Skriptum Algebra

Wintersemester 2002/2003

$$\sqrt[3]{2}$$

LaTeX
Jens Rückert 2003

Vorlesungsscript zur Vorlesung Algebra

Vorlesender: Dr. Schulz

TU Chemnitz
Fakultät für Mathematik
Wintersemester 2002/2003

Gesetzt und geTEXt von Jens Rückert .....
jens.rueckert@mathematik.tu-chemnitz.de

Probegelesen, Titel und Indexverzeichnis von Roman Unger .....
roman.unger@mathematik.tu-chemnitz.de

Dieses Script ist als Ergänzung zur Vorlesung und Prüfungsvorbereitung gedacht, soll aber nicht den Besuch der Vorlesung ersetzen !

Inhaltsverzeichnis

Kapitel 0

Äquivalenzrelationen und verträgliche Funktionen

0.1 Definitionen

Definition 0.1.1. *Sei $M \neq \emptyset$ eine beliebige Menge. Jede Teilmenge $R \subseteq M \times M$ heißt eine (binäre) Relation auf M.*
Schreibweise:

$$(x, y) \in R \Leftrightarrow xRy$$

(x steht in Relation zu y)

Beispiel 0.1.2.

1. *Extremfälle:* $R = \emptyset, \quad R = M \times M$
2. *Identität:* $R = I := \{(x, x) : x \in M\}$, *d.h.,* $xIy \Leftrightarrow x = y$
3. *Sei f eine Funktion, $f : M \to M$, d.h.* $xRy \overset{Definition}{\Leftrightarrow} y = f(x)$
4. *Sei* $M = \mathbb{R}$
   (a)
   $$xR_1y \overset{Definition}{\Leftrightarrow} x \leq y$$
   (b)
   $$xR_2y \overset{Definition}{\Leftrightarrow} |x| = |y|$$
   (c)
   $$xR_3y \overset{Definition}{\Leftrightarrow} x \neq y$$

(d)

$$xR_4y \overset{Definition}{\Leftrightarrow} |x-y|<1$$

5. $M=\mathbb{Z}, \quad m\geq 1$

(a)

$$xR_1y \Leftrightarrow x|y \quad (x \textit{ teilt } y)$$

(b)

$$xR_2y \Leftrightarrow m|x-y \quad (x\equiv y \textit{ modulo } (m))$$

Definition 0.1.3. *Die Relation R auf $M\neq\emptyset$ heißt Äquivalenzrelation, wenn gilt:*

1. *xRx für alle $x\in M$ (Reflexivität)*
2. *Aus $xRy \Rightarrow yRx$ (Symmetrie)*
3. *Aus xRy und $yRz \Rightarrow xRz$ (Transitivität)*

Beispiel 0.1.4.

1. *$5b$ aus* $(0.1.2)$.
2. *Sei $f: M\to N$ eine Funktion und sei die Relation R_f auf M gegeben durch $xR_fy \overset{Definition}{\Leftrightarrow} f(x)=f(y), \quad (x,y\in M)$, dann ist R_f eine Äquivalenzrelation auf M.*

Definition 0.1.5. *Sei R eine Äquivalenzrelation auf M und $x\in M$. Die Menge*

$$\overline{x} := \{y\in M : yRx\}$$

heißt die zu x gehörige Äquivalenzklasse. (Nebenklasse, Restklasse)
Jedes Element $y\in\overline{x}$ heißt Repräsentant der Klasse $\overline{x}$. (insbesondere ist x ein Repräsentant bzw. Vertreter von $\overline{x}$)

Beispiel 0.1.6.

$M=\mathbb{Z}, x\equiv y \quad mod(2)$ *ist eine Äquivalenzrelation*
$\overline{0}=\{y\in\mathbb{Z} : y\equiv 0 \quad (2)\}$ *y kongruent* $\quad 0 \quad mod(2)$
$\overline{1}=\{y\in\mathbb{Z} : y\equiv 1 \quad (2)\}$

$\rightarrow \quad y\equiv 0 \mod 2 \Leftrightarrow 2|y-0=y \Leftrightarrow y$ *gerade* $\overline{0}=\{$*gerade Zahlen*$\}$
$\quad\quad y\equiv 1 \mod 2 \Leftrightarrow 2|y-1 \quad \Leftrightarrow y$ *ungerade* $\overline{1}=\{$*ungerade Zahlen*$\}$

Bemerkung 0.1.7. *Sei R eine Äquivalenzrelation auf M. Es gilt:*

$$x \in \overline{x}, \text{ für alle } x \in M \Rightarrow \overline{x} \neq \emptyset$$

Satz 0.1.8. *Sei R eine Äquivalenzklasse auf M. Dann gilt:*

$$xRy \Leftrightarrow \overline{x} = \overline{y}$$

Beweis.

1. Sei xRy und $u \in \overline{x} \Rightarrow uRx$
   Da R nach Definition transitiv ist, gilt:

   $$uRy \Rightarrow u \in \overline{y} \Rightarrow \overline{x} \subseteq \overline{y}$$

   Analog wird $\overline{y} \subseteq \overline{x}$ gezeigt.
   $\Rightarrow \overline{x} = \overline{y}$
2. Sei $\overline{x} = \overline{y} \Rightarrow x \in \overline{y} \Rightarrow xRy$

□

Satz 0.1.9. *Sei R eine Äquivalenzrelation auf M und $x, y \in M$. Dann gilt entweder $\overline{x} = \overline{y}$ oder $\overline{x} \cap \overline{y} = \emptyset$.*

Beweis. Sei $z \in \overline{x} \cap \overline{y} \Rightarrow zRx \wedge zRy \Rightarrow xRy \Rightarrow \overline{x} = \overline{y}$ □

Definition 0.1.10. *Sei $M \neq \emptyset$ beliebig. Das System $\{M_\tau\}$ von Teilmengen der Menge M ($M_\tau \subseteq M$) heißt eine Klasseneinteilung von M, wenn gilt:*

1. *$M_\tau \neq \emptyset$ für alle τ*
2. *$M_\tau \cap M_{\tau'} = \emptyset$ für alle $\tau \neq \tau'$*
3. *$M = \bigcup_\tau M_\tau$*

Satz 0.1.11. *Jede Äquivalenzrelation R auf M erzeugt eine Klasseneinteilung $\{\overline{x}\}_{x \in M}$ von M, und umgekehrt erzeugt jede Klasseneinteilung von M eine Äquivalenzrelation auf M.*

Beweis.

1. Sei R eine Äquivalenzrelation auf M. Wegen Bemerkung $(0.1.7)$ folgt:

   $$M = \bigcup_{x \in M} \overline{x}, \quad \overline{x} \neq \emptyset$$

   und wegen Satz $(0.1.9)$:

   $$\overline{x} \cap \overline{y} = \emptyset \text{ für alle } \overline{x} \neq \overline{y}$$

2. Sei $\{M_\tau\}$ eine Klasseneinteilung von M. Wir setzen:

$$xRy \overset{Definition}{\Longleftrightarrow} \text{ es existieren } \tau : x, y \in M_\tau \qquad (*)$$

Zeigen: R ist eine Äquivalenzrelation auf M.
Sei $x \in M$. Wegen $3.)$ aus $(0.1.10)$ folgt:

$$\text{Es existieren } \tau : x \in M_\tau \Rightarrow xRx \quad (x \in M) \text{ (Reflexivität)}$$

Sei xRy, d.h., es existieren $\tau : x, y \in M_\tau \Rightarrow y, x \in M_\tau \Rightarrow yRx$ (Symmetrie)
Sei xRy, yRz, d.h., es existieren $\tau, \tau' : x, y \in M_\tau, \quad y, z \in M_{\tau'}$
$\Rightarrow y \in M_\tau \cap M_{\tau'} \overset{2)(0.1.10)}{\Longrightarrow} \tau = \tau' \Rightarrow M_\tau = M_{\tau'} \Rightarrow xRz$ (Transitivität)
Bemerkung: $M_\tau = \overline{x}$

□

Bemerkung 0.1.12.

1. *Ist $\{M_\tau\}$ eine Klasseneinteilung von M auf R, der Relation $(*)$ aus dem Beweis zu Satz $(0.1.11)$, so existiert für alle τ genau ein $\overline{x}$ mit*

$$\overline{x} = M_\tau$$

2. *Sei R eine Äquivalenzrelation auf M. Wählt man aus jeder Klasse $\overline{x}$ genau ein Element τ aus, so erhält man ein Vertretersystem.*

3. *Die Menge der Äquivalenzklassen $\overline{x}$ heißt Faktormenge (kurz: M/R)*

Satz 0.1.13. *Jede Äquivalenzrelation R auf M ist von der Form*

$$R = Rel(\pi)$$

für eine gewisse Funktion π.

Beweis. Sei $\pi : M \to M/R$ gegeben durch $\pi(x) = \overline{x} \quad (x \in \overline{x})$ eine kanonische Abbildung. Es gilt:

$$xRy \Leftrightarrow \overline{x} = \overline{y} \Leftrightarrow \pi(x) = \pi(y)$$

□

Beispiel 0.1.14.

