_r)\varphi_j(\alpha_j)^r + \cdots + \varphi_{j-1}(c_0) \\ &= \varphi_{j-1}(c_r\alpha_j^r + \cdots + c_0) \\ &= \varphi_{j-1}(f_j(\alpha_j)) \\ &= 0\end{aligned}$$

Wir bekommen damit insgesamt höchstens

$$\prod_j \deg(f_j)$$

Möglichkeiten für Elemente in $\mathrm{Aut}_K(L)$. Es gilt:

$$\begin{aligned}[L:K] &= [K(\alpha_1, ..., \alpha_n) : K] \\ &= [K(\alpha_1, ..., \alpha_n) : K(\alpha_1, ..., \alpha_{n-1})] \cdot \ \cdots \ \cdot [K(\alpha_1) : K] \\ &= \prod_j \deg(f_j)\end{aligned}$$

also folgt die Aussage. □

4.4.10 Korollar:

Sei $f \in K[x], L$ Zerfällungskörper. Dann gilt

$$|\mathrm{Aut}_K(L)| \leq [L:K]$$

und Gleichheit, wenn jeder irreduzible Faktor von f keine mehrfachen Nullstellen hat.

Beweis:

Wie im vorherigen Beweis durch Adjunktion der Nullstellen von f.

Jedes Minimalpolynom f_j ist ein Teiler des Minimalpolynoms m_{α_j} von α_j über K. Da

$$f = c \cdot m_{\alpha_1} \cdots m_{\alpha_n}$$

über K die Zerlegung in irreduzible Faktoren ist, und die m_{α_j} nach Voraussetzung keine mehrfachen Nullstellen haben, haben auch die f_j keine mehrfachen Nullstellen und wir haben in jedem Schritt zur Konstruktion der Elemente von $\mathrm{Aut}_K(L)$ die volle Auswahl. □

4.5 Normale und separable Körpererweiterung

4.5.1 Definition: Normale Körpererweiterung

Eine algebraische Körpererweiterung $K \subset L$ heißt normal, wenn jedes irreduzible Polynom $g \in K[x]$ mit einer Nullstelle in L schon über L in Linearfaktoren zerfällt.

Beispiel:

1) $\mathbb{Q} \subset \mathbb{Q}\left(\sqrt[3]{2}\right)$ ist nicht normal, da $x^3 - 2 \in \mathbb{Q}[x]$ irreduzibel ist, aber für die weiteren Nullstellen gilt:

$$\sqrt[3]{2}e^{\frac{2\pi i}{3}},\ \sqrt[3]{2}e^{\frac{4\pi i}{3}} \notin \mathbb{Q}\left(\sqrt[3]{2}\right)$$

2) $\mathbb{R} \subset \mathbb{C}$ ist normal, da jedes irreduzible Polynom in $\mathbb{R}[x]$ über $\mathbb{C}$ in Linearfaktoren zerfällt.

4.5.2 Lemma:

Sei $\varphi:\ K \xrightarrow{\cong} K'$, L Zerfällungskörper von $f \in K[x]$, L' Zerfällungskörper von $\varphi(f) \in K'[x]$.

Dann $\exists\ \Psi:\ L \to L'$ mit $\Psi|_K = \varphi$

Beweis:

Induktion nach $d = \deg(f)$.

Für $d = 1$ ist $L = K$, $L' = K'$, $\Psi = \varphi$.

Sei $d > 1$, sei α_1 eine Nullstelle von f mit Minimalpolynom $g \in K[x]$. g ist ein irreduzibler Faktor von f, und $\varphi(g)$ damit ein irreduzibler Faktor von $\varphi(f)$.

Da L' Zerfällungskörper von $\varphi(f)$ $\exists\ \alpha_1' \in L'$ mit $\varphi(g)(\alpha_1') = 0$.

$$\varphi_1:\ K[\alpha_1] \cong K[x]\big/_{\langle g \rangle} \cong K'[x]\big/_{\varphi(g)} \cong K'[\alpha_1]$$

ist ein Isomorphismus mit $\varphi_1|_K = \varphi$.

Es gilt $f = (x - \alpha_1) \cdot f_1$ mit $\deg(f_1) < d$ und $\varphi(f) = \varphi_1(f) = (x - \alpha_1') \cdot \varphi_1(f_1) \in K[\alpha_1'][x]$.

Damit ist L Zerfällungskörper von $f_1 \in K[\alpha_1][x]$ und L' Zerfällungskörper von $\varphi_1(f_1) \in K'[\alpha_1'][x]$.

Per Induktion können wir φ_1 zu

$$\Psi:\ L \to L'$$

fortsetzen. □

4.5.3 Proposition:

Sei $L =$ Zerfällungskörper von $f \in K[x]$ dann ist $K \subset L$ normal.

Beweis:

Sei $L = K[\alpha_1, ..., \alpha_n]$ mit Nullstellen $\alpha_1, ..., \alpha_n$ von f.

Sei $g \in K[x]$ irreduzibel mit Nullstelle $\beta \in L$, und M der Zerfällungskörper von $g \in L[x]$.

Sei $\gamma \in M$ eine Nullstelle von g. Da g irreduzibel ist gilt:

$$K[\beta] \cong K[x]\big/_{\langle g \rangle} \cong K[\gamma]$$

mit Isomorphismus $\varphi:\ K[\beta] \to K[\gamma]$ und $\varphi|_K = \mathrm{id}_K$.

$L[\gamma] = K[\gamma][\alpha_1, ..., \alpha_n]$ ist Zerfällungskörper von $f \in K[\gamma][x]$.

Genauso ist $L = L[\gamma] = K[\beta][\alpha_1, ..., \alpha_n]$ Zerfällungskörper von $f \in K[\beta][x]$.

Wegen 4.5.2 lässt sich φ zu einem Isomorphismus

$$\Psi:\ L \to L[\gamma]$$

erweitern. Da $L \subset L[\gamma]$ folgt $L = L[\gamma]$ und $\gamma \in L$. □

4.5.4 Proposition:

Eine endliche Erweiterung $K \subset L$ ist normal
$\Leftrightarrow$ L ist Zerfällungskörper eines Polynoms $f \in K[x]$

" $\Leftarrow$ " 4.5.3

" $\Rightarrow$ " $\exists$ algebraische $\alpha_i \in L$ mit $L = K[\alpha_1, ..., \alpha_n]$.

Sei $g_i \in K[x]$ das Minimalpolynom von α_i. Da $K \subset L$ normal und g_i die Nullstelle $\alpha_i \in L$ hat, zerfällt g_i über L in Linearfaktoren.

Damit ist L der Zerfällungskörper von $f = g_1 \cdot \cdots \cdot g_r$. □

4.5.5 Korollar:

Ist $K \subset L$ eine endliche, normale Körpererweiterung und $K \subset M \subset L$ ein Zwischenkörper, dann ist auch $M \subset L$ normal.

Beweis:

Wegen 4.5.4 ist L der Zerfällungskörper von $f \in K[x] \subset M[x]$. □

4.5.6 Definition:

1) Ein irreduzibles Polynom heißt separabel, wenn es keine mehrfachen Nullstellen im Zerfällungskörper besitzt.

   Ein Polynom heißt separabel, wenn seine irreduziblen Faktoren separabel sind.

2) Eine algebraische Körpererweiterung $K \subset L$ heißt separabel, wenn für jedes $\alpha \in L$ das Minimalpolynom m_α separabel ist.

4.5.7 Lemma:

Sei $f \in K[x]$, $K \subset L$, $\alpha \in L$ α ist mehrfache Nullstelle von $f \quad \Leftrightarrow \quad f(\alpha) = 0$ und $f'(\alpha) = 0$

Beweis:

Sei $f = (x - \alpha)^m \cdot g$ mit $g(\alpha) \neq 0 \Rightarrow f' = (x - \alpha)^{m-1} \cdot (mg + (x - \alpha)g')$.

" $\Rightarrow$ " $m \geq 2 \Rightarrow f'(\alpha) = 0$

" $\Leftarrow$ " Da $g(\alpha) \neq 0$ ist $f'(\alpha) = 0$ nur wenn $m - 1 \geq 1$. □

4.5.8 Lemma:

Ein irreduzibles $f \in K[x]$ hat eine mehrfache Nullstelle
$\Leftrightarrow$ $f' = 0$

Beweis:

" $\Rightarrow$ " Sei α die mehrfache Nullstelle, dann gilt $f'(\alpha) = 0$.

Da $\deg(f') < \deg(f)$ und f das Minimalpolynom von α ist, folgt $f' = 0$.

" $\Leftarrow$ " Wenn $f' = 0$ gilt insbesondere $f'(\alpha) = 0$ für jede Nullstelle α von f und damit hat f eine mehrfache Nullstelle nach 4.5.7. □

4.5.9 Lemma:

Ist $K \subset L$ separabel und $K \subset M \subset L$ ein Zwischenkörper, dann sind auch $K \subset M$ und $M \subset L$ separabel.

Beweis:

Für $K \subset M$ nach Definition.

Das Minimalpolynom von $\alpha \in L$ über M ist ein Teiler des Minimalpolynoms über K, daher auch $M \subset L$. □

4.5.10 Proposition:

Sei $\text{char}(K) = 0$, dann ist jede algebraische Körpererweiterung $K \subset L$ separabel.

Beweis:

Sei $\alpha \in L$, $m_\alpha \in K[x]$ das Minimalpolynom, $m_\alpha = x^n + a_{n-1}x^{n-1} + \cdots + a_0$.

Da $n \neq 0$ gilt $m'_\alpha = nx^{n-1} + \cdots \neq 0$

$\Rightarrow m_\alpha$ hat keine mehrfache Nullstelle wegen 4.5.8. □

4.5.11 Korollar:

Sei $\text{char}(K) = 0$, dann ist jedes Polynom separabel.

Beweis:

Sei $f = cf_1 \cdots f_r$ die Zerlegung in irreduzible Faktoren. Wie eben gilt $f_i' \neq 0$.

$\Rightarrow f_i$ hat keine mehrfache Nullstelle wegen 4.5.8

$\Rightarrow f$ ist separabel. □

Beispiel:

Sei $K = \mathbb{Z}_p(t)$ der Körper der rationalen Funktionen über $\mathbb{Z}_p$.

Dann ist $f = x^p - t \in K[x]$ irreduzibel, denn f ist irreduzibel in $\mathbb{Z}_p[t][x] : \mathbb{Z}_p[t]$ ist faktoriell, $t \in \mathbb{Z}_p[t]$ ist prim, $t \mid a_0$, $t^2 \nmid a_0$, f ist primitiv, also folgt die Irreduzibilität mit Eisenstein 4.3.9.

$\Rightarrow f$ ist Minimalpolynom von $[x]$ in $K[x]/\langle f \rangle = L$.
(Erinnerung: $f([x]) = [a_n][x]^n + \cdots + [a_0] = [a_n x^n + \cdots + a_0] = [f(x)] = [0]$)

$K \subset L$ ist nicht separabel, denn f ist nicht separabel: f hat eine mehrfache Nullstelle, da $f' = px^{p-1} = 0$ (4.5.8)

4.6 Endliche Körper

4.6.1 Satz:

Sei F ein Körper mit endliche vielen Elementen. Dann $\exists$ p Primzahl mit $\text{char}(F) = p$, $|F| = p^r$ wobei $r = [F : \mathbb{Z}_p] < \infty$ und $\mathbb{Z}_p$ der Primkörper $P(F)$ ist.

Beweis:

$P(F) = \mathbb{Z}_p$ und $\text{char}(F) = p$ wegen Satz 4.1.6. F ist endlicher $\mathbb{Z}_p$-Vektorraum, also $[F : \mathbb{Z}_p] = r < \infty$

$\Rightarrow F \cong (\mathbb{Z}_p)^r$ als $\mathbb{Z}_p$-Vektorraum

$\Rightarrow |F| = p^r$ □

Beispiel:

$x^2 + x + 1 \in \mathbb{Z}_2[x]$ ist irreduzibel, denn die einzigen Polynome vom Grad 1 in $\mathbb{Z}_2[x]$ sind $x + 1$ und x und $x^2 + x + 1$ ist kein Produkt mit diesen Faktoren.

$\Rightarrow F_4 = {}^{\mathbb{Z}_2[x]}\!/_{\langle x^2 + x + 1 \rangle}$ ist ein endlicher Körper mit $2^2 = 4$ Elementen der Charakteristik 2.

Seine Verknüpfungstabellen sind:

$+$	0	1	x	$x+1$
0	0	1	x	$x+1$
1	1	0	$x+1$	x
x	x	$x+1$	0	1
$x+1$	$x+1$	x	1	0

$\cdot$	1	x	$x+1$
1	1	x	$x+1$
x	x	$x+1$	1
$x+1$	$x+1$	1	x

4.6.2 Definition: Frobeniushomomorphismus

Sei $\text{char}(L) = p$.

$$\begin{aligned} Fr: \ & L \to L \\ & a \mapsto a^p \end{aligned}$$

heißt Frobeniushomomorphismus und ist Körpermonomorphismus, für L endlich Automorphismus.

Beweis:

Für $a, b \in L$ ist

$$Fr(a \cdot b) = (a \cdot b)^p = a^p \cdot b^p = Fr(a) \cdot Fr(b)$$

und

$$Fr(a + b) = (a + b)^p = a^p + \binom{p}{1} a^{p-1} b + \cdots + \binom{p}{j} a^{p-j} b^j + \cdots + \binom{p}{p-1} a b^{p-1} + b^p = a^p + b^p = Fr(a) + Fr(b)$$

Falls $a^p = 0$ ist $a = 0 \Rightarrow Fr$ ist injektiv. □

4.6.3 Satz:

Zu jeder Primzahlpotenz gibt es bis auf Isomorphie genau einen Körper F mit p^r Elementen, den Zerfällungskörper von $f = x^{p^r} - x \in \mathbb{Z}_p[x]$.

Beweis:

$$f' = p^r \cdot x^{p^r - 1} - 1 = -1 \in \mathbb{Z}_p[x]$$

hat keine Nullstellen, also hat f keine mehrfachen Nullstellen und ist separabel.

Der Zerfällungskörper L von f enthält die p^r Nullstellen von f und ist der kleinste solche Körper.