1. *Die natürliche Zahl n ist die Kurzbezeichnung für Äquivalenzklassen aller Mengen mit n Elementen bezüglich der Relation "Gleichmächtigkeit".*

2. *Die ganzen Zahlen sind die Äquivalenzklassen differenzungleicher Paare natürlicher Zahlen*
   (d.h., $M = \mathbb{N} \times \mathbb{N}, \quad (a,b)R(c,d) \overset{Definition}{\Longleftrightarrow} a + d = b + c$*)*
   (Rationale Zahlen $(a,b)R(c,d) \Leftrightarrow ad = cb, \quad [b,d \neq 0]$*)*

3. $M = \mathbb{R}, \quad xRy \Leftrightarrow x - y = 2k\pi \quad (k \in \mathbb{Z})$

$$M/R \cong [0, 2\pi] \cong \textit{Kreislinie}$$

Definition 0.1.15. *Sei* R_i *eine Relation auf* $M_i, \quad (i = 1, 2)$*. Die Funktion* $f : M_1 \to M_2$ *heißt verträglich mit den Relationen* R_1 *und* R_2*, wenn aus* $xR_1y \quad (x, y \in M_1)$ *stets* $f(x)R_2f(y)$ $(f(x), f(y) \in M_2)$ *folgt.*

Beispiel 0.1.16.

1. $M_1 = M_2 = \mathbb{R}$

   (a) $R_1 = R_2 =$ " $\leq$ "
   $f : \mathbb{R} \to \mathbb{R}$ *ist verträglich mit* $R_1, R_2 \Leftrightarrow x \leq y \Rightarrow f(x) \leq f(y) \to$ *monoton wachsend*

   (b) $xR_1y \Leftrightarrow |x| = |y|, \quad R_2 =$ " $=$ " $\Leftrightarrow |x| = |y| \Leftrightarrow f(x) = f(y)$
   $\to$*gerade Funktionen (*$f(x) = f(-x)$*)*

   (c) $p \in \mathbb{R}/\{0\}$ *fix,* $xR_1y \Leftrightarrow \exists k \in \mathbb{Z} : x - y = kp, \quad R_2 =$ " $=$ "
   Eine verträgliche Funktion ist $f(x) = f(x + kp)$

2. *Sei* $f : M_1 \to M_2$ *eine Funktion,* $R_1 = Rel(f), \quad R_2 =$ " $=$ "*. Sei* f *verträglich mit* R_1, R_2*, dann gilt:*

$$xR_1y \overset{Definition}{\Longleftrightarrow} f(x) = f(y)$$

Satz 0.1.17 (Satz über die Faktorabbildung). *Sei* R_i *eine Äquivalenzrelation auf* M_i *und* $\pi_i : M_i \to M_i/R_i$ *die kanonische Abbildung (*$i = 1, 2$*).*
Zu jeder Funktion $f : M_1 \to M_2$ *gibt es genau dann eine eindeutige Funktion* $\overline{f} : M_1/R_1 \to M_2/R_2$ *mit*

$$\pi_2 \circ f = \overline{f} \circ \pi_1 \qquad (*),$$

wenn f *mit* R_1 *und* R_2 *verträglich ist.*
($(*)$ *bedingt, dass folgendes Diagramm kommutativ ist:*

$$\begin{array}{ccc} M_1 & \xrightarrow{f} & M_2 \\ \downarrow{\scriptstyle \pi_1} & & \downarrow{\scriptstyle \pi_2} \\ M_1/R_1 & \xrightarrow{\overline{f}} & M_2/R_2 \end{array}$$

)

Beweis.

1. Sei f verträglich mit R_1, R_2.
   Zeigen die Eindeutigkeit von $\overline{f}$: Sei

   $$\overline{g} : M_1/R_1 \to M_2/R_2 \text{ mit } \pi_2 \circ f = \overline{g} \circ \pi_1$$
   Für $\overline{x} \in M_1/R_1$ gilt:
   $$\overline{g}(\overline{x}) = \overline{g}(\pi_1(x)) = (\overline{g} \circ \pi_1)(\overline{x}) = (\pi_2 \circ (f)(x)) = \pi_2(f(x))$$
   $$\overset{(*)}{=} (\overline{f} \circ \pi_1)(x) = \overline{f}(\pi_1(x)) = \overline{f}(\overline{x}) \text{ für alle } \overline{x} \in M_2/R_2 \Rightarrow \overline{f} = \overline{g}$$

   Zeigen wir nun die Existenz von $\overline{f}$:
   Sei $\overline{x} \in M_1/R_1$. Setzen $\overline{f}(\overline{x}) := \overline{f(x)}\ (\in M_2/R_2)$

   Zeigen noch, dass $\overline{f}$ wohldefiniert ist:
   Sei $y \in \overline{x}$, d.h., $xR_1y \overset{\text{verträglich}}{\Longleftrightarrow} f(x)R_2f(y) \Rightarrow \overline{f(x)} = \overline{f(y)}$
   $\Rightarrow$ Zuordnung hängt nicht von der Wahl des Repräsentanten ab
   $\Rightarrow \overline{f}$ ist eine Funktion, nämlich: $M_1/R_1 \to M_2/R_2$ mit $\overline{f}(\overline{x}) = \overline{f(x)}$
   Weiter gilt: Für $x \in M_1$ ist

   $$(\pi_2 \circ f)(x) = \pi_2(f(x)) = \overline{f(x)} = \overline{f}(\overline{x}) = \overline{f}(\pi_1(x)) = (f \circ \pi_1)(x)$$

2. Seien die Bedingungen erfüllt:
   Zeigen: f ist verträglich mit R_1, R_2
   Sei $xR_1y \Rightarrow \pi_1(x) = \pi_1(y) \Rightarrow \overline{f}(\pi_1(x)) = \overline{f}(\pi_1(y)) \overset{(*)}{\Rightarrow} \pi_2(f(x)) = \pi_2(f(y)) \Rightarrow f(x)R_2f(y) \Rightarrow$ Behauptung
   $\overline{f}$ ist hierbei die Faktorabbildung bezüglich f, R_1, R_2.

□

Bemerkung 0.1.18. *Mit den Beziehungen von Satz* 0.1.17 *gilt:*

1. $\overline{f}$ *injektiv* $\Leftrightarrow$ *Aus* $f(x)R_2f(y)$ *folgt* xR_1y
2. $\overline{f}$ *surjektiv* $\Leftrightarrow$ *Für alle* $y \in M_2$ *existiert ein* $x \in M_1$ *mit* $yR_2f(x)$ $\qquad (**)$
3. *wenn* f *surjektiv ist, so gilt* $(**)$

Beweis zu 2..

1. Sei $\overline{f}$ surjektiv und $y \in M_2$. Da $\overline{y} \in M_2/R_2$ existiert ein $x \in M_1/R_1$ mit $\overline{y} = \overline{f}(\overline{x}) \Rightarrow \overline{y} = \overline{f(x)} \Rightarrow yR_2f(x)$

2. Sei $(**)$ erfüllt und $\overline{y} \in M_2/R_2 \overset{(**)}{\Rightarrow}$ Für $y \in \overline{y}$ existieren $x \in M_1$ mit $yR_2(f(x))$
   $\Rightarrow \quad \overline{y} = \overline{f(x)} = \overline{f}(\overline{x}) \quad (\overline{x} \in M_1/R_1) \Rightarrow \overline{f}$ ist surjektiv

□

Folgerung 0.1.19. *Jede Funktion $f : M_1 \to M_2$ läßt sich als Verknüpfung der kanonischen Abbildung $\pi : M_1 \to M_1/Rel(f)$ und einer eindeutig bestimmten injektiven Funktion $\overline{f} : M_1/Rel(f) \to M_2$ darstellen, d.h.:*

$$f = \overline{f} \circ \pi$$

und damit ist folgendes Diagramm kommutativ:

$$\begin{array}{ccc} M_1 & \xrightarrow{f} & M_2 \\ \downarrow{\scriptstyle \pi} & \nearrow{\scriptstyle \overline{f}} & \\ M_1/Rel(f) & & \end{array}$$

Beweis. Mit Satz $(0.1.17)$, $R_1 = Rel(f), R_2 = I =$ " = "
folgt: $\pi_1 = \pi, \quad \pi_2 = id_{M_2}$
Zu Injektivität von $\overline{f}$:
Sei $f(x)R_2f(y)$, d.h., $f(x) = f(y) \Rightarrow xRel(f)y \overset{\text{Satz}(0.1.18(1))}{\Longrightarrow} \overline{f}$ ist injektiv □

Bemerkung 0.1.20. *Ist in Folgerung $(0.1.19)$ f zusätzlich noch surjektiv, so ist $\overline{f}$ eine Bijektion von $M_1/Rel(f)$ auf M_2, d.h., $M_1/R_1 \ni \overline{x} \Longleftrightarrow y \in M_2$*

Beispiel 0.1.21.

$M_1 -$ *Menge aller Studenten der BRD*
$M_2 -$ *Menge aller Fakultäten in der BRD*

$f : M_1 \to M_2 \quad f(x)$ *ist die Fakultät, an der Student x studiert*
$xR_1y \overset{\textit{Definition}}{\Longleftrightarrow} x$ *in gleicher Gruppe wie y*
$XR_2Y \overset{\textit{Definition}}{\Longleftrightarrow}$ *Fakultät X an der gleichen HochschuleY*

Wie sieht $\overline{f}$ aus? $\to \overline{f}$ ordnet jeder Gruppe die Hochschule zu, der sie angeört.

Kapitel 1

Algebraische Strukturen

1.1 Definitionen

Definition 1.1.1. *Sei $M \neq \emptyset$ eine beliebige Menge. Eine Funktion $f : M \times M \to M$ heißt (binäre) innere Verknüpfung oder kurz eine Operation auf M.*
Es ist üblich, die Funktion nicht mit einem Buchstaben, sondern mit "$\circ, +, -, \cdot, *$" zu bezeichnen.
Daher schreibt man anstelle von $*((m_1, m_2))$ kurz $m_1 * m_2$.
Das Paar $(M, *)$ nennt man algebraische Struktur mit einer Operation (Verknüpfung), kurz algebraische Struktur.

Beispiel 1.1.2.

1. *(a) Summe und Produkt auf $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$*
   (b) Differenzen in $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$
2. *(a) Summe der Matrizen gleichen Typs*
   (b) Produkt zweier quadratischer Matrizen gleicher Ordnung
3. *Vektorprodukt im $\mathbb{R}^3$*
4. *Summe und Produkt von Funktionen aus $C[0, 1]$*
5. *$M = \mathbb{R}$, $m * n := max(m, n)$*
6. *$M = \mathbb{C}$, $z_1 * z_2 := \frac{1}{2}(z_1 + z_2)$*
7. *Sei $X \neq \emptyset$ eine beliebige Menge. Sei weiterhin $(M; \circ)$ eine algebraische Struktur und F die Menge der Funktionen von X in M.*
   Für f und g aus F sei $(f * g)(x) := f(x) \circ g(x)$.
   $(F, *)$ ist wieder eine algebraische Struktur.

Definition 1.1.3. *Sei "$*$" eine Operation auf $M \neq \emptyset$.*

1. *diese Operation heißt assoziativ, wenn gilt:*
   $(m_1 * m_2) * m_3 = m_1 * (m_2 * m_3)$ *für alle* $m_1, m_2, m_3 \in M$.
2. *diese Operation heißt kommutativ, wenn gilt:*
   $m_1 * m_2 = m_2 * m_1$ *für alle* $m_1, m_2 \in M$.

Definition 1.1.4.

1. *Eine algebraische Struktur $(M, *)$ heißt Halbgruppe, wenn die Operation "$*$" assoziativ ist.*
2. *Ist die Operation zusätzlich noch kommutativ, so spricht man von einer kommutativen Halbgruppe.*

1.2 Ausgezeichnete Elemente in algebraischen Strukturen

Definition 1.2.1. *Sei $(M, *)$ eine algebraische Struktur.*

1. *Ein Element $e_l \in M$ (bzw. $e_r \in M$) heißt linkes (rechtes) Einselement von $(M, *)$ oder bezüglich der Operation "$*$", wenn gilt:*

   $$e_l * m = m \text{ für alle } m \in M \qquad (m * e_r = m, \text{ für alle } m \in M)$$

   (Ein Element aus M, das gleichzeitig linkes und rechtes Einselement in $(M, *)$ ist, heißt kurz Einselement $\mathbf{1}$ [neutrales Element])
2. *Das Element $0_l \in M, \quad (0_r \in M)$ heißt linkes (rechtes) Nullelement von $(M, *)$ oder bezüglich der Operation "$*$", wenn gilt:*

   $$0_l * m = 0_l \text{ für alle } m \in M \qquad (m * 0_r = 0_r)$$

   (Ein Element $0 \in M$, das gleichzeitig linkes und rechtes Nullelement von $(M, *)$ oder bezüglich der Operation "$*$" ist, heißt kurz Nullelement.)

Beispiel 1.2.2.

1. $(\mathbb{N} \cup \{0\}, \cdot)$, "$\cdot$"-gewöhnliche Multiplikation, 1 ist $\mathbf{1}$-Element, 0 ist 0-Element
2. In $(\mathbb{N} \cup \{0\}, +)$, "$+$"-Addition, 0 ist $\mathbf{1}$-Element, (neutrales Element)
3. Sei $M \neq \emptyset$ beliebig, "$*$" gegeben durch $n * m := m$ für alle $n, m \in M$
   Jedes n ist linkes $\mathbf{1}$-Element
   Jedes m ist rechtes 0-Element

Satz 1.2.3. *Existiert in einer algebraischen Struktur $(M, *)$ gleichzeitig ein linkes und ein rechtes* **1***-Element (*0*-Element), so stimmen diese überein und sind eindeutig (d.h., wenn überhaupt, dann existiert genau ein* **1***-Element [*0*-Element]).*

Beweis. Sei $e_l \in M$ ein linkes und $e_r \in M$ ein rechtes **1**-Element, d.h., $e_l * m = m$ bzw. $m * e_r = m$ für alle $m \in M$.
Wir setzen:

$$m := e_r \qquad m := e_l \tag{1.1}$$

$$\Rightarrow e_l * e_r = e_r \qquad \Rightarrow e_l * e_r = e_l \tag{1.2}$$

$$\Rightarrow e_r = e_l$$

□

Bemerkung 1.2.4. *Wie Beispiel $(1.2.2(3))$ zeigt, können beliebig viele 0-Elemente bzw.* **1***-Elemente existieren, wenn jedoch ein rechtes und ein linkes* **1***-Element (*0*-Element) existieren, so gibt es nur genau ein* **1***-Element (*0*-Element). Siehe auch Beweis $(1.2 - 3)$.*

Definition 1.2.5. *Sei $(M, *)$ eine algebraische Struktur mit* **1***-Element $e \in M$. Das Element $x \in M$ (in $(M, *)$) heißt von links (rechts) invertierbar, wenn ein Element $y \in M$ existiert, mit*

$$y * x = e \qquad (x * y = e)$$

Das Element y heißt Links- (Rechts-) Inverse von x. Ist x beidseitig invertierbar, so heißt x kurz invertierbar und y eine Inverse zu x.
(Schreibweise für $y : x^{-1}$ oder $-x$)

Bemerkung 1.2.6. *Das* **1***-Element $e \in M$ ist stets invertierbar (da $e * e = e$)*

Beispiel 1.2.7.

1. $(\mathbb{N} \cup \{0\}; +)$*, neutrales Element* 0*, aber $n \neq 0, n \in \mathbb{N} \cup \{0\}$ nicht invertierbar*
2. *In $(\mathbb{Z}, +)$ ist jedes Element $x \in \mathbb{Z}$ durch $(-x)$ invertierbar*
3. *Sei $M = \mathbb{R}^{n*n}$ $(= M(n * n, \mathbb{R})$ die Menge der quadratischen Matrizen n-ter Ordnung mit Einträgen aus $\mathbb{R}$ und der Matrizenmultiplikation, dann gilt:*

$$A \in M \text{ in } M \text{ invertierbar } \Leftrightarrow det(A) \neq 0 \quad (det(A^{-1}) = \frac{1}{det(A)})$$

4. *Sei $X \neq \emptyset$, $M = \{f : X \to X\}$, wobei die Komposition Operation auf M ist, d.h*

$$(f \circ g)(x) = f(g(x)), \text{ für alle } x \in X$$

   $(M, \circ)$ ist eine algebraische Struktur und Halbgruppe mit **1***-Element id_x.*
   Es gilt:

(a) $f \in M$ *injektiv* $\Leftrightarrow$ f *von links invertierbar*

(b) $f \in M$ *surjektiv* $\Leftrightarrow$ f *von rechts invertierbar*

5. *Sei* $X = \{(\xi_k)_{k=0}^{\infty} : \xi_k \in \mathbb{R} \quad (k = 0, 1, \ldots)\}$ *und* $M = \{f : X \to X\}$ *mit "*$\circ$*" Komposition (siehe auch* 4.*)*

   Betrachten die Funktion $f \in M$*, wobei* $f((\xi_k)_{k=0}^{\infty}) = (0, \xi_0, \xi_1, \ldots)$ *(Verschiebungsoperatoren) und* $g \circ ((\xi_k)_{k=0}^{\infty}) = (\xi_1, \xi_2, \ldots)$.
   Offenbar ist $g \circ f = id_x \Leftrightarrow g_0$ *eine Links-Inverse zu* f.
   Weitere Links-Inversen für beliebige $\alpha \in \mathbb{R}$ *sind die Funktionen* $g_x \in M$ *und* $g_\alpha((\xi_k)_{k=0}^{\infty}) = (\alpha, \xi_0, \xi_1, \ldots)$.