Behauptung: Die Menge der Nullstellen von f ist ein Körper (damit gleich L, und $|L| = p^r$)

Es gilt:

α Nullstelle von f
$\Leftrightarrow$ $f(\alpha) = 0$
$\Leftrightarrow$ $a^{p^r} - \alpha = 0$
$\Leftrightarrow$ $a^{p^r} = \alpha \Rightarrow Fr^r(\alpha) = \alpha$
$\Leftrightarrow$ α ist Fixpunkt von Fr^r

Seien α, β Nullstellen von f.

- $Fr^r(\alpha + \beta) = Fr^r(\alpha) + Fr^r(\beta) = \alpha + \beta$
  $\Rightarrow \alpha + \beta$ ist Nullstelle.
- 0 ist Nullstelle von f
- $Fr^r(-\alpha) = -Fr^r(\alpha) = -\alpha$
  $\Rightarrow -\alpha$ ist Nullstelle von f

$\Rightarrow \{\text{Nullstellen}\} \subset (L, +)$ ist Untergruppe.

- $Fr^r(\alpha \cdot \beta) = Fr^r(\alpha) \cdot Fr^r(\beta)$
- $Fr^r\left(\frac{1}{\alpha}\right) = \frac{1}{Fr^r(\alpha)}$
- $Fr^r(1) = 1$

$\Rightarrow \{\text{Nullstellen}\} \subset (L\backslash\{0\}, \cdot)$ ist Untergruppe.

Damit ist

$$L = \text{Zerfällungskörper von } f = \{\text{Nullstellen von } f\}$$

ein Körper mit $|L| = p^r$.

Sei F ein beliebiger Körper mit $|F| = p^r$.

$$|F^*| = p^r - 1 \Rightarrow \forall\ a \in F^* :\ (a)^{p^r - 1} = 1$$

da die Ordnung eines Elements in F^* die Gruppenordnung teilt.

$\Rightarrow$ $a^{p^r} = a\ \forall a \in F^*$
$\Rightarrow$ $a^{p^r} = a\ \forall a \in F$
$\Rightarrow$ $F \subset \{\text{Nullstellen von } f\}$
$\Rightarrow$ $F = \{\text{Nullstellen von } f\} = L$ □

Wir schreiben F_{p^r} für den Körper mit p^r Elementen.

4.6.4 Definition: Eulersche Phifunktion

Wir nennen

$$\begin{aligned} \varphi :\ & \mathbb{N} \to \mathbb{Z} \\ & n \mapsto \varphi(n) = \#\{r \in \mathbb{Z} \mid 1 \leq r \leq n,\ \text{ggT}(r, n) = 1\} \end{aligned}$$

die eulersche Phifunktion.

4.6.5 Korollar:

Sei $G = \langle g \rangle$ eine zyklische Gruppe. Sei $|G| = n$, $d \mid n$. Dann gibt es $\varphi(d)$ Elemente der Ordnung d in G

$$\left\{ g^{r \cdot \frac{n}{d}} \mid 1 \leq r \leq d,\ \text{ggT}(r, d) = 1 \right\}$$

Insbesondere gibt es $\varphi(n)$ Elemente der Ordnung n, also Erzeuger.

Folgt aus dem Satz über Untergruppen zyklischer Gruppen.

Beispiel: $(\mathbb{Z}_{12}, +)$

Element	0	1	2	3	4	5	6	7	8	9	10	11
Ordnung	1	12	6	4	3	12	2	12	3	4	6	12

- $\varphi(12) = 4$

  Erzeuger von $\mathbb{Z}_{12}$: $1,\ 5,\ 7,\ 11$

- $\varphi(6) = 2$

  Elemente der Ordnung 6:

$$\left(1 \cdot \frac{12}{6}\right) \cdot 1 = 2, \quad \left(5 \cdot \frac{12}{6}\right) \cdot 1 = 10$$

  denn $\{1,5\} = \{r \mid 1 \leq r \leq 6,\ \text{ggT}(r,6) = 1\}$

- $\varphi(2) = 1$

  Element der Ordnung 2:

$$\left(1 \cdot \frac{12}{2}\right) \cdot 1 = 6$$

4.6.6 Korollar:

Sei $n \in \mathbb{N}$:

$$\sum_{d \mid n} \varphi(d) = n$$

Beweis:

Sei G die Zyklische Gruppe der Ordnung n. Jedes Element hat als Ordnung einen Teiler d von n, für jeden Teiler gibt es $\varphi(d)$ Elemente dieser Ordnung. Daher ist $\sum_{d \mid n} \varphi(d)$ die Anzahl der Elemente von G. □

4.6.7 Satz:

Sei K ein Körper, $H \subset K^*$ endliche Untergruppe

$\Rightarrow$ H zyklisch

Beweis:

Sei $|H| = n,\ d \mid n,\ a \in H$ mit Ordnung d.

Dann ist $a^d = 1, (a^2)^d = 1, ..., (a^{d-1})^d = 1$

$\Rightarrow 1, a, ..., a^{d-1}$ sind Nullstellen von $f = x^d - 1 \in K[x]$. Da $\deg(f) = d$ sind dies alle Nullstellen und

$$\left\{b \in K \mid b^d = 1\right\} = \{1, a, ..., a^{d-1}\}$$

ist eine zyklische Untergruppe von H der Ordnung g.

Unter diesen Elementen sind $\varphi(d)$ Elemente der Ordnung d.

Setze $\Psi(d) = \#$ Elemente der Ordnung d in H. Dann gilt:

$$\varphi(d) = \begin{cases} \varphi(d) & \exists \text{ Element der Ordnung } d \\ 0 & \text{sonst} \end{cases}$$

$\Rightarrow n = |H| = \sum_{d \mid n} \Psi(d) \leq \sum_{d \mid n} \varphi(d) = n$

$\Rightarrow \Psi(d) = \varphi(d)\ \forall\ d$

$\Rightarrow \exists$ Elemente der Ordnung $d\ \forall\ d \mid n$, insbesondere $\exists$ Element der Ordnung n und H ist zyklisch. □

4.6.8 Definition: Einfache Körpererweiterung

Eine Körpererweiterung der Form $K \subset K(\alpha)$ heißt einfach.

α heißt primitives Element.

4.6.9 Satz vom primitiven Element

Jede endliche Erweiterung eines endlichen Körpers ist einfach.

Beweis:

Sei $K \subset L$ endlich, $|K| < \infty$
$\Rightarrow |L| < \infty$
$\overset{4.6.7}{\Rightarrow}$ L^* ist zyklisch, also $L^* = \langle \alpha \rangle$ und $L = K(\alpha)$. □

4.6.10 Korollar:

In $\mathbb{Z}_p[x]$ gibt es irreduzible Polynome vom Grad $r \; \forall \; r \in \mathbb{N}_{>0}$.

Beweis:

Sei F_{p^r} der Körper mit p^r Elementen. $\mathbb{Z}_p = P(F_{p^r}) \subset F_{p^r}$ ist eine einfache Erweiterung wegen 4.6.9

$\Rightarrow F_{p^r} = \mathbb{Z}_p(\alpha) = \mathbb{Z}_p[\alpha]$, da α algebraisch und

$$r = [F_{p^r} : \mathbb{Z}_p] = [\mathbb{Z}_p(\alpha) : \mathbb{Z}_p] = \deg(m_\alpha)$$

für das Minimalpolynom m_α von α

$\Rightarrow m_\alpha$ ist ein irreduzibles Polynom in $\mathbb{Z}_p[x]$ vom Grad r. □

In 4.4.5 haben wir Fixkörper eingeführt. Wir untersuchen jetzt Fixkörper von endlichen Körpern.

Beispiel:

$$F_4 = {}^{F_2[x]}\!/_{\langle x^2 + x + 1 \rangle} = \{0, 1, x, x+1\}$$

mit

$$\begin{aligned} Fr: \; & 0 \mapsto 0 \\ & 1 \mapsto 1 \\ & x \mapsto x^2 = x + 1 \\ & x + 1 \mapsto (x+1)^2 = x^2 + 2x + 1 = x + 1 + 1 = x \end{aligned}$$

$\Rightarrow \mathrm{Fix}(Fr) = F_2$

(Beachte, allgemein ist Fr ein $\mathbb{Z}_p$-Automorphismus von F_{p^r} wegen 4.4.2)

$$\begin{aligned} Fr^2: \; & 0 \mapsto 0 \\ & 1 \mapsto 1 \\ & x \mapsto x^4 = (x+1)^2 = x \\ & x + 1 \mapsto (x+1)^4 = x^2 = x + 1 \end{aligned}$$

$\Rightarrow \mathrm{Fix}(Fr^2) = F_4$

4.6.11 Satz:

In F_{p^r} $\exists$ zu $s \mid r$ genau ein Zwischenkörper

$$\mathbb{Z}_p \subset F_{p^s} \subset F_{p^r}$$

mit p^s Elementen, nämlich

$$F_{p^s} = \mathrm{Fix}(Fr^s) = \{a \in F_{p^r} \mid a^{p^s} = a\}$$

Beweis:

$\left|F_{p^r}^*\right| = p^r - 1$, wegen 4.6.7 ist $F_{p^r}^* = \langle \alpha \rangle$ zyklisch.

$$p^r - 1 = p^{s \cdot k} - 1 = (p^s - 1) \cdot \left(p^{(k-1)s} + \cdots + p^s + 1\right)$$

$\Rightarrow p^s - 1 \mid p^r - 1$

In zyklischen Gruppen $\exists$ zu jedem Teiler der Gruppenordnung genau eine Untergruppe dieser Ordnung

$\Rightarrow \exists!$ Untergruppe U der Ordnung $p^s - 1$ von $F_{p^r}^*$, wobei

$$U = \left\langle \alpha^{\frac{p^r-1}{p^s-1}} \right\rangle$$

Für jedes $\beta \in U$ gilt $\beta^{p^s-1} = 1$ und jedes Element, dessen Ordnung $p^s - 1$ teilt, liegt in U. Es folgt:

$$\beta^{p^s} = \beta \;\Leftrightarrow\; Fr^s(\beta) = \beta \;\Leftrightarrow\; \beta \in U \cup \{0\}$$

$\Rightarrow U \cup \{0\} = \mathrm{Fix}(Fr^s)$ ist der eindeutige Unterkörper mit p^s Elementen. □

Beispiel:

Durch Probieren sieht man, dass $x^4 + x + 1 \in F_2[x]$ irreduzibel ist. Damit gilt:

$$\begin{aligned} F_{16} &= \{0, 1, x, x+1, x^2, x^2+x, x^2+1, x^2+x+1, x^3, x^3+x^2, x^3+x^2+x, x^3+x, x^3+x^2+x+1, \\ &\qquad x^3+x+1, x^3+x^2+1, x^3+1\} \\ F_{16} &= \mathrm{Fix}(Fr^4) = \{a \mid a^{16} = a\} \\ F_2 &= \mathrm{Fix}(Fr) \end{aligned}$$

Für Fr^2 gilt:

$$\begin{aligned} (x^2+x)^4 &= x^8 + x^4 \\ &= x^4 \cdot x^4 + x^4 \\ &= (x+1)(x+1) + x + 1 \\ &= x^2 + 1 + x + 1 \\ &= x^2 + x \end{aligned}$$

und

$$\begin{aligned} (x^2+x+1)^4 &= x^8 + x^4 + 1 \\ &= (x+1)^2 + x + 1 + 1 \\ &= x^2 + 1 + x \end{aligned}$$

$0^4 = 0$, $1^4 = 1$, alle anderen werden nicht festgehalten.

$\Rightarrow \mathrm{Fix}(Fr^2) = \{0, 1, x^2+x, x^2+x+1\}$

4.6.12 Satz:

$x^{p^r} - x \in F_p[x]$ ist das Produkt aller irreduziblen normierten Polynome vom Grad d mit $d \mid r$.

Beweis:

Sei f irreduzibel und normiert vom Grad d.

Wir zeigen: $f \mid x^{p^r} - x \;\Leftrightarrow\; d \mid r$

Da $x^{p^r} - x$ nur einfache Nullstellen hat folgt dann die Behauptung.

" $\Leftarrow$ " Sei $d \mid r$. Sei α eine Nullstelle von f. Sei $K = F_p(\alpha)$. Es gilt $[K : F_p] = d$, also $|K| = p^d$

$\overset{4.6.11}{\Rightarrow} K \cong \mathrm{Fix}(Fr^d) \subset F_{p^r}$. Das Polynom

$$x^{p^r} - x = \prod_{a \in F_{p^r}} (x - a)$$

hat α als Nullstelle. Damit wird es vom Minimalpolynom f von α geteilt.

" $\Rightarrow$ " $f \mid x^{p^r} - x$. In F_{p^r} zerfällt $x^{p^r} - x$ und damit auch f in Linearfaktoren. Sei α eine Nullstelle von f, dann ist

$$r = [F_{p^r} : F_p] = [F_{p^r} : F_p(\alpha)] \cdot \underbrace{[F_p(\alpha) : F_p]}_{d}$$

also $d \mid r$. □

4.6.13 Satz:

$\mathrm{Aut}(F_{p^r})$ ist zyklisch der Ordnung r mit Erzeuger Fr.

Beweis:

Fr hat die Ordnung r, denn

$$Fr^r(\alpha) = \alpha^{p^r} = \alpha \;\Rightarrow\; Fr^r = \mathrm{id}$$

aber $Fr^k \neq \mathrm{id}$ für $k < r$, denn $\mathrm{Fix}(Fr^k) \subsetneq F_{p^r}$.

Damit ist $\langle Fr\rangle \subset \mathrm{Aut}(F_{p^r})$ eine zyklische Untergruppe der Ordnung r.

Es gilt $F_{p^r} = F_p(\alpha)$ und das Minimalpolynom m_α von α hat Grad

$$r = [F_{p^r} : F_p] = [F_p(\alpha) : F_p]$$

$m_\alpha \in F_p[x]$ und F_{p^r} ist F_p-Automorphismus wegen 4.4.2.

$\Rightarrow F_r(m_\alpha) = m_\alpha$. Damit ist mit α auch $Fr(\alpha)$ eine Nullstelle von m_α und $Fr^j(\alpha)$, $j > 0$ auch

$$\Rightarrow m_\alpha = \prod_{j=1}^{r} (x - Fr^j(\alpha))$$

Sei $\varphi \in \mathrm{Aut}_{F_p}(F_{p^r})$, dann gilt wegen 4.4.7 $\varphi(\alpha)$ ist Nullstelle von m_α

$\Rightarrow \exists\, j :\; \varphi(\alpha) = Fr^j(\alpha)$

Wegen 4.4.8 ist φ eindeutig durch $\varphi(\alpha)$ festgelegt, also folgt $\varphi = Fr^j$.