Satz 1.2.8. *Sei* $(H, *)$ *eine Halbgruppe mit* **1***-Element* e*. Besitzt das Element* $x \in H$ *eine Links- und eine Rechts-Inverse, so stimmen diese überein und sind eindeutig bestimmt (d.h., zu einem invertierbaren Element* $x \in H$ *existiert genau nur eine Inverse).*

Beweis. Sei $y \in M$ eine L-Inverse und $z \in M$ ein R-Inverse zu x, d.h.,

$$y * x = e \qquad x * z = e$$

Wegen der Assoziativität von "$*$" (Halbgruppe) gilt:

$$y = y * e = y * (x * z) = (y * x) * z = e * z = z$$

□

Satz 1.2.9. *Sei* $(H, \circ)$ *eine Halbgruppe mit* **1***-Element* e *und*
$H^* := \{a \in H : a$ *invertierbar in* $(H, \circ)\}$.
Dann gilt:

1. $e \in H^*$
2. $a^{-1} \in H^*$*, für alle* $a \in H^*$ *und* $(a^{-1})^{-1} = a$
3. $a \cdot b \in H^*$ *für alle* $a, b \in H^*$ *und* $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$

Beweis. Sei $(H, \circ)$ eine Halbgruppe mit **1**-Element e und H^* die Menge der in $(H, \circ)$ invertierbaren Elemente.

1. Sei $e \circ e = e$, das **1**-Element $\Rightarrow$ e invertierbar $\Rightarrow e \in H^*$
2. $a^{-1} \circ a = a \circ a^{-1}$, weil a^{-1} Inverse ist, also Links- wie Rechts-Inverse
   $\Rightarrow a^{-1} \circ a = e = a \circ a^{-1} \Rightarrow a^{-1}$ invertierbar mit $a \Rightarrow a \in H^*$ und es gilt:

   $(a^{-1})^{-1} = a,$ da Inverse eindeutig bestimmt ist

3. Zeigen: $a \cdot b \in H^*$ für alle $a, b \in H^*$ und $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$

$$
\begin{aligned}
& a, b \in H^* \Rightarrow a^{-1}, b^{-1} \in H^* \\
& \Rightarrow e = a^{-1} \cdot a, \quad e = b^{-1} \cdot b \\
& \overset{e=e\cdot e}{\Rightarrow} e = b^{-1} \cdot a^{-1} \cdot a \cdot b = abb^{-1}a^{-1} \\
& \Rightarrow e = (b^{-1}a^{-1})(ab) = (ab)(b^{-1}a^{-1}) \\
& \Rightarrow (ab)^{-1} = b^{-1}a^{-1}
\end{aligned}
$$

□

Definition 1.2.10. *Eine Halbgruppe $(G, \cdot)$ mit $\mathbf{1}$-Element e heißt Gruppe, wenn jedes Element von G in $(G, \cdot)$ invertierbar ist.*

Beispiel 1.2.11.

1. $(\mathbb{Z}, +); (\mathbb{Q}, +); (\mathbb{R}, +); (\mathbb{C}, +)$ *sind Gruppen mit dem neutralem Element* 0 *und der Inversen* $(-x)$.
2. $(\mathbb{Q}\backslash\{0\}; \cdot); (\mathbb{R}\backslash\{0\}, \cdot); (\mathbb{C}\backslash\{0\}, \cdot)$ *sind Gruppen mit dem* $\mathbf{1}$*-Element* 1 *und der Inversen* $\frac{1}{x}$
3. *Wenn $(H, \cdot)$ eine Halbgruppe mit $\mathbf{1}$-Element e ist, so ist $(H^*, \cdot)$ eine Gruppe (vergleiche Satz $(1.2 - 9)$)*

Satz 1.2.12. *Sei $(H, \cdot)$ eine Halbgruppe. $(H, \cdot)$ ist eine Gruppe genau dann, wenn gilt:*
Für jedes $a, b \in H$ besitzen die Gleichungen

$$
\begin{aligned}
a \cdot x &= b \qquad (1) \\
y \cdot a &= b \qquad (2)
\end{aligned}
$$

mindestens eine Lösung x bzw. y in H.

Beweis. 1. Sei $(H, \cdot)$ eine Gruppe.

$$
\begin{aligned}
\Rightarrow x &= a^{-1} \cdot b \text{ ist Lösung von } (1) \\
y &= b \cdot a^{-1} \text{ ist Lösung von } (2) \text{ (eindeutig)}
\end{aligned}
$$

2. Sei die Bedingung erfüllt.
   Zeigen, dass eine L-Inverse e_l existiert und dass jedes Element von H von links invertierbar ist.
   Sei $a \in H$ beliebig und $y = e_l$, die Lösung der Gleichung

$$\overline{y} \cdot a = a$$

Weiterhin existieren für alle $b \in H$ ein $x \in H$ mit

$$\begin{aligned} & ax = b \\ \Rightarrow\ & b = ax = (e_l \cdot a)x = e_l(ax) = e_l b \\ \Rightarrow\ & e_l \text{ ist L-Inverse von } H. \end{aligned}$$

Aus (2) folgt für alle $a \in H$ existiert ein $y \in H$ mit $y \cdot a = e_l$ (a von links invertierbar).
Zeigen nun, dass e_l auch R-**1**-Element und y R-Inverse von a ist.
Aus $y \cdot a = e_l \Rightarrow y \cdot a \cdot y = e_l \cdot y = y$
Weiterhin existiert ein $z \in H$ mit $z \cdot y = e_l$ (2)

$$\begin{aligned} \Rightarrow e_l &= z \cdot y = z(y \cdot a \cdot y) \\ &= (z \cdot y)(a \cdot y) = e_l \cdot a \cdot y = a \cdot y \\ &\quad (y \text{ ist R-Inverse von } a) \text{ und} \\ a \cdot e_l &= a(ya) = (ay)a = e_l \cdot a = a \Leftrightarrow e_l \text{ ist auch R-}\mathbf{1}\text{-Element} \end{aligned}$$

□

Folgerung 1.2.13. *In einer Gruppe $(G, \cdot)$ gelten die Kürzungsregeln, d.h., für alle $a, b, c \in G$ muss gelten:*

$$\left.\begin{aligned} a \cdot c = b \cdot c \\ c \cdot a = c \cdot b \end{aligned}\right\} \Rightarrow a = b$$

Folgerung 1.2.14. *Eine endliche Halbgruppe $(H, \cdot)$ (d.h., $|H| < \infty$) ist genau dann eine Gruppe, wenn die Kürzungsregeln gelten.*

Beweis. Sei $a \in H$ beliebig und $f : H \to H$ gegeben durch $f(x) = a \cdot x \quad (x \in H)$ und $g : H \to H$ gegeben durch $g(y) = ya, \quad (y \in H)$.
Aus der Kürzungsregel folgt, dass f, g injektiv sind ,da aus

$$ax_1 = ax_2 \overset{\text{Kürzungsregel}}{\Longrightarrow} x_1 = x_2$$

Analog gilt dies für g:

$$\Rightarrow y_1 = y_2$$

$\Rightarrow f, g$ surjektiv, da $|H| < \infty$
$\Rightarrow$ für alle $b \in H$ existieren $x, y \in H$ mit $ax = f(x) = b$ und $ya = g(y) = b$
$\Rightarrow$ Gleichung ist lösbar

□

Beispiel 1.2.15 (Beispiele für endliche Gruppen).

$$(\{-1, 1\}, \circ), \quad G = \{z \in \mathbb{C} : z^n = 1\} = \{-1, 1, -i, i\}$$

1.3 Faktorstrukturen und Homomorphismus

Definition 1.3.1. *Sei $(M, \cdot)$ eine algebraische Struktur. Die Äquivalenzrelation "$\sim$" auf M heißt verträglich mit der Operation "$\cdot$", wenn aus $x_i \sim y_i \quad (i = 1, 2)$ stets folgt:*

$$x_1 \cdot x_2 \sim y_1 \cdot y_2$$

Bemerkung 1.3.2. *Setzt man in der Definition $(0.1 - 15)$ $M_1 = M \times M$ und $M_2 = M$, sowie $f =$"$\cdot$".*
Setzt man weiter

$$(x_1, x_2) R_1 (y_1, y_2) \overset{Def.}{\Leftrightarrow} x_1 \sim y_1, \quad x_2 \sim y_2$$

und $R_2 =$"$\sim$", so folgt die Definition $(1.3 - 1)$ aus dieser. (R_1 ist Äquivalenzrelation)

Satz 1.3.3. *Sei $(M, \cdot)$ eine algebraische Struktur und "$\sim$" eine Äquivalenzrelation auf M, die mit der Operation "$\cdot$" verträglich ist.*
Die Faktormenge $M/\sim$ wir durch folgende Operation "$\circ$" zu einer algebraischen Struktur.

$$\overline{x} \circ \overline{y} := \overline{x \cdot y} \text{ für alle } \overline{x}, \overline{y} \in M/\sim;$$

d.h., für die kanonische Abbildung $\pi : M \to M/\sim$ gilt:

$$\pi(x \cdot y) = \pi(x) \circ \pi(y) \text{ für alle } x, y \in M$$

Beweis. Zeigen, dass "$\circ$" wohldefiniert ist:
Seien $x, x' \in \overline{X}; y, y' \in \overline{Y}$, d.h.,

$$x \sim x', y \sim y', \text{ da " } \sim \text{ " verträglich ist mit "} \cdot \text{"}$$

$$\Rightarrow x \cdot y \sim x' \cdot y' \Rightarrow \overline{x \cdot y} = \overline{x' \cdot y'}$$

Offenbar gilt: $\overline{x \cdot y} \in M/\sim \quad \Rightarrow$ Behauptung □

Bemerkung 1.3.4.