$\Rightarrow \mathrm{Aut}_{F_p}(F_{p^r}) = \langle Fr\rangle$ □

4.6.14 Satz:

Sei $K \subset L$ eine Erweiterung endlicher Körper, also $K = F_q$, $L = F_{q^n}$ mit $q = p^r$ Primzahlpotenz, dann ist $K = \mathrm{Fix}(Fr_q)$ mit $(Fr_q = Fr^r)$

$$\begin{aligned} Fr_q :\; L &\to L \\ a &\mapsto a^q \end{aligned}$$

$\langle Fr_q\rangle = \mathrm{Aut}_K(L)$, $|\mathrm{Aut}_K(L)| = n$.

Beweis:

$$F_p \subset K = F_q = F_{p^r} \subset L = F_{q^n} = F_{p^{r\cdot n}}$$

$\mathrm{Fix}(Fr^r) = K$ wegen 4.6.11

$\mathrm{Aut}(L) \overset{4.6.13}{=} \langle Fr\rangle$, $|\mathrm{Aut}(L)| = n \cdot r$. Wie in 4.6.11 ist $L^* = \langle\alpha\rangle$, $K^* = \langle\beta\rangle$ mit $\beta = \alpha^{\frac{p^{rn}-1}{p^r-1}}$ und $\mathrm{ord}(\beta) = p^r - 1$
$\Rightarrow\; Fr^j \notin \mathrm{Aut}_K(L)$ für $j < r$ (denn $\beta^{pj-1} \neq 1 \;\Rightarrow\; \beta^{pj} = Fr^j(\beta) \neq \beta$) aber $Fr^r \in \mathrm{Aut}_K(L)$, also $\mathrm{Aut}_K(L) = \langle Fr^r\rangle$. □

Bemerkung:

Damit erhalten wir Bijektionen

$$\begin{aligned} \{\text{Teiler von } n\} &\overset{1:1}{\leftrightarrow} \{\text{Zwischenkörper } K \subset M \subset L\} \\ s &\mapsto \mathrm{Fix}\left(Fr_q^s\right) \cong F_{q^s} \end{aligned}$$

denn $q^n = p^{rn}$ und die Zwischenkörper kommen von Teilern von rn, die Vielfache von r sind.

$$\begin{aligned} \{\text{Teiler von } n\} &\overset{1:1}{\leftrightarrow} \{\text{Untergruppen von } \mathrm{Aut}_K(L)\} \\ s &\mapsto \langle Fr_q^s\rangle \end{aligned}$$

da $\mathrm{Aut}_K(L)$ zyklisch der Ordnung n.

Zusammen ergibt sich damit:

4.6.15 Hauptsatz der Galoistheorie für endliche Körper

Sei $K \subset L$ eine Erweiterung endlicher Körper. Dann ist

$$\begin{aligned} \{\text{Untergruppen von } \mathrm{Aut}_K(L)\} &\overset{1:1}{\leftrightarrow} \{\text{Zwischenkörper } K \subset M \subset L\} \\ U &\mapsto \mathrm{Fix}(U) \\ \mathrm{Aut}_M(L) &\hookleftarrow M \end{aligned}$$

eine Bijektion.

Außerdem gilt:

$$\mathrm{Aut}_K(L) \big/ \mathrm{Aut}_M(L) \cong \mathrm{Aut}_K(M)$$

Beweis:

$K = F_q$, $L = F_{q^n}$, die Bijektion folgt aus der vorangegangenen Bemerkung.

Genauer: Sei M ein Zwischenkörper, $K \subset M \subset L$.

Da $q = p^r$ ist $F_p \subset K \subset M \subset L$

$\Rightarrow M$ ist Zwischenkörper von $F_p \subset L$

$\Rightarrow M$ ist von der Form $\left(Fr_p^{s'}\right)$ (4.6.11) und hat $p^{s'}$ Elemente, wobei s' Teiler von rn ist, denn L hat $q^n = p^{rn}$ Elemente.

Da $K \subset M$ muss M q^s Elemente haben für ein s

$\Rightarrow q^s = p^{rs} = p^{s'}$
$\Rightarrow s'$ ist ein Teiler von rn, der Vielfaches von r ist.
$\Rightarrow s$ ist ein Teiler von n.

Umgekehrt können wir für jeden Teiler s von n den Teiler rs von rn betrachten und erhalten mit 4.6.11 einen Körper

$$M = \mathrm{Fix}\left(Fr_p^{rs}\right) = \mathrm{Fix}\left(Fr_q^{s}\right)$$

mit $F_p \subset M \subset L$, da außerdem $K = \mathrm{Fix}\left(Fr_p^{r}\right) = \mathrm{Fix}(Fr_q)$ gilt $K \subset M$.

Aus 4.6.14 folgt $\mathrm{Aut}_K(L) = \langle Fr_q \rangle$ ist zyklisch der Ordnung n, die Untergruppen von $\mathrm{Aut}_K(L)$ sind also genau die $\langle Fr_q^s \rangle$ mit $s \mid n$.

Für einen Zwischenkörper $K \subset M \subset L$ gilt dabei:

$$\mathrm{Aut}_K(L) \big/ \mathrm{Aut}_M(L) = \langle Fr_q \rangle \big/ \langle Fr_q^s \rangle \overset{*}{\cong} \mathbb{Z}_n \big/ \mathbb{Z}_{\frac{n}{s}} \cong \mathbb{Z}_s \cong \mathrm{Aut}_K(M),$$

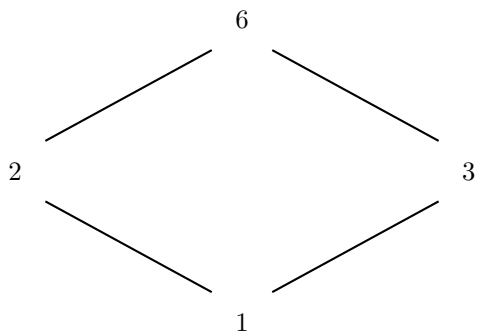
denn mit $K = F_q, M = F_{qs}$ ist $\mathrm{Aut}_K(L)$ zyklisch der Ordnung s.
Erklärung zu $*$: Die Untergruppe $\langle \text{Erzeuger}^s \rangle$ ist zyklisch der Ordnung $\text{Gruppenordnung} \big/ s$. □

Beispiel:

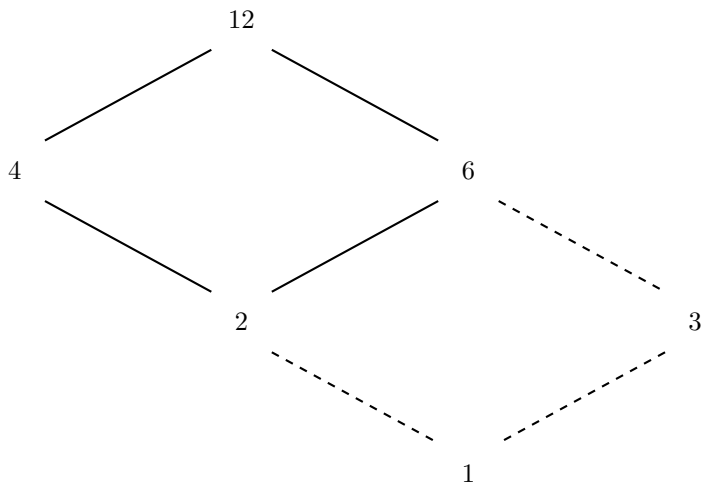
$q = 4$, $n = 6$: $p = 2$, $q = 2^2$, $q^6 = 4^6 = 2^{12}$.

Teiler von 6: 1, 2, 3, 6

Wir zeichnen ein Unterkörper-, Untergruppen- und Teilerdiagramm (Wir fassen diese wie im obigen Beweis als Teiler von 12 auf, die Vielfache von 2 sind):



gestrichelt: weitere Teiler von 12



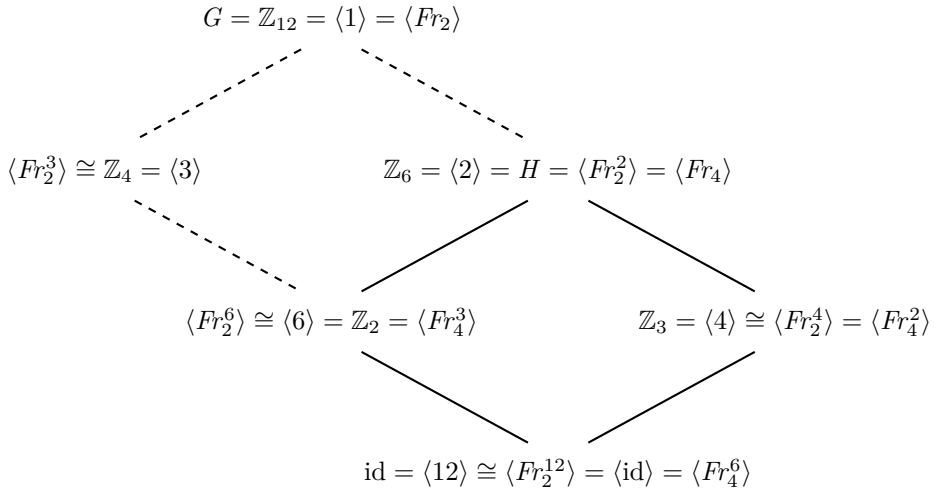
$\mathrm{Aut}_K(L) \cong \mathbb{Z}_6, \mathrm{Aut}_K(L) \subset \mathrm{Aut}_{F_2}(L) \cong \mathbb{Z}_{12}, G = \mathrm{Aut}_{F_2}(L)$ wird erzeugt von Fr_2, das heißt

$$\begin{array}{c} \mathrm{Aut}_{F_2} \xrightarrow{\cong} \mathbb{Z}_{12} \\ Fr_2 \mapsto 1 \end{array}$$

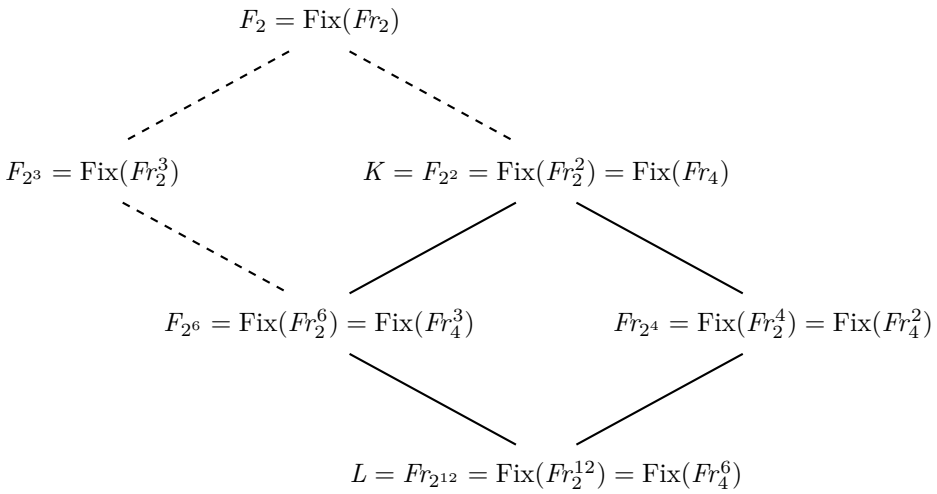
$H = \mathrm{Aut}_K(L)$ ist erzeugt von $Fr_2^2 = Fr_4$.

$$\begin{array}{lccc} \Rightarrow & H = \mathrm{Aut}_K(L) & \subset & \mathrm{Aut}_{F_2}(L) = G \\ & \| & & \| \\ & \mathbb{Z}_6 \cong \langle 2 \rangle & \subset & \mathbb{Z}_{12} \end{array}$$

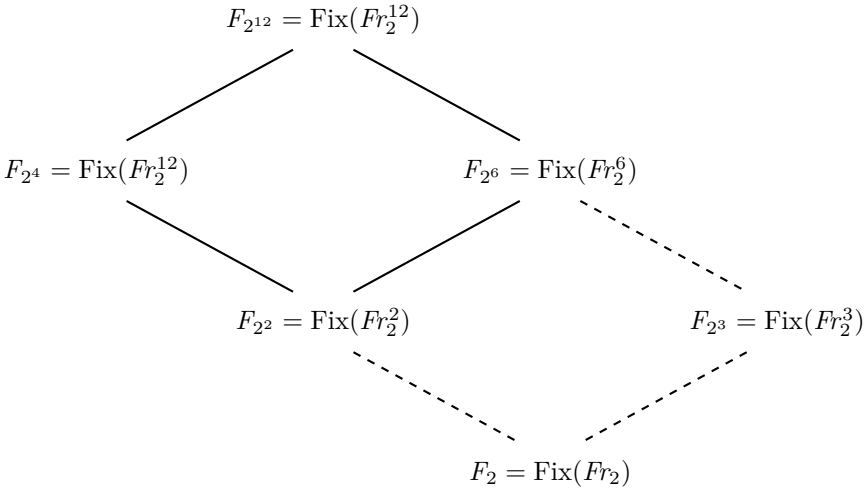
Untergruppen der $\mathbb{Z}_{12}$, die auch Untergruppen der $\mathbb{Z}_6 \cong \langle 2 \rangle \subset \mathbb{Z}_{12}$ sind:



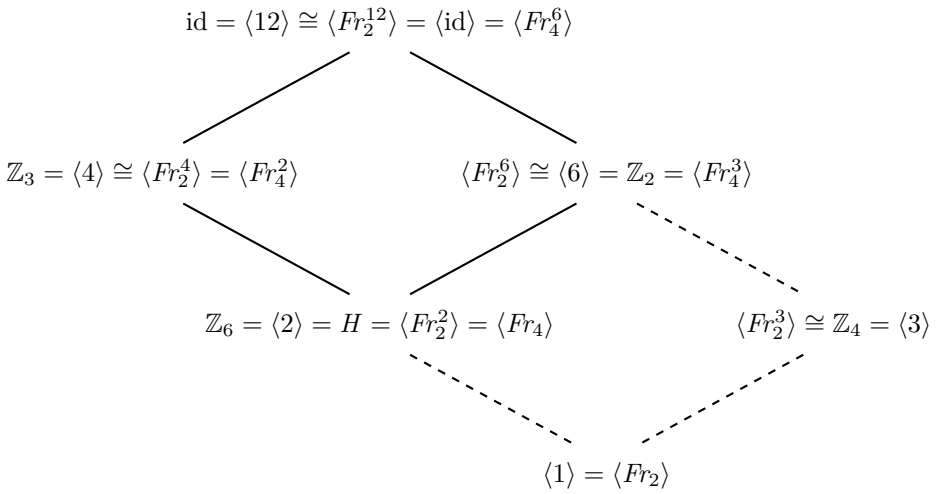
Das dazugehörige Zwischenkörperdiagramm (gestrichelt: Zwischenkörper von $F_2 \subset L$, die nicht Zwischenkörper von $K \subset L$ sind).
Achtung: Dieses Diagramm ist von oben nach unten zu lesen (d.h. oben steht der kleinste Körper, unten der größte), wenn man es analog zum Untergruppendiagramm betrachten will (mit id unten, G oben), denn „je größer die Gruppe, desto kleiner der Fixkörper “



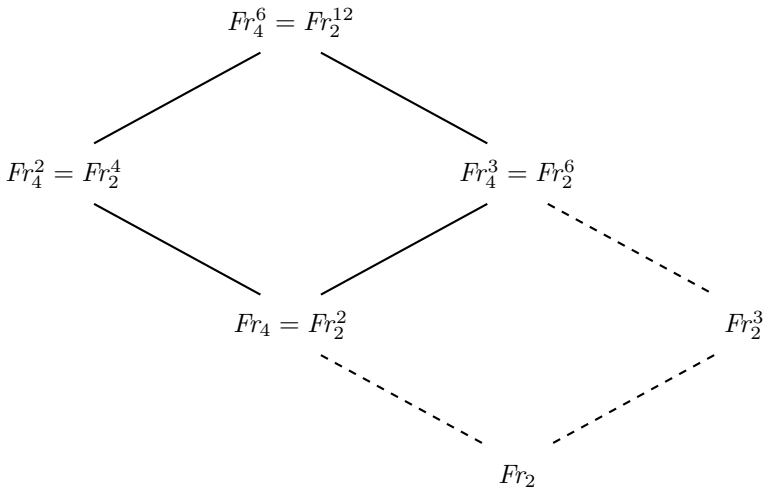
Wenn man das Unterkörperdiagramm von unten nach oben (von kleinsten zum größten Körper) sympathischer findet, dreht man es um:



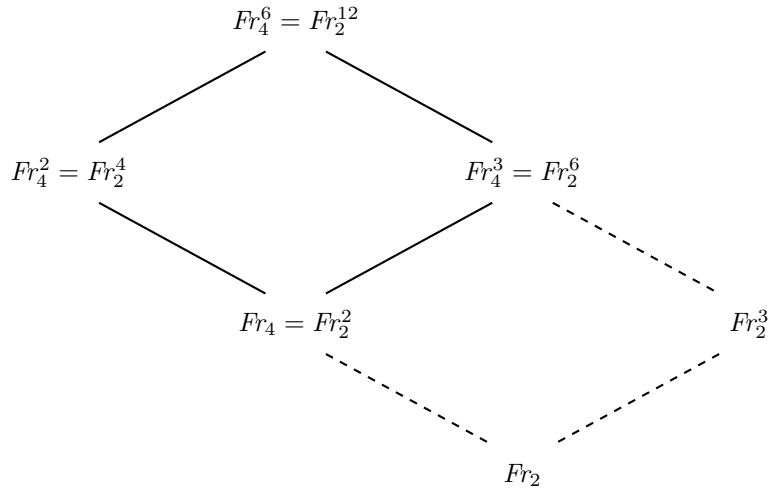
Dann passt es so nicht mehr zum Untergruppendiagramm, aber das Untergruppendiagramm lässt sich hier auch in sinnvoller Weise umdrehen, indem wir zu einem Teiler $d \mid n$ nicht die Untergruppe der Ordnung d listen, sondern die Untergruppe der Ordnung $\frac{n}{d}$, die von $d \cdot 1^{=}(\text{Erzeuger})^d$ erzeugt wird (gestrichelt: alle Untergruppen der $\mathbb{Z}_{12}$):

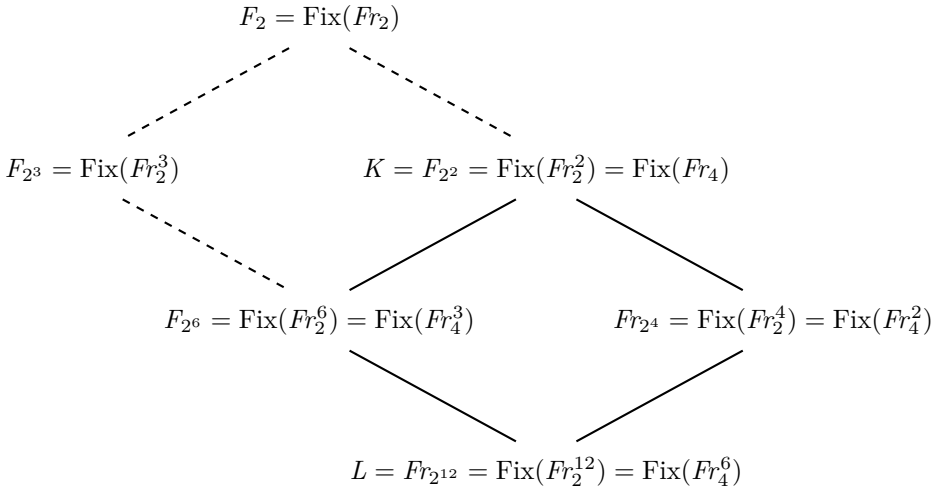


oder kurz gefasst:



Damit kann man sich das (umgedrehte) Untergruppendiagramm und das Zwischenkörperdiagramm nebeneinander halten und sehen, dass es dasselbe ist:





4.7 Die Galoiskorrespondenz

4.7.1 Satz vom primitiven Element

Jede endliche separable Körpererweiterung ist einfach.

Beweis:

Wir wissen bereits, dass für endliche Körper jede endliche Erweiterung einfach ist (4.6.9).
Sei nun $|K| = \infty$

Behauptung: Falls $K \subset K[\alpha_1, \beta_1]$, so ist die Erweiterung einfach. Dann folgt die Aussage des Satzes mit Induktion.

Seien f, g die Minimalpolynome von α_1, β_1 vom Grad d bzw. e. Da f und g separabel sind, gibt es im Zerfällungskörper (4.6.3) von $f \cdot g$ d verschiedene Nullstellen $\alpha_1, ..., \alpha_d$ von f und e verschiedene Nullstellen $\beta_1, ..., \beta_e$ von g.

Da $|K| = \infty$ $\exists \lambda \in K$ mit $\lambda \neq \frac{\alpha_i - \alpha_1}{\beta_1 - \beta_j}$ $\forall\ 1 \leqslant i \leqslant d, 2 \leqslant j \leqslant e$.
Setze $\gamma = \alpha_1 + \lambda\beta_1$

Behauptung: $K[\alpha_1, \beta_1] = K[\gamma]$

„$\subseteq$“ ist klar

„$\supseteq$“ Sei $h = f(\gamma - \lambda x) \in K[\gamma][x]$

Dann ist $h(\beta_1) = f(\gamma - \lambda\beta_1) = f(\alpha_1) = 0$.
Das Minimalpolynom von β_1 über $K[\gamma]$ ist also ein Teiler von h und von g. Dabei können h und g, außer β_1 keine weitere gemeinsame Nullstelle haben, denn wäre $h(\beta_j) = 0$ für $j \geqslant 2$, so gilt für ein i:

$$\begin{aligned} & 0 = f(\alpha_i) = f(\gamma - \lambda\beta_j) = h(\beta_j) \\ \Rightarrow\ & \alpha_i = \gamma - \lambda\beta_j = (\alpha_1 + \lambda\beta_1) - \lambda\beta_j = \alpha_1 + \lambda(\beta_1 - \beta_j) \\ \Rightarrow\ & \frac{\alpha_i - \alpha_1}{\beta_1 - \beta_j} = \lambda \quad \lightning \end{aligned}$$

Damit hat das Minimalpolynom von β_1 über $K[\gamma]$ den Grad 1.

$$\begin{aligned} &\Rightarrow \beta_1 \in K[\gamma] \\ &\Rightarrow \alpha_1 = \gamma - \lambda\beta_1 \in K[\gamma] \end{aligned}$$

□

4.7.2 Lemma

Sei $U \subset \mathrm{Aut}(L)$ eine endliche Untergruppe und $\alpha \in L$. Dann ist α algebraisch über $\mathrm{Fix}(U)$ mit seperablem Minimalpolynom

$$f = \prod_{\beta \in U_\alpha} (x - \beta) \in \mathrm{Fix}(U)[x]$$

Hierbei ist U_α die Bahn von α unter der Operation von U (Insbesondere gilt also $\varphi(\tilde{\varphi}(\alpha) = (\varphi \circ \tilde{\varphi})(\alpha))$:

$$U_\alpha = \{\varphi(\alpha) \mid \varphi \in U\}$$

Beweis:

Wegen $f(\alpha) = 0$, für $\varphi \in U$ gilt:

$$\begin{aligned} \varphi(f) &= \prod_{\beta \in U_\alpha} (x - \varphi(\beta)) \\ &= \prod_{\beta \in U_\alpha} (x - \beta) \\ &= f \end{aligned}$$

denn φ permutiert die Elemente der Bahn.

$$\Rightarrow f \in \mathrm{Fix}(U)[x]$$

Dabei ist f normiert, separabel und wird vom Minimalpolynom $m_\alpha \in \mathrm{Fix}(U)[x]$ geteilt.
Es gilt:

$$m_\alpha(\varphi(\alpha)) = \varphi(m_\alpha(\alpha)) = m_\alpha(\alpha) = 0 \ \ \forall\ \varphi \in U$$

Somit sind alle $\beta \in U_\alpha$ Nullstellen von m_α.
Daraus folgt dann $m_\alpha = f$. □

4.7.3 Satz

Sei $K \subset L$ endlich und $U \subset \mathrm{Aut}_K(L)$ eine Untergruppe, dann ist $\mathrm{Fix}(U) \subset L$ eine einfache, normale und separable Erweiterung.

Beweis:

Für jedes $\alpha \in L$ ist $m_\alpha \in \mathrm{Fix}(U)[x]$ separabel. Mit 4.7.2 folgt dann $\mathrm{Fix}(U) \subset L$ ist separabel.
Wegen 4.7.1 ist $\mathrm{Fix}(U) \subset L$ einfach.

$\Rightarrow \exists\, \gamma \in L : L = \mathrm{Fix}(U)[\gamma]$

Sei $m_\gamma \in \mathrm{Fix}(U)[\gamma]$ das Minimalpolynom von γ. Aus 4.7.2 folgt:

$$m_\gamma = \prod_{\beta \in U_\gamma} (x - \beta)$$

und da gilt $\beta = \varphi(\gamma) \in L$ folgt m_γ zerfällt über L. Der Zerfällungskörper ist also in L enthalten. (Zerfällungskörper $\subset L$)
Der Zerfällungskörper von m_γ muss die Nullstellen von γ enthalten, also ist $L \subset$ Zerfällungskörper.

$\Rightarrow L =$ Zerfällungskörper von m_γ
$\overset{4.5.3}{\Rightarrow} \mathrm{Fix}(U) \subset L$ ist normal

□

4.7.4 Proposition

Sei $K \subset L$ endlich, $U \subset \mathrm{Aut}_K(L)$ eine Untergruppe. Dann gilt:

$$\mathrm{Aut}_{\mathrm{Fix}(U)}(L) = U$$

und

$$|U| = [L : \mathrm{Fix}(U)]$$

Beweis:

Nach 4.7.1 gilt es existiert $\gamma \in L$ mit $L = \mathrm{Fix}(U)[\gamma]$. Das Minimalpolynom m_γ von γ über $\mathrm{Fix}(U)$ hat den Grad $[L : \mathrm{Fix}(U)]$

$\overset{4.4.10}{\Rightarrow} |\mathrm{Aut}_{\mathrm{Fix}(U)}| \leqslant [L : \mathrm{Fix}(U)]$

Es gilt $U \subset \mathrm{Aut}_{\mathrm{Fix}(U)}(U)$, denn die Elemente aus U halten $\mathrm{Fix}(U)$ fest.
Mit 4.7.2 folgt

$$\begin{aligned} [L : \mathrm{Fix}(U)] = deg(m_\gamma) = |U_\gamma| \leqslant |U| \\ \Rightarrow |U| \leqslant |\mathrm{Aut}_{\mathrm{Fix}(U)}(L)| \leqslant [L : \mathrm{Fix}(U)] \leqslant |U| \\ \Rightarrow \text{Gleichheit und } U = \mathrm{Aut}_{\mathrm{Fix}(U)}(L) \end{aligned}$$

□

4.7.5 Definition: Galoiserweiterung

Eine endliche, normale, separable Körpererweiterung heißt Galoiserweiterung (galoisch).

Beispiel
Sei $\mathrm{char}(K) = 0$, $f \in K[x]$, $L =$ Zerfällungskörper von f. Dann ist $K \subset L$ Galoiserweiterung.

4.7.6 Lemma

Sei $K \subset L$ normal und endlich, $L \subset F$ eine Körpererweiterung.
Sei

$$\varphi : L \hookrightarrow F$$

ein Körpermonomorphismus mit $\varphi|_K = \mathrm{id}_K$, dann ist $\varphi \in \mathrm{Aut}_K(L)$

Beweis:

Wegen 4.5.4 ist L der Zerfällungskörper eines Polynoms $f \in K[x]$ und über L gilt:

$$f = a \cdot \prod (x - d_i)$$

und

$$L = K(\alpha_1, .., \alpha_n)$$

Sei $\varphi : L \to F$.
Da $f \in K[x]$ und $\varphi|_K = \mathrm{id}_K$ gilt, folgt:

$$\begin{aligned} & 0 = \varphi(0) = \varphi(f(\alpha_i)) = f(\varphi(\alpha_i)) \\ \Rightarrow\ & \varphi(\alpha_i) \in \{\alpha_1, ..., \alpha_n\} \ \ \forall\ i \\ \Rightarrow\ & \varphi : L \to L \end{aligned}$$

und

$$\varphi|_{\{\alpha_1,...,\alpha_n\}} : \{\alpha_1, ..., \alpha_n\} \to \{\alpha_1, ..., \alpha_n\}$$

da φ injektiv ist gilt:

$$\begin{aligned} & \varphi(\{\alpha_1, ..., \alpha_n\}) = \{\alpha_1, ..., \alpha_n\} \\ \Rightarrow\ & \forall\ i : \alpha_i \in Im(\varphi) \\ \Rightarrow\ & L \subset \mathrm{Im}(\varphi) \\ \Rightarrow\ & \varphi \in \mathrm{Aut}_K(L) \end{aligned}$$

□

4.7.7 Proposition

Sei $K \subset L$ eine Galoiserweiterung und $K \subset M \subset L$ ein Zwischenkörper.