1. *Anstelle von "$\circ$" auf $M/\sim$ schreibt man wieder "$\cdot$".*
2. *Ist die Operation "$\cdot$" auf M assoziativ oder kommutativ, so auch die Funktion auf der Faktormenge ($M/\sim$).*
   *Ist $e \in M$ **1**-Element bzw. $0 \in M$ Nullelement auf $(M, \cdot)$, so ist entsprechend $\overline{e} \in M/\sim$ bzw $\overline{0} \in M/\sim$ ein solches.*
   Gilt in M (mit e) die Beziehung $x \cdot y = e$ für gewisse $x, y \in M$, so ist:

$$\overline{x} \cdot \overline{y} = \overline{e}$$

Beweis zu 2.. Sei $e \in M$ **1**-Element. Wir zeigen, dass $\overline{e} \in M/\sim$ auch **1**-Element in $M/\sim$ ist:

$$\overline{x} \cdot \overline{e} = \overline{x \cdot e} = \overline{x} \Rightarrow \text{ Behauptung}$$

□

Definition 1.3.5. *Seien $(M_1, *)$ und $(M_2, \circ)$ algebraische Strukturen. Die Funktion $f : M_1 \to M_2$ heißt Homomorphismus von $(M_1, *)$ in $(M_2, \circ)$, wenn gilt:*

$$f(x * y) = f(x) \circ f(y) \text{ für alle } x, y \in M_1$$

Ist f bijektiv, so heißt f ein Isomorphismus von M_1 auf M_2 und die Strukturen $(M_1, *)$ und $(M_2, \circ)$ zueinander isomorph.
(symbolisch schreibt man $(M_1, *) \cong (M_2, \circ)$ oder kurz $M_1 \cong M_2$)

Bemerkung 1.3.6. *Ist $f : M_1 \to M_2$ ein Isomorphismus, so ist $f^{-1} : M_2 \to M_1$ auch ein Isomorphismus.*

Beweis. Seien $x', y' \in M_2$ beliebig $\overset{f \text{ bijektiv}}{\Rightarrow}$, so existieren genau ein x und $y \in M_1$ mit $f(x) = x'$ und $f(y) = y'$.

$$\Rightarrow f^{-1}(x' \circ y') = f^{-1}(f(x) \circ f(y)) = f^{-1}(f(x * y)) = x * y = f^{-1}(x') * f^{-1}(y')$$
$$\Rightarrow \text{ Behauptung}$$

□

Beispiel 1.3.7.

1. $M_1 = \mathbb{R}$, "$*$"="+";$M_2 = (0; \infty)$, "$\circ$"'='"$\cdot$"
   $f : M_1 \to M_2$ *mit* $f(x) = exp(x) = e^x$
   $exp(x + y) = exp(x) \cdot exp(y)$
   f *bijektiv* $\Rightarrow$ *Isomorphismus*

2. $M_1 = M(n \times n, \mathbb{C})$ *mit Matrizenmultiplikation und* $M_2 = \mathbb{C}$ *mit* "$\cdot$"
   $f : M_1 \to M_2$ *mit* $f(A) = det(A)$
   Es gilt: $f(A \cdot B) = f(A) \cdot f(B) = det(A) \cdot det(B)$
   $\Rightarrow$ *Homomorphismus*

3. *Die kanonische Abbildung in Satz* $(1.3-3)$ *ist ein Homomorphismus, genannt kanonischer Homomorphismus*

Definition 1.3.8.

1. *Sei $(M, *)$ eine algebraische Struktur und $\emptyset \neq N \subseteq M$. $(N, *)$ heißt Unter- oder Teilstruktur von $(M, *)$, wenn gilt:*

   $$n_1 * n_2 \in N$$

   für alle $n_1, n_2 \in N$, (d.h., $(N, *)$ ist algebraische Struktur)

2. *Sei $f : (M_1, *) \to (M_2, \circ)$ ein Homomorphismus. Die Menge*

$$im(f) := \{y \in M_2 : \text{ es existiert ein } x \in M_1 \text{ mit } y = f(x)\}$$

heißt Bild des Homomorphismus.

3. *Sei $f : (M_1, *) \to (M_2, \circ)$ ein Homomorphismus und e_2 ein* **1***-Element in $(M_2, \circ)$.*
Die Menge

$$ker(f) := \{x \in M_1 : f(x) = e_2\}$$

heißt Kern des Homomorphismus von f.

Bemerkung 1.3.9. *Die Mengen $im(f)$ und $ker(f)$ (wenn $ker(f) \neq \emptyset$) sind entsprechend Unterstrukturen von $(M_2, \circ)$ bzw. $(M_1, *)$.*

Beweis. Sei $x_1, x_2 \in ker(f)$. Wir betrachten:

$$\begin{aligned} &f(x_1 * x_2) \overset{\text{Hom.}}{=} f(x_1) \circ f(x_2) = e_2 \circ e_2 = e_2 \\ &\Rightarrow x_1 * x_2 \in ker(f) \end{aligned}$$

□

Satz 1.3.10 (Homomorphiesatz). *vergleiche Folgerung (0.1-19)*
Sei $f : (M_1, *) \to (M_2, \cdot)$ ein Homomorphismus; $(M_1/Rel(f), *) =: (M, *)$ die Faktorstruktur von M_1 nach $Rel(f)$ (vergleiche Beispiel $(0.1 - 4)$) und $\pi : M_1 \to M/Rel(f)$ der kanonische Homomorphismus.
Dann existiert genau ein injektiver Homomorphismus $\overline{f} : (M, *) \to (M_2, \cdot)$ mit

$$f = \overline{f} \circ \pi$$

$$\begin{array}{ccc} M_1 & \xrightarrow{f} & M_2 \\ \downarrow{\scriptstyle \pi} & \nearrow{\scriptstyle \overline{f}} & \\ M/Rel(f) & & \end{array}$$

Beweis. Folgt eigentlich aus dem Satz $(0.1 - 17)$.
Noch einmal wesentliche Teile:

Def.:

$\overline{f} : (M, *) \to (M_2, \cdot)$ wie folgt:
$\overline{f}(\overline{x}) := f(x) \qquad (x \in \overline{X})$ für alle $\overline{x} \in M$
Wir zeigen: $\overline{f}$ ist wohldefiniert.
Sei $x, x' \in \overline{X},$ d.h., $xRel(f)x' \Leftrightarrow f(x) = f(x')$
$\Rightarrow \overline{f}(\overline{x}) = f(x') \Rightarrow$ wohldefiniert
$\Rightarrow f(x) = \overline{f}(\overline{x}) = \overline{f}(\pi(x)) = (\overline{f} \circ \pi)(x)$ für alle $x \in M_1$
$f = \overline{f} \circ \pi$

Zeigen nun, dass $\overline{f}$ injektiv ist.
$Sei \overline{f}(\overline{x}) = \overline{f}(\overline{y}) \Leftrightarrow f(x) = f(y) \Leftrightarrow xRel(f)y \Leftrightarrow \overline{x} = \overline{y}$
Zeigen noch, dass $\overline{f}$ Homomorphismus ist.
$\overline{f}(\overline{x} * \overline{y}) = \overline{f}(\overline{x * y}) = f(x * y) = f(x) \cdot f(y) = \overline{f}(\overline{x}) \cdot \overline{f}(\overline{y})$
$\Rightarrow$ Behauptung

□

Folgerung 1.3.11 (Isomorphiesatz). *Betrachtet man den obigen Homomorphismus $\overline{f}$ als Abbildung von M auf $im(f)$, so ist $\overline{f} : M \to im(f)$ bijektiv und damit ein Isomorphismus zwischen M und $im(f)$, d.h.,*

$$(M_1/Rel(f), *) \cong (im(f), \cdot)$$

Beispiel 1.3.12.

1.

$M_1 = M(n \times n, \mathbb{C})$ *mit der Matrixmultiplikation,* $M_2 = \mathbb{C}$ *mit Multiplikation*
$f : M_1 \to M_2$ *gegeben durch* $f(A) = det(A)$
dann gilt: $f(A \cdot B) = det(A \cdot B) = det(A) \cdot detB = f(A) \cdot f(B)$
$\Rightarrow f$ *ist Homomorphismus*
$ARel(f)B \overset{Definition}{\Leftrightarrow} det(A) = det(B)$
$im(f) = \mathbb{C} \Rightarrow M_1/Rel(f) \cong \mathbb{C}$

2.

$M_1 = C[0,1],$ *reellwertige, stetige Funktionen auf* $[0,1]$ *mit punktweiser Multiplikation,*
$M_2 = \mathbb{R}$ *mit Multiplikation*
$f : M_1 \to M_2$ *mit* $f(x) = (\frac{1}{2})x$
offenbar ist $im(f) = \mathbb{R}$
f *ist Homomorphismus*
$xRel(f)y \Leftrightarrow (\frac{1}{2})x = (\frac{1}{2})y$
$M_1/Relf(f) \cong \mathbb{R}$

Kapitel 2

Gruppentheorie

2.1 Definitionen und Beispiele

Definition 2.1.1. *Eine algebraische Struktur $(G, \quad)$ heißt Gruppe, wenn folgende Gruppenaxiome gelten:*

1. $(ab)c = a(bc)$ *für alle* $a, b, c \in G$ *(Assoziativgesetz)*
2. *Es existiert ein* $e \in G : ea = ae = a$ *für alle* $a \in G$ *(***1***-Element)*
3. *Für alle* $a \in G$ *existiert ein* $a^{-1} \in G : a^{-1}a = aa^{-1} = e$ *(Inverses Element)*

   Eine Gruppe heißt abel'sche Gruppe oder kommutative Gruppe, wenn gilt:

4. $ab = ba$ *für alle* $a, b \in G$
   $(H, \quad)$ *Halbgruppe mit* $e \Rightarrow \quad (H^*, \quad)$ *Gruppe*

Beispiel 2.1.2.