Dann gilt $\mathrm{Fix}(\mathrm{Aut}_M(L)) = M$

Beweis:

Da alle M-Automorphismen M festhalten, gilt $M \subset \mathrm{Fix}(\mathrm{Aut}_M(L))$.

Sei $\alpha \in L \setminus M$ und $m_\alpha \in M[x]$ das Minimalpolynom, dann ist $deg(m_\alpha) \geqslant 2$.

Wegen 4.5.9 ist $M \subset L$ separabel, insbesondere ist m_α separabel.

Wegen 4.5.5 ist $M \subset L$ normal, insbesondere ist $M \subset L$ Galoiserweiterung.

Daher existieren $\beta \neq \alpha$, $\beta \in L$ mit β ist die Nullstelle von m_α. Es gilt:

$$\varphi : M[\alpha] \cong M[\beta]$$

Da $M[\alpha] \subset L$ wegen 4.5.9 separabel ist, existiert mit 4.7.1 γ mit $L = M[\alpha][\gamma]$.
Sei $m_\gamma \in M[\alpha][\gamma]$ das Minimalpolynom. Dann ist

$$\varphi' : L = M[\alpha][\gamma] \cong M[\alpha][x] \big/ \langle m_\gamma \rangle \cong M[\beta][x] \big/ \langle \varphi(m_\gamma) \rangle = M[\beta][\gamma']$$

ein Isomorphismus, wobei γ' eine Nullstelle von $\varphi(m_\gamma)$ ist.

Damit ist

$$\psi : L \xrightarrow{\psi'} M[\beta][\gamma'] \subset M[\gamma']$$

ein Körpermonomorphismus mit $\psi|_K = \mathrm{id}_K$ und $K \subset L$ ist normal. Dann folgt mit 4.7.6 $\psi \in \mathrm{Aut}_M(L)$.

Wir erhalten so mit einen Automorphismus

$$\psi : L \to L$$

der α nicht festhält, aber M.

$\Rightarrow \alpha \notin \mathrm{Fix}_{\mathrm{Aut}_M(L)}(L)$
$\Rightarrow \mathrm{Fix}_{\mathrm{Aut}_M(L)}(L) \subset M$
$\Rightarrow \mathrm{Fix}_{\mathrm{Aut}_M(L)}(L) = M$

□

4.7.8 Korollar

$$K \subset L \text{ Galoiserweiterung} \Leftrightarrow \mathrm{Fix}(\mathrm{Aut}_K(L)) = K$$

Beweis:

„⇒“ 4.7.7

„⇐“ 4.7.3 (Fix(U)$\subset L$ ist Galoiserweiterung)

□

4.7.9 Hauptsatz der Galoistheorie

Sei $K \subset L$ Galoiserweiterung.

1.
$$\{\text{Untergruppe von } \mathrm{Aut}_K(L)\} \overset{1:1}{\leftrightarrow} \{\text{Zwischenkörper von } K \subset L\}$$
$$U \mapsto \mathrm{Fix}(U)$$
$$\mathrm{Aut}_M(L) \hookleftarrow M$$

2. $|\mathrm{Aut}_M(L)| = [L : M]$

3. $M \subset L$ ist Galoiserweiterung

4.
$$K \subset M \text{ ist Galoiserweiterung } \Leftrightarrow \mathrm{Aut}_M(L) \subset \mathrm{Aut}_K(L) \text{ Normalteiler}$$

und dann gilt

$$\mathrm{Aut}_K(M) \cong {}^{\mathrm{Aut}_K(L)}\!/_{\mathrm{Aut}_M(L)}$$

Beweis:

1. Wegen 4.7.4 gilt $U = \mathrm{Aut}_{\mathrm{Fix}(U)}(L)$, wegen, 4.7.7 gilt $\mathrm{Fix}(\mathrm{Aut}_M(L))= M$. Daraus folgt, die beiden Abbildungen,
$$U \mapsto \mathrm{Fix}(U)$$
und
$$M \mapsto \mathrm{Aut}_M(L)$$
sind invers zueinander und liefern, daher die Bijektion.

2. Folgt aus 4.7.4, da jeder Zwischenkörper ein Fixkörper ist.

3. $M \subset L$ ist endlich, normal (mit 4.5.5) und separabel (mit 4.5.9)

4. „⇐“ Wegen 4.5.9 ist $K \subset M$ separabel.
$K \subset M$ ist endlich.

   Behauptung: $K \subset M$ ist normal

   Sei $g \in K[x]$ irreduzibel mit Nullstelle $\alpha \in M$. Da $K \subset L$ normal, zerfällt G über L in Linearfaktoren.
   Sei $\beta \in L$ eine Nullstelle.
   Wir zeigen $\beta \in \mathrm{Fix}(Aut_M(L)) = M$.
   Sei $\varphi \in Aut_M(L)$.
   Wie im Beweis von 4.7.7 existiert $\psi : L \to L$ mit $\psi|_K = \mathrm{id}_K$ und $\psi(\alpha) = \beta$. Es gilt:
$$\psi^{-1} \circ \varphi \circ \psi = \varphi' \in \mathrm{Aut}_M(L)$$
   ist ein Normalteiler, also
$$\varphi(\beta) = \varphi(\psi(\alpha)) = \psi(\varphi'(\alpha)) \overset{a \in M}{=} \psi(\alpha) = \beta$$
$$\Rightarrow \beta \in \mathrm{Fix}(\mathrm{Aut}_M(L))$$
   Damit ist $K \subset M$ normal und daher Galoiserweiterung.

„⇒“ Sei $K \subset M$ normal. Betrachte

$$\begin{aligned} \pi : \mathrm{Aut}_K(L) &\to \mathrm{Aut}_K(M) \\ \varphi &\mapsto \varphi \mid_M \end{aligned}$$

- Wohldefiniert, i.e. $\varphi\!\diagup_M : M \overset{\cong}{\to} M$ wegen Lemma 4.7.6
- Gruppenhomomorphismus
- $\mathrm{Kern}(\pi) = \{\varphi \mid \varphi|_M = \mathrm{id}\} = \mathrm{Aut}_M(L)$
- π ist surjektiv, da sich jeder Automorphismus von M zu einem von L erweitern lässt, da $M \subset L$ endlich

$\Rightarrow$ $\mathrm{Aut}_M(L)$ ist Normalteiler also Kern eines Gruppenhomomorphismus und
$\mathrm{Aut}_K(L)\!\diagup_{\mathrm{Aut}_M(L)} = \mathrm{Aut}_K(L)\!\diagup_{\mathrm{Kern}(\pi)} \cong \mathrm{Im}(\pi) = \mathrm{Aut}_K(L)$

□

4.7.10 Korollar:

Sei $K \subset L$ endlich.

$$K \subset L \text{ ist Galoiserweiterung } \Leftrightarrow |\mathrm{Aut}_K(L)| = [L : K]$$

Beweis:

„⇒“ Aus dem Hauptsatz der Galoistheorie 4.7.9 2)

„⇐“ Sei $F = \mathrm{Fix}(\mathrm{Aut}_K(L))$.

Aus M 4.7.4 folgt:

$$\begin{aligned} \mathrm{Aut}_F(L) &= \mathrm{Aut}_{\mathrm{Fix}(\mathrm{Aut}_K(L))}(L) \\ &= \mathrm{Aut}_K(L). \end{aligned}$$

und

$$\begin{aligned} |\mathrm{Aut}_K(L)| &= [L : \mathrm{Fix}(\mathrm{Aut}_K(L))] \\ &= [L : K] \end{aligned}$$

Es gilt:

$$\begin{aligned} [L : F] \cdot [F : K] &= [L : K] \\ &= |\mathrm{Aut}_K(L)| \\ &= |\mathrm{Aut}_F(L)| \\ &= [L : F] \end{aligned}$$

$\Rightarrow [F : K] = 1$

$\Rightarrow K = F$

$\overset{4.7.3}{\Rightarrow}$ $K \subset L$ ist Galoiserweiterung □

4.7.11 Korollar:

Sei $K \subset L$ endlich.

$$K \subset L \text{ ist Galoiserweiterung } \Leftrightarrow L \text{ ist Zerfällungskörper eines separablen Polynoms } f \in K[x]$$

Beweis:

„⇒“ $K \subset L$ ist normal.

$\overset{4.5.4}{\Rightarrow}$ L ist Zerfällungskörper eines Polynoms $f \in K[x]$.

Sei $f = c \cdot f_1 \cdots f_r$ mit normierten irreduziblen Faktoren f_i.

Sei $\alpha_i \in L$ eine Nullstelle von f_i.

Dann ist f_i das Minimalpolynom von α_i, und da $K \subset L$ separabel ist, ist jedes f_i separabel und damit f.

„⇐ “ Aus 4.5.4 folgt $K \subset L$ normal.

Aus 4.4.10 folgt $|\mathrm{Aut}_K(L)| = [L : K]$ und mit 4.7.10 daher $K \subset L$ ist Galoiserweiterung. □

4.7.12 Beispiel:

Sei $f = x^4 - 2 \in \mathbb{Q}[x]$ und L der Zerfällungskörper.

$\mathbb{Q} \subset L$ ist Galoiserweiterung.

Die Nullstellen von f sind:

$$\begin{aligned}\alpha_1 &= \sqrt[4]{2}\\ \alpha_2 &= i \cdot \sqrt[4]{2}\\ \alpha_3 &= -\sqrt[4]{2}\\ \alpha_4 &= -i \cdot \sqrt[4]{2}\end{aligned}$$

und

$$\begin{aligned}L &= \mathbb{Q}(\alpha_1, \ldots, \alpha_4)\\ &= \mathbb{Q}[i, \sqrt[4]{2}].\end{aligned}$$

Man erhält aus 4.7.10:

$$\begin{aligned}|\operatorname{Aut}_{\mathbb{Q}}(L)| &= [L : \mathbb{Q}]\\ &= \left[L : \mathbb{Q}\left[\sqrt[4]{2}\right]\right] \cdot \left[\mathbb{Q}\left[\sqrt[4]{2}\right] : \mathbb{Q}\right]\\ &= 2 \cdot 4 = 8,\end{aligned}$$

da $x^4 - 2$ das Minimalpolynom von $\sqrt[4]{2}$ über $\mathbb{Q}$ ist und $x^2 + 1$ das von i über $\mathbb{Q}[\sqrt[4]{2}]$.

Ein $\mathbb{Q}-$Automorphismus muss Nullstellen der Minimalpolynome auf Nullstellen abbilden, somit gibt es folgende Möglichkeiten:

$$\begin{array}{cccccccccc} i & \mapsto & i & i & i & i & -i & -i & -i & -i\\ \sqrt[4]{2} & \mapsto & \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 & \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4\\ & & \varphi_1 & \varphi_2 & \varphi_3 & \varphi_4 & \varphi_5 & \varphi_6 & \varphi_7 & \varphi_8 \end{array}$$

Es gilt: $\varphi_1 = \mathrm{id}$.

Um $\operatorname{Aut}_{\mathbb{Q}}(L) \subset \mathbb{S}_4$ darzustellen, bestimmen wir die Operation der φ_i auf der Nullstellenmenge $\{\alpha_1, \ldots, \alpha_4\}$:

$$\begin{aligned}\varphi_1 &= \mathrm{id}\\ \varphi_2 : \alpha_1 &\mapsto \alpha_2 = i\sqrt[4]{2},\\ \alpha_2 &\mapsto ii\sqrt[4]{2} = -\sqrt[4]{2} = \alpha_3\\ \alpha_3 &\mapsto -i\sqrt[4]{2} = \alpha_4\\ \alpha_4 &\mapsto -i \cdot i\sqrt[4]{2} = \alpha_1\\ \Rightarrow \varphi_2 &= (1\ 2\ 3\ 4)\\ \varphi_3 : \alpha_1 &\mapsto \alpha_3 = -\sqrt[4]{2}\\ \alpha_2 &\mapsto i(-\sqrt[4]{2}) = -i\sqrt[4]{2} = \alpha_4\\ \alpha_3 &\mapsto -(-\sqrt[4]{2}) = \alpha_1\\ \alpha_4 &\mapsto -(-i\sqrt[4]{2}) = i\sqrt[4]{2} = \alpha_2\\ \Rightarrow \varphi_3 &= (1\ 3)(2\ 4)\\ \varphi_4 : \alpha_1 &\mapsto \alpha_4 = -i\sqrt[4]{2}\\ \alpha_2 &\mapsto i(-i\sqrt[4]{2}) = \sqrt[4]{2} = \alpha_1\\ \alpha_3 &\mapsto -(-i\sqrt[4]{2}) = \alpha_2\\ \alpha_4 &\mapsto -i(-i\sqrt[4]{2}) = -\sqrt[4]{2} = \alpha_3\\ \Rightarrow \varphi_4 &= (1\ 4\ 3\ 2)\\ \varphi_5 : \alpha_1 &\mapsto \alpha_1 = \sqrt[4]{2}\\ \alpha_2 &\mapsto -i\sqrt[4]{2} = \alpha_4\\ \alpha_3 &\mapsto -\sqrt[4]{2} = \alpha_3\\ \alpha_4 &\mapsto i\sqrt[4]{2} = \alpha_2\\ \Rightarrow \varphi_5 &= (2\ 4)\end{aligned}$$

$$
\begin{aligned}
\varphi_6 : \alpha_1 &\mapsto \alpha_2 = i\sqrt[4]{2} \\
\alpha_2 &\mapsto (-i)(i\sqrt[4]{2}) = \sqrt[4]{2} = \alpha_1 \\
\alpha_3 &\mapsto -i\sqrt[4]{2} = \alpha_4 \\
\alpha_4 &\mapsto -(-i)(i\sqrt[4]{2}) = -\sqrt[4]{2} = \alpha_3 \\
\Rightarrow \varphi_6 &= (1\ 2)(3\ 4) \\
\varphi_7 : \alpha_1 &\mapsto \alpha_3 = -\sqrt[4]{2} \\
\alpha_2 &\mapsto (-i)(-\sqrt[4]{2}) = i\sqrt[4]{2} = \alpha_2 \\
\alpha_3 &\mapsto \sqrt[4]{2} = \alpha_1 \\
\alpha_4 &\mapsto -(-i)(-\sqrt[4]{2}) = -i\sqrt[4]{2} = \alpha_4 \\
\Rightarrow \varphi_7 &= (1\ 3) \\
\varphi_8 : \alpha_1 &\mapsto \alpha_4 = -i\sqrt[4]{2} \\
\alpha_2 &\mapsto (-i)(-i\sqrt[4]{2}) = -\sqrt[4]{2} = \alpha_3 \\
\alpha_3 &\mapsto -(-i\sqrt[4]{2}) = i\sqrt[4]{2} = \alpha_2 \\
\alpha_4 &\mapsto -(-i)(-i\sqrt[4]{2}) = \sqrt[4]{2} = \alpha_1 \\
\Rightarrow \varphi_8 &= (1\ 4)(2\ 3)
\end{aligned}
$$

$$
\begin{aligned}
\Rightarrow \mathrm{Aut}_{\mathbb{Q}}(L) &= \{\mathrm{id}, (1\ 3), (2\ 4), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3), (1\ 2\ 3\ 4), (1\ 4\ 3\ 2)\} \\
&= \mathrm{Sym}(\text{Quadrat}) \\
&= \mathrm{Sym}\left(\begin{array}{cc} 1 & 4 \\ 2 & 3 \end{array}\right) = \mathrm{Sym}\left(\begin{array}{cc} \alpha_1 & \alpha_4 \\ \alpha_2 & \alpha_3 \end{array}\right)
\end{aligned}
$$

Wobei die Automorphismen mit

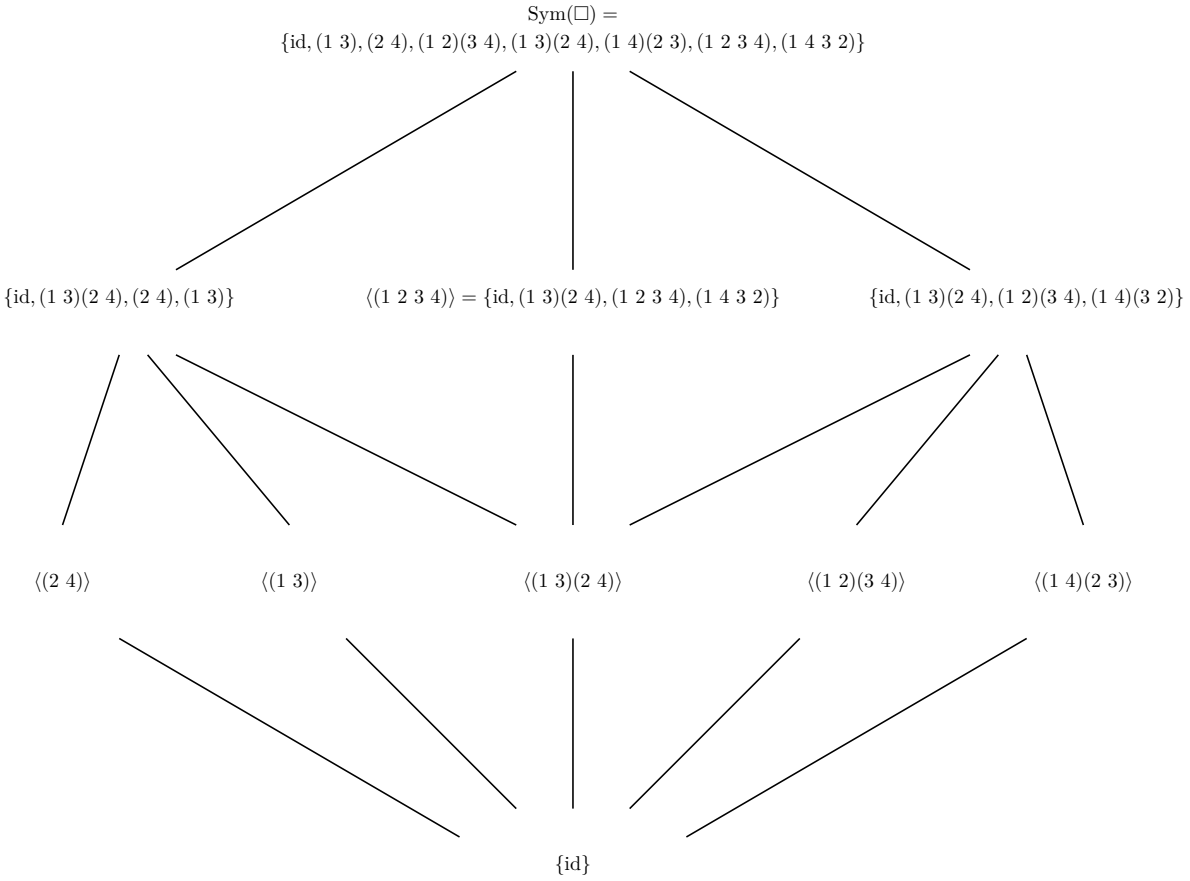
$$i \mapsto -i$$

genau die Spiegelungen sind und die mit

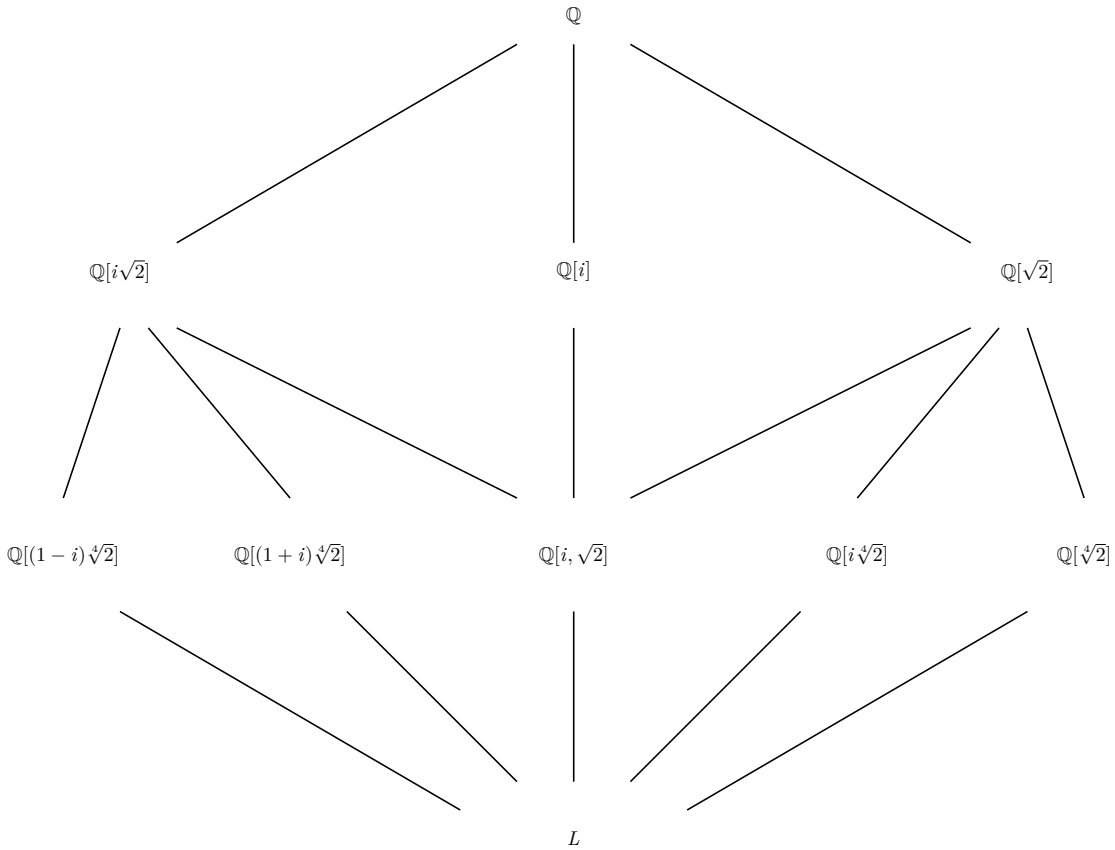
$$i \mapsto i$$

genau die Drehungen.

Untergruppenverband der Sym$\left(\begin{array}{cc} 1 & 4 \\ 2 & 3 \end{array}\right)$:



Zwischenkörperverband von $\mathbb{Q} \subset L$:



5 Anwendungen

5.1 Der Fundamentalsatz der Algebra

5.1.1 Lemma:

1) $\mathbb{R}$ besitzt keine Körpererweiterung von ungeradem Grad $n > 1$.

2) $\mathbb{C}$ besitzt keine Körpererweiterung vom Grad 2

Beweis

1. Sei $\mathbb{R} \subset L$ eine Körpererweiterung vom Grad n. Wegen 4.5.10 ist $\mathbb{R} \subset L$ separabel.

   Aus dem Satz vom primitiven Elementen 4.7.1 folgt:

   $$\exists\, \alpha \in L:\ L = \mathbb{R}(\alpha), \text{ und das Minimalpolynom } m_\alpha \in \mathbb{R}[x] \text{ ist irreduzibel von ungeradem Grad } n.$$

   Dann gilt

   $$\lim_{x \to -\infty} m_\alpha(x) = -\infty,$$
   $$\lim_{x \to \infty} m_\alpha(x) = \infty.$$

   Aus dem Zwischenwertsatz folgt, dass m_α eine Nullstelle in $\mathbb{R}$ hat. Da m_α irreduzibel ist, muss damit $m_\alpha = x - \alpha$ Grad 1 haben.

2. Wäre $\mathbb{C} \subset L$ vom Grad 2, so wäre wie vorher

   $$L = \mathbb{C}(\alpha) \text{ und } m_\alpha = x^2 + px + p \in \mathbb{C}[x].$$

   Dann hat m_α aber die Nullstelle

   $$x = -\frac{p}{2} \pm \sqrt{\frac{p^2}{4} - q} \in \mathbb{C}$$

   und zerfällt in Linearfaktoren $\lightning$

5.1.2 Lemma:

Sei $K \subset L$ eine Galoiserweiterung und $p^k \mid [L : K]$ für eine Primzahl p, dann $\exists$ Zwischenkörper $K \subset N \subset L$ mit

$$[L : N] = p^k$$

Beweis:

Nach dem Hauptsatz der Galoistheorie gilt

$$[L : K] = |\operatorname{Aut}_K(L)| \text{ also } p^k \mid |\operatorname{Aut}_K(L)|$$

Nach Satz 1.5.4 $\exists$ Untergruppe $H \subset \operatorname{Aut}_K(L)$ mit $|H| = p^k$, und nach dem Hauptsatz der Galoistheorie damit

$$N = \operatorname{Fix}(H) \text{ mit } K \subset N \subset L$$

und

$$[L : N] = |\operatorname{Aut}_N(L)| = |H| = p^k$$

□

5.1.3 Fundamentalsatz der Algebra

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

Beweis.

Sei $f \in \mathbb{C}[x]$ ein nicht konstantes Polynom und L der Zerfällungskörper von f.

Es gilt $\mathbb{R} \subset \mathbb{C} \subset L$, und $\mathbb{R} \subset L$ ist endlich und separabel (4.7.1, Satz von primitiven Element).

$$\Rightarrow L = \mathbb{R}(\alpha) \text{ für ein } \alpha \in L$$

Sei m_α das Minimalpolynom von α über $\mathbb{R}$ und M der Zerfällungskörper von m_α.

$\mathbb{R} \subset M$ ist endlich, normal (4.5.3) und separabel (4.5.10), also eine Galoiserweiterung.

$$\begin{aligned} &\mathbb{R} \subset \mathbb{C} \subset L = \mathbb{R}(\alpha) \subset M \\ \Rightarrow\ & 2 = [\mathbb{C} : \mathbb{R}] \ \Big|\ [M : \mathbb{R}] \\ \overset{*}{\Rightarrow}\ & 2 \ \Big|\ |\operatorname{Aut}_{\mathbb{R}}(M)| \end{aligned}$$

*Hauptsatz der Galoistheorie

Nach Satz 1.5.4 $\exists$ 2-Sylowgruppe $H \subset \operatorname{Aut}_{\mathbb{R}}(M)$ und nach dem Hauptsatz der Galoistheorie

$$N = \operatorname{Fix}(M) \text{ mit } \operatorname{Aut}_N(M) = H$$

und

$$[M : N] = |\operatorname{Aut}_N(M)| = |H|$$

Da $\mathbb{R} \subset N \subset M$ folgt

$$\begin{aligned} &[\mathbb{R} : N] \cdot [M : N] = [M : \mathbb{R}] \\ \Rightarrow\ & [\mathbb{R} : N] \cdot |H| = [M : \mathbb{R}] = |\operatorname{Aut}_{\mathbb{R}}(M)| \end{aligned}$$

Da H 2−Sylowgruppe in $\operatorname{Aut}_{\mathbb{R}}(M)$ folgt $[\mathbb{R}\colon N]$ ist ungerade.

Mit Lemma 5.1.2 2) folgt dann $N = \mathbb{R}$.

$$\begin{aligned} &\Rightarrow [M\colon \mathbb{R}] = |H| = 2^k \\ &\Rightarrow [M\colon \mathbb{C}] = {}^{[M\colon \mathbb{R}]}\!/_{[M\colon \mathbb{C}]} = 2^{k-1} \end{aligned}$$

Wäre also $k \geq 2$, so wäre $\mathbb{C} \subset M$ endlich, separabel und normal (4.5.5), also Galoiserweiterung.