1. *Sei* $m \in \mathbb{Z}$ *mit* $m \geq 1$ *und* $\mathbb{Z}_m$ *die Menge der Restklassen* $mod \quad (m)$. *(dabei ist Äquivalenzrelation wie folgt auf* $\mathbb{Z}$ *erklärt:*

$$\begin{aligned} x \equiv y \quad mod(m) &\Leftrightarrow m|x - y \\ &\Rightarrow \mathbb{Z}_m := \{\overline{0}, \overline{1}, \ldots, \overline{m-1}\} \\ Add : \overline{x} + \overline{y} &:= \overline{x+y} \\ \overline{x} \cdot \overline{y} &:= \overline{x \cdot y} \end{aligned}$$

   $(\mathbb{Z}_m, +)$ *ist eine abel'sche Gruppe mit neutralem Element* $\overline{0}$ *und der Inversen* $\overline{-x}$ *von* $\overline{x}$.

2. $G = \{\begin{pmatrix} a & b \\ -b & a \end{pmatrix} : a, b \in \mathbb{R}, a^2 + b^2 \neq 0\}$ *und der Matrixmultiplikation ist eine abel'sche Gruppe (siehe Übung 2)*

3. $(\mathbb{Z}_m, \cdot)$ *ist offenbar eine Halbgruppe mit* **1***-Element* $\overline{1}$ *(*$\overline{1} \cdot \overline{x} = \overline{1 \cdot x} = \overline{x}$*)*
$m = 4 : \mathbb{Z}_4 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\} \Rightarrow \overline{2} \cdot \overline{2} = \overline{2 \cdot 2} = \overline{4} = \overline{0}$
Was ist $\mathbb{Z}_m^*$*?*
Behauptung: $\mathbb{Z}_m^* = \{x \in \mathbb{Z}_m : m$ *und* x *sind teilerfremd*$\}$

Beweis.

1. Sei $\overline{x} \in \mathbb{Z}_m^* \Rightarrow$ es existiert ein $\overline{y} \in \mathbb{Z}_m : \overline{xy} = \overline{1}$
$\Rightarrow xy - 1 = (-k)m, \quad [(-k) \in \mathbb{Z}]$
$\Rightarrow xy + km = 1 \Rightarrow ggT(x, m) = 1$
$\Rightarrow x$ und m sind teilerfremd

2. Sei umgekehrt x, m teilerfremd, d.h., $ggT = 1$
$\overset{\text{0.Übung}}{\Longrightarrow}$ es existieren $y, k \in \mathbb{Z} : xy + km = 1$
$\Rightarrow xy - 1 = -km$
$\Rightarrow m|xy - 1 \Leftrightarrow \overline{xy} = \overline{1} \Rightarrow \overline{x} \cdot \overline{y} = \overline{1} \Rightarrow \overline{x} \in \mathbb{Z}_m^*$

$\mathbb{Z}_m^*$ - prime Restklassengruppe $mod(m)$
$\mathbb{Z}_p^* = \{\overline{1}, \overline{2}, \ldots, \overline{p-1}\}, \quad p \geq 2$ Primzahl □

Bemerkung 2.1.3. *Die Anzahl* $\varphi(m)$ *der Elemente von* $\mathbb{Z}_m^*$ *heißt Eulersche Phi-Funktion, d.h.,* $\varphi(m) =$ *Anzahl der natürlichen Zahlen* x *mit* $1 \leq x \leq m$*, die zu* m *teilerfremd sind.*

Beispiel 2.1.4.

1. *Für die Primzahl* $p \geq 2$ *ist* $\varphi(p) = p - 1$

2. *Sei* $X \neq \emptyset, M = \{f : X \to X\}$ *mit der Komposition als Operation auf* M*. Offenbar ist* $(M, \circ)$ *eine Halbgruppe mit* **1***-Element* id_x*.*
Bekanntlich gilt:

$$(M^*, \circ) = \{f : X \to X | f \text{ bijektiv}\}$$
$$S(X) - \text{ die symetrische Gruppe auf } X =: S(X)$$

Ist $X = \{1, \ldots, n\}$*, so sei* $S_n := S(\{1, \ldots, n\})$
Ein Element von S_n *ist eine Permutation vom Grade* n*.*

2.2 Untergruppen

Definition 2.2.1. *Sei G eine Gruppe mit $\mathbf{1}$-Element e.*

1. *Jede nichtleere Teilmenge $K \subseteq G$ von G heißt ein Komplex von G. Wir setzen:*
2. $KL := \{kl : k \in K \text{ und } l \in L\}$ *(Komplexprodukt)*
   $K^{-1} := \{k^{-1} : k \in K\}$ *bei K, L Komplexe von G*
3. *Ein Komplex U von G heißt Untergruppe, wenn U mit der Operation von G selbst wieder eine Gruppe bildet. (kurz $U \leq G$)*

Satz 2.2.2. *Sei G eine Gruppe mit $\mathbf{1}$-Element e und sei $U \subseteq G$ ein Komplex. Dann sind nachfolgende Beziehungen äquivalent:*

1. *U ist Untergruppe von G*
2. *$u, v \in U \Rightarrow uv \in U$ und $u^{-1} \in U$*
3. *$UU \subseteq U$ und $U^{-1} \subseteq U$*
4. *$UU = U$ und $U^{-1} = U$*
5. *$u, v \in U \Rightarrow uv^{-1} \in U$*
6. *$UU^{-1} \subseteq U$*
7. *$UU^{-1} = U$*

Beweis.

$1 \Rightarrow 2$: U ist Gruppe $\Rightarrow$ $(u, v) \mapsto uv$ für alle $u, v \in U$ ist die Abbildung von $U \times U$ in U. Bezüglich dieser Operation auf U besitzt U ein $\mathbf{1}$-Element e_u (d.h., $e_u \cdot u = u \cdot e_u = u$).

Zeigen: $e_u = e$

$$e_u = e \cdot e_u = (e_u^{-1} e_u) e_u = e_u^{-1}(e_u e_u) = e_u^{-1} e_u = e$$

Wegen $(u, v) \mapsto uv$, für alle $u, v \in U$ ist $uv \in U$ für alle $u, v \in U$.
Zeigen: $u^{-1} \in U$ für alle $u \in U$
Sei $u \in U \Rightarrow$ es existiert $u^{-1} \in G$, d.h. $u \cdot u^{-1} = e$
Da U selbst eine Gruppe ist, existiert ein $v \in U : uv = e_u = e$.
Da die Inverse eindeutig bestimmt sein muss, gilt:
$v = u^{-1} \Rightarrow u^{-1} \in U$

$2 \Leftrightarrow 3$: trivial

$3 \Rightarrow 4$: Für $u \in U$ gilt:

$$e = uu^{-1} \in UU^{-1} \subseteq UU \subseteq U$$

also ist $e \in U$.

$$\Rightarrow U = Ue \subseteq UU \subseteq U \Rightarrow UU = U$$

Weiter folgt aus $U^{-1} \subseteq U$ sofort $U = (U^{-1})^{-1} \subseteq U^{-1} \subseteq U$
$\Rightarrow U^{-1} = U$

$2 \Rightarrow 5$: Für $u, v \in U \Rightarrow uv^{-1} \in UU^{-1} \subseteq UU \subseteq U$

$5 \Leftrightarrow 6$: trivial

$6 \Rightarrow 7$: Mit $u \in U$ ist $e = uu^{-1} \in UU^{-1} \subseteq U$.
Wegen $e = e^{-1}$ ist $e \in U^{-1}$, so dass gilt:

$$U = Ue \subseteq UU^{-1} \subseteq U \Rightarrow UU^{-1} = U$$

$7 \Rightarrow 1$: Es ist $e = uu^{-1} \in U \quad (u \in U)$. Damit folgt

$$U^{-1} = eU^{-1} \subseteq UU^{-1} = U \Rightarrow u^{-1} \in U \text{ für alle } u \in U$$

Weiter gilt für $u, v \in U : uv = u(v^{-1})^{-1} \in UU^{-1} \subseteq U$
$\Rightarrow (u, v) \mapsto uv$ ist eine Operation auf U mit dem $\mathbf{1}$-Element e.
$\Rightarrow U$ ist selbst eine Gruppe (Assoziativgesetz ist trivialerweise erfüllt.)

□

Satz 2.2.3. *Eine endlicher Komplex U der Gruppe G ist genau dann Untergruppe zu G, wenn gilt:*

$$UU \subseteq U \qquad (*) \quad (\textit{d.h. } u, v \in U \Rightarrow uv \in U)$$

Beweis.

1. $(*) \Rightarrow U$ ist ein Halbgruppe. Da in G die Kürzungsregeln gelten, so gelten diese auch in U.
   Mit $|U| < \infty$ folgt die Behauptung aus Folgerung $(1.2 - 14)$.

2. Sei $u \in U$. Wegen $(*)$ folgt: $u^2 \in U$
   $\Rightarrow u^2 \cdot u \in U$. Per vollständiger Induktion folgt $u^n \in U$ für alle $n \geq 1$.
   Da $|U| < \infty$ müssen in einer unendlichen Folge $\{u^n\}$ Wiederholungen auftreten, d.h., es existieren $k, j \geq 1$ und $k > j$ mit $u^k = u^j$.
   Nach dem Kürzen folgt: $u^{k-j} = e \Rightarrow e \in U$ und $u^{k-j-1}u = uu^{k-j-1} = u^{k-j} = e$
   $\Rightarrow u \in U$ ist invertierbar $\Rightarrow$ Behauptung

□

Beispiel 2.2.4.

a) $\{e\}, G$ *sind die trivialen Untergruppen der Gruppe* G

b) Sei $U \leq G$ *und* $V \leq U \Rightarrow V \leq G$

c) $(\mathbb{Z}, +) \leq (\mathbb{R}, +) \leq (\mathbb{C}, +)$

d) Sei $n \in \mathbb{N}\backslash\{0\}$ *und* $n\mathbb{Z} := \{nz : z \in \mathbb{Z}\}$
Es gilt:$(n\mathbb{Z}, +) \leq (\mathbb{Z}, +)$.
Ist d *ein Teiler von* n*, d.h.,* $n = d \cdot n'$*, so gilt:*
$(n\mathbb{Z}, +) \leq (d\mathbb{Z}, +)$

e) Sei $X \neq \emptyset$ *eine beliebige Menge;* $S(X)$ *eine symetrische Gruppe auf* X *und* $x_0 \in X$ *fix.*
Wir setzen: $U := \{f \in S(X) | f(x_0) = x_0\}$
Dann ist $U \leq S(X)$
$X = \{1, \ldots, n\}, S(X) = S_n$
$x_0 = n \Rightarrow \quad U \cong S_{n-1}$

f) Sei $V = \{e, a, b, c\}$ *die Klein'sche Vierergruppe (,d.h.,* $a^2 = e = b^2, c = ab$*)*
$U_1 = \{e, a\}, U_2 = \{e, b\}, U_3 = \{e, c\}$ *sind Untergruppen von* V.

g) Sei G *eine Gruppe mit* **1***-Element* e*. Für* $a \in G$ *beliebig sei*

$$a_k = \begin{cases} e^k = \overbrace{a \cdot a \cdot \ldots \cdot a}^{k-n-1} & ; \quad k \geq 1 \\ e & ; \quad k = 0 \\ (a^{-1})^{-k} & ; \quad k < 0 \end{cases}$$

Die Menge $U := \{a^k\}$ *ist eine Untergruppe zu* G*, die von* a *erzeugte zyklische Untergruppe*

$$\left(C_n := \{z \in \mathbb{C} : z^n = 1\} \quad \textit{zyklische Gruppe mit } n\textit{-Elementen}\right)$$

Definition 2.2.5. *Sei* G *eine beliebige Gruppe,* $a \in G$ *beliebig und* $U = \langle a \rangle$*, die von* a *erzeugte zyklische Untergruppe.*
Die "Zahl"

$$ord(a) := \begin{cases} \infty & ; \quad \textit{wenn } U \textit{ unendlich ist} \\ n & ; \quad \textit{wenn } |U| = n < \infty \end{cases}$$

heißt die Ordnung des Elementes a *in* G*.*

Bemerkung 2.2.6. *Seien* G, a *wie oben.*

1. *Wenn* $ord(a) = n < \infty$*, so gilt:*

   (a) $ord(a) = min\{k \in \mathbb{N}\backslash\{0\} : a^k = e\}$
   (b) $U = \{e, a, a^2, \ldots, a^{n-1}\}$
   (c) $ord(a) = 1 \Leftrightarrow a = e$

2. *Ist* G *eine endliche Gruppe, d.h.,* $|G| < \infty$*, so gilt:*
   $1 \leq ord(a) \leq |G|$

Satz 2.2.7. *In* $(\mathbb{Z}, +)$ *ist jede Untergruppe* U *von der Gestalt*

$$U = m\mathbb{Z} = \{mz : z \in \mathbb{Z}\} \quad (m \geq 0)$$

Beweis. Für $m = 0; 1$ liegen triviale Untergruppen vor, nämlich $\{0\}, \mathbb{Z}$.
Seien nun $U < \mathbb{Z} \quad (U \neq \mathbb{Z})$ mit $\{0\} \neq U$
$\Rightarrow$ es existiert $a \neq 0$ mit $a \in U \Rightarrow -a \in U$
$\Rightarrow$ es existiert ein $b > 0$ mit $b \in U$
Sei $m = min\{b > 0 : b \in U\} \qquad (*)$
Da $m \in U \Rightarrow m + m \in U$, d.h., $2m \in U$
$\overset{Induktion}{\Longrightarrow} n \cdot m \in U, n \geq 0 \Rightarrow (-n) \cdot m \in U$ für alle $n \geq 0$
$\Rightarrow m\mathbb{Z} \subseteq U$

Sei $a \in U$ beliebig, dann existieren $q, r \in \mathbb{Z}$, mit $a = mq + r \quad (0 \leq r < m)$.
Da $mq, a \in U \Rightarrow r = a - mq \in U$

Ann.: $r > 0 \Rightarrow m \leq r$ wegen $(*)$. Dies ist ein Widerspruch zu $0 \leq r < m$.
$\Rightarrow r = 0, \quad a = mq \in m\mathbb{Z}$
$\Rightarrow U = m\mathbb{Z}$ □

Bemerkung 2.2.8. *Für beliebige* $m \in \mathbb{N} \cup \{0\}$ *ist* $m\mathbb{Z}$ *eine zyklische Gruppe (additiv geschrieben), die von* m *erzeugt wird.*

Beweis. Sei $U := m\mathbb{Z} \Rightarrow m \in U \Rightarrow m + m \in U$, also $2m \in U \Rightarrow k \cdot m \in U$ für alle $k \in \mathbb{Z}$.
$\Rightarrow$ Behauptung ($m\mathbb{Z} = \langle m \rangle$)
z.B. $f \cdot m = 1 \Rightarrow \mathbb{Z} = \langle 1 \rangle$ □

2.3 Der Satz von Lagrange

Definition 2.3.1. *Sei* G *eine Gruppe und* $U \leq G$ *(*U*-Untergruppe). Die Elemente* $a, b \in G$ *heißen rechts- (bzw. links-) äquivalent* $mod(U)$ *(oder bezüglich* U*), wenn gilt:*

$$ab^{-1} \in U \qquad (a^{-1}b \in U)$$

Bezeichnung: $a \overset{r}{\sim} b \mod(U) \qquad (a \overset{l}{\sim} b \mod(U))$

Satz 2.3.2. *Beide Relationen "$\overset{r}{\sim}$" bzw. "$\overset{l}{\sim}$" sind Äquivalenzrelationen auf G und die dem Element $x \in G$ zugeordneten Äquivalenzklassen haben die Gestalt Ux (Rechtsnebenklasse) bzw. xU (Linksnebenklasse).*

Beweis. $a \overset{r}{\sim} a$ für alle $a \in G$, da $a \cdot a^{-1} = e \in U$.
Sei $a \overset{r}{\sim} b \Rightarrow ab^{-1} \in U \Rightarrow (ab^{-1})^{-1} \in U$, also $ba^{-1} \in U \Rightarrow b \overset{r}{\sim} a$
Sei $a \overset{r}{\sim} b, b \overset{r}{\sim} c$, d.h. $ab^{-1} \in U$ und $bc^{-1} \in U$.
$\Rightarrow (ab^{-1})(bc^{-1}) \in U$, d.h. $ac^{-1} \in U \Rightarrow a \overset{r}{\sim} c$
$\Rightarrow$ "$\overset{r}{\sim}$" ist Äquivalenzrelation auf G.
(Analog beweist man dies für "$\overset{l}{\sim}$")

Zeigen: Für $x \in G$ gilt: $\overline{x} = Ux$

Sei also $a \in Ux$, d.h., es existiert ein $u \in U : a = ux$
$\Rightarrow ax^{-1} = u \in U \Rightarrow a \overset{r}{\sim} x \Rightarrow a \in \overline{x} \Rightarrow Ux \subseteq \overline{x}$
Sei nun $a \in \overline{x} \Rightarrow a \overset{r}{\sim} x \mod(U) \Rightarrow$ es existiert $u = ax^{-1} \in U \Rightarrow a = ux \in Ux \Rightarrow \overline{x} \subseteq Ux$
$\Rightarrow Ux = \overline{x}$ □

Beispiel 2.3.3. $G = (\mathbb{Z}, +), U = m\mathbb{Z} \qquad (m \geq 0$ *fix*$)$
$a \overset{r}{\sim} b \mod(U) \Leftrightarrow a + (-b) \in U \Leftrightarrow a - b \in U = m\mathbb{Z} \Rightarrow m | a - b \Rightarrow a \equiv b \mod(m)$