Mit Lemma 5.1.2 $\exists$ dann ein Zwischenkörper $\mathbb{C} \subset N' \subset M$ mit $[N'\colon \mathbb{C}] = 2$ $\lightning$ zu Lemma 5.1.1 1) .

$$\begin{aligned} &\Rightarrow k = 1 \\ &\Rightarrow M = \mathbb{C}, \text{ da } \mathbb{R} \subset \mathbb{C} \subset L \subset M \text{ auch } L = \mathbb{C} \end{aligned}$$

Damit zerfällt f aber schon über $\mathbb{C}$ in Linearfaktoren und $\mathbb{C}$ ist algebraisch abgeschlossen. □

5.2 Auflösbarkeit polynomischer Gleichungen

Sei $f = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ ein Polynom in $\mathbb{C}[x]$.

Wir möchten die Nullstellen von f durch die Koeffizienten ausdrücken.

5.2.1 Beispiel

- $n = 1$: $f = x + a_0$, $-a_0$ ist Nullstelle.
- $n = 2$: $f = x^2 + px + q$, Nullstellen sind $-\frac{p}{2} \pm \sqrt{\frac{p^2}{4} - q}$
- $n = 3$ die Formeln von **Cardano**:

  Setze

  $$g = f(x - \frac{a_2}{3}) = x^3 + px + q$$

  mit $p = a_1 - \frac{a_2^2}{3}$, $q = a_0 - \frac{a_1 a_2}{3} + \frac{2a_2^3}{27}$.

  Ist $p = 0$, so sind die 3. Wurzeln aus q die Nullstellen.

  Ist $p \neq 0$, setze $x = u + v$ mit $u \neq 0$ und $v = -\frac{p}{3u}$.

  Aus $g(x) = 0$ wird

  $$u^3 + v^3 + 3uv(u + v) + p(u + v) + q = 0$$

  $$\Rightarrow u^3 + v^3 + q = 0$$
  $$\Rightarrow u^3 + q - \frac{p^3}{27u^3} = 0$$
  $$\Rightarrow u^6 + qu^3 - \frac{p^3}{27}$$
  $$\Rightarrow u^3 = -\frac{q}{2} \pm \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}$$

  Sei $u \in \mathbb{C}$ eine dritte Wurzel auf der rechten Seite, so gilt mit $v = -\frac{p}{3u}$, dass $u + v$ eine Lösung von $g(x) = 0$ ist.
- $n = 4$ so ähnlich.

5.2.2 Definition: Radikalerweiterung

1) Eine Körpererweiterung $K \subset L$ heißt Radikalerweiterung, wenn $L = K(\alpha_1, \ldots, \alpha_n)$ und $\alpha_i^{k_i} \in K(\alpha_1, \ldots, \alpha_{i-1})$ für ein $k_i \geq 2$.
2) Eine Radikalerweiterung heißt abelsch, wenn $K(\alpha_1, \ldots, \alpha_{i-1}) \subset K(\alpha_1, \ldots, \alpha_i)$ eine Galoiserweiterung mit abelscher Galoisgruppe ist $\forall i = 2, \ldots, n$.
3) $f \in K[x]$ heißt durch Radikale auflösbar über K, wenn es eine Radikalerweiterung $K \subset L$ gibt, so dass f über L in Linearfaktoren zerfällt.

Bemerkung:

Sei $f = a_n x^n + \cdots + a_0 \in \mathbb{C}[x]$, $K = K(a_0, \ldots, a_n)$.

Genau dann, wenn $f \in K[x]$ über K durch Radikale auflösbar ist, können wir wie in Bsp. 5.2.1 die Nullstellen von f durch Wurzeln von rationalen Funktionen der Koeffizienten ausdrücken.

5.2.3 Satz

Sei $f \in K[x]$, $char(K) = 0$, L der Zerfällungskörper von f. Dann:

$$f \text{ ist über } K \text{ durch Radikale auflösbar } \Leftrightarrow \mathrm{Aut}_K(L) \text{ ist auflösbar}$$

Erinnerung an Auflösbarkeit von Gruppen: 1.6.4

5.2.4 Lemma:

Sei $\text{char}(K) = 0$, $\zeta_n = e^{\frac{2\pi i}{n}} \in K$

1) Ist $L = K(\alpha)$ mit $\alpha^n \in K$, dann ist L der Zerfällungskörper von $x^n - \alpha^n$, $K \subset L$ ist Galoiserweiterung und $\text{Aut}_K(L)$ ist zyklisch mit $|\text{Aut}_K(L)| \mid n$

2) Ist $K \subset L$ Galoiserweiterung mit $\text{Aut}_K(L) \cong \mathbb{Z}_n$ und n prim, dann ist $L = K(\alpha)$ mit $\alpha^n \in K$.

Beweis:

1) Es gilt:

$$x^n - \alpha^n = \left(x - \zeta_n^0\alpha\right) \cdot (x - \zeta_n\alpha) \cdot \ \cdots \ \cdot \left(x - \zeta_n^{n-1}\alpha\right)$$

Und es folgt:

$S_n \in K$
$\Rightarrow \zeta_n^i \in K$
$\Rightarrow \alpha\zeta_n^i \in K$
$\Rightarrow L = K(\alpha) = K(\zeta_n^0\alpha, \zeta_n\alpha, ..., \zeta_n^{n-1}\alpha)$ ist der Zerfällungskörper von $x^n - \alpha^n$, $x^n - \alpha^n$ ist separabel
$\Rightarrow K \subset L$ ist Galoiserweiterung

Wir setzen:

$$\begin{aligned} \pi : \ \text{Aut}_K(L) &\to \mathbb{Z}_n \\ \delta_k &\mapsto k \end{aligned}$$

wobei $\delta_K(\alpha) = \zeta_n^k\alpha$.

Da $\delta_k \circ \delta_l = \delta_{k+l}$ ist π ein Gruppenhomomorphismus. π ist auch injektiv.

$\Rightarrow \text{Aut}_K(L)$ ist eine Untergruppe von $\mathbb{Z}_n$ und damit selbst zyklisch mit einer Ordnung, die n teilt.

2) $\text{Aut}_K(L) = \langle b \rangle$, $\text{ord}(\delta) = n$.

Betrachte δ als K-Vektorraumendomorphismus $\delta : \ L \to L$.

Da $\delta^n = \text{id}$ muss das Minimalpolynom $\mu_\delta \ x^n - 1$ teilen.

$x^n - 1$ zerfällt über K in die Linearfaktoren $\left(x - \zeta_n^0\alpha\right) \cdots \left(x - \zeta_n^{n-1}\alpha\right)$

Da das Minimalpolynom paarweise verschiedene Linearfaktoren hat, ist δ diagonalisierbar.

Alle Eigenwerte sind $n-$te Einheitswurzeln.Wäre 1 der einzige Eigenwert $\Rightarrow \delta = \text{id}$

$\Rightarrow n = 1 \ \lightning$ zu n prim

Sei $0 \neq \alpha \in L$ Eigenvektor zum Eigenwert $\zeta \in K$, also $\delta(\alpha) = \zeta_\alpha$

$\Rightarrow \delta(\alpha^n) = \delta(\alpha)^n = \zeta^n\alpha^n = \alpha^n$

$\Rightarrow \alpha^n \in \text{Fix}(\text{Aut}_K(L)) = K$ da $K \subset L$ Galoiserweiterung siehe 4.7.1.

Behauptung: $L = K(\alpha)$

" $\subset$ " klar

" $\supset$ " Da mit 4.7.10

$$[L : K(\alpha)] \cdot [K(\alpha) : K] = [L : K] = |\text{Aut}_K(L)| = n$$

und prim folgt $[K(\alpha) : K] \in \{1, n\}$.

Wäre $[K(\alpha) : K] = 1 \Rightarrow a \in K \Rightarrow \delta(\alpha) = \alpha \ \lightning$ zu $\delta(\alpha) = \zeta_\alpha$ mit Eigenwert $\zeta \neq 1$

$\Rightarrow [K(\alpha : K)] = n \Rightarrow [L : K(\alpha)] = 1 \Rightarrow L = K(\alpha)$. □

5.2.5 Korollar:

Sei L Zwischenkörper einer Radikalerweiterung mit $\text{char}(L) = 0$.

Dann ist L Zwischenkörper einer abelschen Radikalerweiterung.

Beweis:

Sei $K \subset L \subset M$, $M = K(\alpha_1, ..., \alpha_n)$, $\alpha_i^{k_i} \in K(\alpha_1, ..., \alpha_{i-1})$.

Sei $K_i = K(\alpha_1, ..., \alpha_i)$, dann ist $k_i = [K_i : K_{i-1}]$. Sei $n = K_1 \cdots k_m$ und sei $\zeta_n = e^{\frac{2\pi i}{n}} \in \mathbb{C}$.

Betrachte

$$K = K_0 \subset K_0(\zeta_n) \subset K_1(\zeta_n) \subset \cdots \subset K_m(\zeta_n) = M(\zeta_n)$$

Da mit ζ_n auch die k_i-ten Einheitswurzeln in $K_0(\zeta_n)$ enthalten sind, gilt mit 5.2.4 1) angewendet auf

$$K_{i-1}(\zeta_n)$$

und

$$K_i(\zeta_n) = K_{i-1}(\zeta_n)(\alpha_i) \text{ mit } \alpha_i^{k_i} \in K_{i-1}(\zeta_n)$$

$K_{i-1}(\zeta_n) \subset K_i(\zeta_n)$ ist Galoiserweiterung mit zyklischer, damit abelscher, Galoisgruppe.

Auch $K_0 \subset K_0(\zeta_n)$ ist Galoiserweiterung, da $K_0(\zeta_n)$ Zerfällungskörper von $x^n - 1$ ist, und die Galoisgruppe ist $\mathbb{Z}_n^*$, da für $\delta_k(\zeta_n) = \zeta_n^k$ (wegen $\delta_{kl} = \delta_k \circ \delta_l$)

$$\begin{aligned} \text{Aut}_{K_0}(K_0(\zeta_n)) &\xrightarrow{\cong} \mathbb{Z}_n^* \\ \delta_k &\longmapsto k \end{aligned}$$

Die Einheitengruppe eines endlichen Körpers ist wegen 4.6.7 zyklisch, also abelsch.

Da $\zeta_n^n = 1$ ist $K \subset M(\zeta_n) = K(\alpha_1, ..., \alpha_m, \zeta_n)$ eine abelsche Radikalerweiterung, die L als Zwischenkörper enthält. $\square$

5.2.6 Proposition: Translationssatz

Sei $K \subset M$ eine Erweiterung, N und L Zwischenkörper, $K \subset N$ Galoiserweiterung.

Dann sind auch $L \cap N \subset N$ und $L \subset L(N)$ Galoiserweiterungen mit

$$\mathrm{Aut}_{L\cap N}(N) \cong \mathrm{Aut}_L(L(N))$$

Beweis:

$L \cap N$ ist Zwischenkörper der Galoiserweiterung $K \subset N$ damit ist $L \cap N \subset N$ auch Galoiserweiterung wegen des Hauptsatzes der Galoistheorie 4.7.9

Wegen 4.7.11 ist N Zerfällungskörper eines separablen Polynoms $f \in K[x]$.

Seien $\alpha_1, ..., \alpha_n$ die Nullstellen von f

$\Rightarrow N = K(\alpha_1, ..., \alpha_n)$

$\Rightarrow L(N) = L(\alpha_1, ..., \alpha_n)$ ist der Zerfällungskörper von f über L und damit ist $L \subset L(N)$ Galoiserweiterung wegen 4.7.11

Sei $\delta \in \mathrm{Aut}_L(L(N))$, dann hält δ insbesondere K fest, und da $K \subset N$ normal ist folgt mit 4.7.6 $\delta|_N : N \to L(N)$ ist schon in $\mathrm{Aut}_K(N)$. Es folgt:

$$\begin{aligned} \pi : \mathrm{Aut}_L(L(N)) &\to \mathrm{Aut}_K(N) \\ \delta &\mapsto \delta|_N \end{aligned}$$

ist wohldefinierter Gruppenhomomorphismus.

Da δ durch die Bilder der α_i festgelegt ist und $\alpha_i \in N \ \forall \ i$ folgt π ist injektiv. Es folgt:

$$\mathrm{Aut}_L(L(N)) \cong U$$

ist Untergruppe von $\mathrm{Aut}_K(N)$.

Dann gilt

$$\begin{aligned} \mathrm{Fix}(U) &= \{\alpha \in N \mid \delta(\alpha) = \alpha \ \forall \ \delta \in \mathrm{Aut}_L(L(N))\} \\ &= N \cap \{\alpha \in L(N) \mid \delta(\alpha) = \alpha \text{ für } \delta \in \mathrm{Aut}_L(L(N))\} \\ &= N \cap \mathrm{Fix}(\mathrm{Aut}_L(L(N)) \\ &= N \cap L \end{aligned}$$

da $L \subset L(N)$ Galoiserweiterung ist.

$\Rightarrow U = \mathrm{Aut}_{N\cap L}(N)$ wegen des Hauptsatzes der Galoistheorie. □

Beweis: von Satz 5.2.3

> Erinnerung: 5.2.3 **Satz:**
> Sei $f \in K[x]$, $\text{char}(K) = 0$, L der Zerfällungskörper von f. Dann:
>
> $$f \text{ sei über } K \text{ durch Radikale auflösbar } \Leftrightarrow \text{ Aut}_K(L) \text{ ist auflösbar}$$

Beweis:

„⇒“ Nach Definition ∃ Radikalerweiterung $K \subset M$, so dass f über M in Linearfaktoren zerfällt.

Da L der Zerfällungskörper von f ist, ist $K \subset L \subset M$ Zwischenkörper.

Da $\text{char}(L) = \text{char}(K) = 0$ folgt mit 5.2.5, dass L Zwischenkörper einer abelschen Radikalerweiterung

$$M' = K(\alpha_1, ..., \alpha_m)$$

ist mit $\alpha_i^{k_i} \in K(\alpha_1, ..., \alpha_{i-1})$.

Setze $K_i = K(\alpha_1, ..., \alpha_i)$.

Wir zeigen per Induktion über m, dass $\text{Aut}_K(L)$ auflösbar ist.

Für $m = 0$ gilt $K = L = M'$ und $\text{Aut}_K(L) = \{e\}$.

Sei $m > 0$. $L(K_1)$ ist der Zerfällungskörper von $f \in K_1[x]$ und ist Zwischenkörper der abelschen Radikalerweiterung $K_1 \subset M'$. Per Induktion können wir annehmen, dass $\text{Aut}_{K_1}(L(K_1))$ auflösbar ist. Es gilt:

$$\text{Aut}_{K_1}(L(K_1)) = \text{Aut}_{K_1}(K_1(L)) \overset{5.2.6}{\cong} \text{Aut}_{K_1 \cap L}(L)$$

(da $K \subset L$ Galoiserweiterung ist, da f separabel wegen $\text{char}(K) = 0$, 4.5.11)

$\Rightarrow \text{Aut}_{K_1 \cap L}(L)$ ist auflösbar. $(*)$

Da $K \subset M'$ abelsche Radikalerweiterung ist, ist $K \subset K_1$ Galoiserweiterung und $\text{Aut}_K(K_1)$ abelsch.

Da $K \subset L \cap K_1 \subset K_1$ Zwischenkörper ist $\text{Aut}_{L \cap K_1}(K_1)$ Untergruppe von $\text{Aut}_K(K_1)$, damit Normalteiler, und aus dem Hauptsatz der Galoistheorie 4.7.9 folgt $K \subset K_1 \subset L$ ist Galoiserweiterung und

$$\text{Aut}_K(K_1) \big/ \text{Aut}_{K_1 \cap L}(K_1) \cong \text{Aut}_K(K_1 \cap L)$$

wobei letztere als Faktorgruppe einer abelschen Gruppe auch abelsch ist.

Da $K \subset L \cap K_1 \subset L$ Zwischenkörper ist und $K \subset L \cap K_1$ Galoiserweiterung folgt wieder mit dem Hauptsatz 4.7.9 $\text{Aut}_{L \cap K_1}(L)$ Normalteiler in $\text{Aut}_K(L)$ und

$$\text{Aut}_K(L) \big/ \text{Aut}_{L \cap K_1}(L) \cong \text{Aut}_K(L \cap K_1)$$

und diese Gruppe ist abelsch und damit auflösbar.

$\Rightarrow$ Der Normalteiler $\text{Aut}_{L \cap K_1}(L)$ ist auflösbar $(*)$, die Faktorgruppe

$$\text{Aut}_K(L) \big/ \text{Aut}_{L \cap K_1}(L)$$

ist auflösbar.

$\overset{1.6.5}{\Rightarrow} \text{Aut}_K(L)$ ist auflösbar.

„⇐“ Sei $\mathrm{Aut}_K(L)$ auflösbar. Sei $n = [L : K]$.

1. Fall: Sei $\zeta_n \in K$.

Da $\mathrm{Aut}_K(L)$ auflösbar, $\exists$ nach Satz 1.6.9 eine Kompositionsreihe, d.h.

$$\{e\} = G_m \subset G_{m-1} \subset \cdots \subset G_0 = \mathrm{Aut}_K(L)$$

so dass $G_i \subset G_{i-1}$ Normalteiler und ${}^{G_{i-1}}\!/_{G_i}$ zyklisch von Primzahlordnung p_i.

Betrachte die Zwischenkörper

$$K \subset K_i := \mathrm{Fix}(G_i) \subset L$$

Da $K \subset L$ Galoiserweiterung (f separabel, 4.5.11 und 4.7.11) ist auch $K_{i-1} \subset L$ Galoiserweiterung mit

$$\mathrm{Aut}_{K_{i-1}}(L) = \mathrm{Aut}_{\mathrm{Fix}(G_{i-1})}(L) = G_{i-1}$$

nach dem Hauptsatz der Galoistheorie 4.7.9

Da G_i in G_{i-1} Normalteiler ist, gilt

$${}^{G_{i-1}}\!/_{G_i} = {}^{\mathrm{Aut}_{K_{i-1}}(L)}\!/_{\mathrm{Aut}_{K_i}(L)} \cong \mathrm{Aut}_{K_{i-1}}(K_i)$$

und $K_{i-1} \subset K_i$ ist Galoiserweiterung mit zyklischer Galoisgruppe ${}^{G_{i-1}}\!/_{G_i}$.

Da

$$K = K_0 \subset K_1 \subset \cdots \subset K_m = L$$

und

$$[L : K] = [K_m : K_{m-1}] \cdot \ \cdots \ \cdot [K_i : K_{i-1}] \cdot [K_1 : K_0]$$

und

$$[K_i : K_{i-1}] = |\mathrm{Aut}_{K_{i-1}}(K_i)| = \left|{}^{G_{i-1}}\!/_{G_i}\right| = p_i$$

folgt $p_i \mid n$.

Damit ist auch $\zeta_{p_i} = e^{\frac{2\pi i}{p_i}} = e^{\frac{2\pi i}{n} \cdot \frac{n}{p_i}} = \zeta_n^{\frac{n}{p_i}} \in K$

Damit können wir 5.2.4 2) anwenden und erhalten $K_i = K_{i-1}(\alpha_i)$ mit $\alpha_i^{p_i} \in K_{i-1}$.

Damit ist $L = K(\alpha_1, ..., \alpha_m)$ eine Radikalerweiterung.

2. Fall: Sei $\zeta_n \notin K$.

Verwende den Translationssatz 5.2.6 für $K \subset L\zeta_n)$, Zwischenkörper L, $K(\zeta_n)$ mit $K \subset L$ Galoiserweiterung, dann ist $L \cap K(\zeta_n) \subset L$ und $K(\zeta_n) \subset L(\zeta_n)$ Galoiserweiterung mit

$$\mathrm{Aut}_{K(\zeta_n)}(L(\zeta_n)) \cong \mathrm{Aut}_{L \cap K(\zeta_n)}(L)$$

Dann ist

$$\begin{aligned} k &:= [L(\zeta_n) : K(\zeta_n)] \\ &= \left|\mathrm{Aut}_{K(\zeta_n)}(L(\zeta_n))\right| \\ &= \left|\mathrm{Aut}_{L \cap K(\zeta_n)}(L)\right| \\ &= [L \cap K(\zeta_n) : L] \ \Big| \ [L : K] = n \end{aligned}$$

$\Rightarrow \zeta_k = \zeta_n^{\frac{n}{k}} \in K(\zeta_n)$.

Da $\mathrm{Aut}_K(L)$ auflösbar ist auch die Untergruppe $\mathrm{Aut}_{L \cap K(\zeta_n)}(L)$ auflösbar, also $\mathrm{Aut}_{K(\zeta_n)}(L(\zeta_n))$ auflösbar.

Damit erfüllt $K(\zeta_n) \subset L(\zeta_n)$ die Voraussetzungen von Fall 1.

Der Zerfällungskörper $L(\zeta_n)$ von f über $K(\zeta_n)[x]$ ist wegen Fall 1 eine Radikalerweiterung

$$L(\zeta_n) = K(\zeta_n)(\alpha_1, ..., \alpha_m)$$

mit

$$\alpha_i^{k_i} \in K(\zeta_n)(\alpha_1, ..., \alpha_{i-1})$$

Da $\zeta_n^n = 1 \in K$ ist auch $K \subset L(\zeta_n)$ Radikalerweiterung, über der f zerfällt.

$\Rightarrow f$ ist durch Radikale auflösbar. $\square$

5.2.7 Korollar:

Sei $f \in K[x]$ vom Grad höchstens 4, K ein Teilkörper von $\mathbb{C}$, L der Zerfällungskörper von f.

Wegen 4.4.8 ist $\mathrm{Aut}_K(L) \subset \mathbb{S}_4$ Untergruppe und wegen Bsp 2) nach 1.6.4 ist f durch Radikale auflösbar.

(Wussten wir schon wegen den Formeln von Cardano 5.2.1 3))

5.2.8 Beispiel:

Sei $f = x^5 + x^4 - 4x^3 - 3x^2 + 3x + 1 \in \mathbb{Q}[x]$.

Man kann zeigen, dass f das Minimalpolynom von $\alpha = \zeta_{11} + \zeta_{11}^{-1}$ ist.

Dann ist $\mathbb{Q} \subset \mathbb{Q}(\alpha) \subset \mathbb{Q}(\zeta_{11})$ und $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\zeta_{11})) = \mathbb{Z}_{11}^*$ (siehe Beweis von 5.2.5), $\mathbb{Z}_{11}^* \cong \mathbb{Z}_{10}$ ist zyklisch, daher ist jede Untergruppe ein Normalteiler und damit $\mathbb{Q} \subset \mathbb{Q}(\alpha)$ Galoiserweiterung.

$$\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\alpha)) \cong {}^{\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\zeta_{11}))}\!\diagup_{\mathrm{Aut}_{\mathbb{Q}(\alpha)}(\mathbb{Q}(\zeta_{11}))}$$

ist Faktorgruppe einer zyklischen Gruppe und damit selbst zyklisch.

Da $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 5$ folgt $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\alpha)) = \mathbb{Z}_5$.

Insbesondere ist $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\alpha))$ auflösbar, und da f über $\mathbb{Q}(\alpha)$ schon zerfällt, gilt f ist durch Radikale auflösbar.

Die Radikalausdrücke für die Nullstellen von f kennen wir dadurch aber nicht.

5.2.9 Proposition:

Sei p eine Primzahl, $\tau \in \mathbb{S}_p$ eine Transposition und δ ein p-Zykel, dann gilt

$$\mathbb{S}_p = \langle \tau, \delta \rangle$$

Beweis:

Sei ohne Einschränkung $\tau = (1\ 2)$. Ist $\delta = (1\ 2\ 3\ \cdots\ p)$ so gilt:

$$(i\ \ i+1) = (\delta^{i-1}(1)\ \delta^{i-1}(2)) = \delta^{i-1} \circ (1\ 2)\delta^{-(i-1)} \in \langle \tau, \delta \rangle \quad \forall i = 1, ..., p-1$$

Da $\mathbb{S}_p$ von Nachbartranspositionen erzeugt wird, folgt die Behauptung.

Ist δ ein beliebiger p-Zykel, so sind seine Potenzen auch p-Zykel (da p prim) und wir können eine Potenz wählen, so dass

$$\delta^i = (1\ 2\ a_3\ \cdots\ a_p)$$

Für

$$\delta' = \begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & p \\ 1 & 2 & a_3 & a_4 & \cdots & a_p \end{pmatrix}$$

gilt

$$\delta'^{-1} \circ \delta^i \circ \delta' = (1\ \cdots\ p)$$

und

$$\delta'^{-1} \circ (1\ 2) \circ \delta' = (1\ 2)$$

so dass für $U = \langle \tau, \delta \rangle$ gilt

$$\begin{aligned} &\mathbb{S}_p = \langle \tau, (1\ \cdots\ p) \rangle \subset \delta'^{-1} U \delta' \subset \mathbb{S}_p \\ &\Rightarrow\ \delta'^{-1} U \delta' = \mathbb{S}_p \\ &\Rightarrow\ U = \delta' \mathbb{S}_p \delta'^{-1} = \mathbb{S}_p \end{aligned}$$

□

5.2.10 Satz: Abel-Ruffini

Sei $f \in \mathbb{Q}[x]$ irreduzibel von ungeradem Primzahlgrad p mit genau 2 nicht-reellen Nullstellen, sei L der Zerfällungskörper von f, dann gilt

$$\mathrm{Aut}_{\mathbb{Q}}(L) \cong \mathbb{S}_p$$

Beweis:

Sei $\lambda \in \mathbb{C}$ eine Nullstelle von f, so gilt $f(\overline{\lambda}) = \overline{f(\lambda)} = \overline{0} = 0$.

$\Rightarrow$ Die komplexe Konjugation $j: \mathbb{C} \to \mathbb{C}$ permutiert die Nullstellen von f

$\Rightarrow j|_L: L \to L \subset \mathrm{Aut}_{\mathbb{Q}}(L)$

Da f genau $p-2$ reelle Nullstellen hat, ist $j|_{\text{Nullstellen}}$ eine Transposition.

Sei α eine Nullstelle von f dann gilt

$$P = [\mathbb{Q}(\alpha) : \mathbb{Q}] \;\Big|\; [L : \mathbb{Q}] = |\mathrm{Aut}_{\mathbb{Q}}(L)|$$

da $\mathbb{Q} \subset L$ Galoiserweiterung wegen 4.7.11 und 4.5.11 ($\mathrm{char}(\mathbb{Q}) = 0$, also f seperabel).

Damit enthält $\mathrm{Aut}_{\mathbb{Q}}(L)$ p-Sylowgruppen mit Ordnung p, also einen p-Zykel.

Mit 5.2.9 folgt $\mathrm{Aut}_{\mathbb{Q}}(L) \cong \mathbb{S}_p$. □

5.2.11 Korollar:

$f = x^5 - 4x + 2 \in \mathbb{Q}[x]$ ist über $\mathbb{Q}$ nicht durch Radikale auflösbar.

Beweis:

Wegen dem Eisensteinkriterium 4.3.9 ist f irreduzibel über $\mathbb{Z}$ und wegen 4.3.10 auch über $\mathbb{Q}$. Es gilt für $t \in \mathbb{R}$:

t	-2	-1	1	2
$f(t)$	-22	5	-1	26

Aus dem Zwischenwertsatz folgt dann, dass f mindestens 3 reelle Nullstellen besitzt.

$$f' = 5x^4 - 4$$

besitzt zwei reelle Nullstellen $x = \pm\sqrt[4]{\frac{4}{5}}$, daher gibt es nur 2 lokale Extrema und daher höchstens 4 reelle Nullstellen.

Damit hat f genau zwei nicht-reele Nullstellen.

Aus Abel-Ruffini 5.2.10 folgt, dass für den Zerfällungskörper L von f gilt $\mathrm{Aut}_{\mathbb{Q}}(L) \cong \mathbb{S}_5$.

Wegen 1.6.6 ist $\mathrm{Aut}_{\mathbb{Q}}(L)$ nicht auflösbar.

Wegen 5.2.3 ist f nicht durch Radikale auflösbar.

Bemerkung:

Daraus folgt, dass es für Polynome vom Grad ≥ 5 keine allgemeinen Formeln für die Nullstellen wie die Cardano-Formel geben kann.

Auch wenn für einzelne Polynome (siehe 5.2.6) solche Formeln gibt, so gibt es aber auch welche, für die es keine gibt (siehe 5.2.11), so dass es keine allgemeingültige geben kann.

6 Literatur

Dieses Skript beruft sich auf folgende Literatur:

1. Janko Boehm, Grundlagen der Algebra und Zahlentheorie
2. Rainer Schulze-Pillot, Einfuehrung in die Algebra und Zahlentheorie
3. Gerd Fischer, Lehrbuch der Algebra
4. Siegfried Bosch, Algebra
5. D. J. H. Garling, A course in Galois theory