Satz 2.3.4. *Sei G eine Gruppe, $U \leq G$ und $g \in G$ fix. Dann gilt:*

(a) Die Funktion $f_1 : U \to U_g$ mit $f_1(u) = ug \quad (u \in U)$ ist bijektiv, insbesondere gilt:

$$|Ux| = card(Ux) = |U| = card(U) \text{ (Mächtigkeit)}$$

(b) Die Funktion $f_2 : G/\overset{r}{\sim} \to G/\overset{l}{\sim}$ mit $f_2(Ux) = x^{-1}U \quad (Ux \in G/\overset{r}{\sim})$ ist bijektiv, d.h., $|G/\overset{r}{\sim}| = |G/\overset{l}{\sim}|$

Beweis.

zu (a) : Offenbar ist die Funktion $h_1 : U_g \to U$ mit $h_1(ug) = u$ die Umkehrfunktion zu $f_1 \Rightarrow$ Behauptung

$$\Big((h_1 \circ f_1)(u) = h_1(f_1(u)) = h_1(ug) = u \Rightarrow h_1 \circ f_1 = id_u\Big)$$

zu (b) : Zeigen: f_2 ist wohldefiniert
Sei $Ux = Uy \Leftrightarrow xy^{-1} \in U \Leftrightarrow (x^{-1})^{-1}y^{-1} \in U \Leftrightarrow x^{-1} \overset{l}{\sim} y^{-1} \Leftrightarrow x^{-1}U = y^{-1}U$
Wegen der Gültigkeit von $\Leftarrow$ gilt: f_2 ist injektiv.

Zeigen: f_2 ist surjektiv
Sei $yU \in G/\overset{r}{\sim} \Rightarrow f_2(Uy^{-1}) = (y^{-1})^{-1}U = yU$
$\Rightarrow f_2$ ist surjektiv $\Rightarrow$ Behauptung

□

Definition 2.3.5. *Sei G eine Gruppe und $U \leq G$. Die Anzahl verschiedener Rechtsnebenklassen, d.h. die Mächtigkeit von $G/\overset{r}{\sim}$, bezüglich der Untergruppe U in G heißt Index von U in G. Bezeichnung: $[U : G]$*

Bemerkung 2.3.6. *Es gilt:*

1. $[G : \{e\}] = |G|$
2. $[G : G] = 1$
3. $[\mathbb{Z} : m\mathbb{Z}] = m$

Satz 2.3.7 (Satz von Lagrange). *Sind für Untergruppen U von G je zwei der Größen $|G|, |U|, [G : U]$ endlich, so auch die dritte, und es gilt:*

$$|G| = [G : U] \cdot |U| \qquad \left(\textit{oder} [G : U] = \frac{|G|}{|U|}\right)$$

Beweis. Sei $G = U_g, \quad g \in V$ (V-Vertretersystem)

$$\begin{aligned} |G| &= \sum_{g \in V} |U_g| \\ &= \sum_{g \in V} |U| = [G : U] \cdot |U|, \\ \text{da } |V| &= [G : U] \Rightarrow \text{ Behauptung} \end{aligned}$$

□

Folgerung 2.3.8. *Sei G eine endliche Gruppe und $U \leq G$. Dann gilt:*

1. *$|U|$ teilt $|G|$*
2. *$ord(a)$ teilt $|G|$ für alle $a \in G$*
3. *(kleiner Fermat'scher Satz)*
   $a^{|G|} = e$ für alle $a \in G$

$$\left(m \geq 1, \quad G = \mathbb{Z}_m^*, \quad a^{\varphi(m)} = 1, \quad m \textit{ mit } ggT(a, m) = 1\right)$$

Beweis.

zu (b) : Sei p eine Primzahl, $\varphi(p) = p-1 \Rightarrow a^{p-1} \equiv 1 \mod(p)$ wenn $p \nmid a \Rightarrow a^p \equiv a \mod(p)$

Sei nun $a = kp \Rightarrow a \equiv 0 \mod(p)$, aber auch $a^p \equiv 0 \mod(p) \Rightarrow a^p \equiv a \mod(p)$.

□

Folgerung 2.3.9. *Sei $G \neq \{e\}$ eine Gruppe, dann gilt:*

1. *Ist $|G| = p$ Primzahl, so ist G zyklisch (d.h., es existiert ein $a \in G/\{e\} : G = \langle a \rangle$)*
2. *$|G| = p$ Primzahl $\Leftrightarrow$ G besitzt nur triviale Untergruppen.*

Beweis.

zu (1) : Sei $|G| = p$ (p-Primzahl)
Vor.: es existiert ein $a \in G/\{e\} \Rightarrow ord(a) \geq 2$

$$\Rightarrow ord(a) = p = |G|$$
$$\Rightarrow U = \langle a \rangle \text{ hat } p \text{ Elemente}$$
$$\Rightarrow U = G, \text{ d.h. } G = \langle a \rangle$$

zu (2) : G besitzt nur triviale Lösungen.

Zeigen: $|G| = p$, (p-Primzahl)

Sei $a \in G/\{e\} \Rightarrow U := \langle a \rangle \neq \langle e \rangle$
Da $U \leq G \Rightarrow U = \langle a \rangle = G$

Ann.:

$|G| = ord(a) = \infty$
$\Rightarrow U_1 = \langle a^2 \rangle$ ist nicht-triviale Untergruppe von G. Dies ist ein Widerspruch zu Voraussetzung
$\Rightarrow |G| = n \leq \infty$

Ann.: Sei n keine Primzahl$\Rightarrow n = n_1 n_2$ mit $n_{1,2} > 1 \Rightarrow \langle a^n \rangle$ ist nicht-triviale Untergruppe von G. Widerspruch
$\Rightarrow$ Behauptung

□

2.4 Gruppenhomomorphismen

Definition 2.4.1. *Seien $(G, *)$, $(H, \circ)$ Gruppen. Die Funktion $\varphi : G \to H$ heißt (Gruppen-)Homomorphismus, wenn gilt:*

$$\varphi(x * y) = \varphi(x) \circ \varphi(y) \qquad \text{für alle } x, y \in G$$

(Bez.:$\varphi \in Hom(G, H)$)

Definition 2.4.2. *Seien G, H Gruppen und $\varphi : G \to H$ ein Homomorphismus, dann gelten folgende Aussagen:*

1. *φ heißt Monomorphismus, wenn φ injektiv ist*
2. *φ heißt Epimorphismus, wenn φ surjektiv ist*
3. *φ heißt Isomorphismus, wenn φ bijektiv ist*
4. *φ heißt Endomorphismus, wenn $\varphi : G \to G$*
5. *φ heißt Automorphismus, wenn $\varphi : G \to G$ bijektiv ist*
6. *G und H heißen isomorph zueinander ($G \cong H$), falls es einen Isomorphismus zwischen G und H gibt.*

Satz 2.4.3. *Seien G, H Gruppen, $\varphi : G \to H$ ein Homomorphismus und $e \in G$ das $\mathbf{1}$-Element zu G. Dann gilt:*

1. *$\varphi(e)$ ist das $\mathbf{1}$-Element zu H*
2. *$\varphi(a^{-1}) = [\varphi(a)]^{-1}$ für alle $a \in G$*
3. *$\varphi(a^n) = [\varphi(a)]^n$ für alle $a \in G$ und $n \in \mathbb{Z}$*

Beweis.

1. Da e $\mathbf{1}$-Element in G ist und φ ein Homomorphismus, so gilt:

   $$\varphi(e) = \varphi(ee) = \varphi(e)\varphi(e)$$

   Dies bedeutet, dass $\varphi(e)$ nur das $\mathbf{1}$-Element in H sein kann.

2. Mit $\varphi(e)$, dem $\mathbf{1}$-Element in H, folgt:

   $$\varphi(e) = \varphi(a^{-1}a) = \varphi(a^{-1})\varphi(a)$$

   Weil die Inverse eindeutig ist, folgt:

   $$\varphi(a^{-1}) = [\varphi(a)]^{-1}$$

3. Für $n = 0$ ist die Aussage bewiesen. (Fall 1)
   Per Induktion für $n > 0$ erhält man dann die Aussage.

□

Satz 2.4.4. *Ein Gruppenhomomorphismus $\varphi : G \to H$ ist genau dann injektiv, wenn*

$$ker(\varphi) = \{e\} \qquad e \in G \text{ (}\mathbf{1}\text{-Element)}$$

Beweis.

1. Sei φ injektiv und $x \in ker(\varphi)$, d.h., $\varphi(x) = e'$ (e' ist $\mathbf{1}$-Element von H). Nun gilt: $\varphi(e) = e'$
   $\Rightarrow \varphi(x) = \varphi(e) \overset{\text{injektiv}}{\Rightarrow} x = e$

2. Sei $ker(\varphi) = \{e\}$
   Zeigen: φ ist injektiv

   Behauptung: $\varphi(x) = \varphi(y) \Rightarrow \varphi(x) \cdot \varphi(y)^{-1} = e'$

   $$\Rightarrow \varphi(x) \cdot \varphi(y^{-1}) = e' = \varphi(x \cdot y^{-1}) \Rightarrow xy^{-1} \in ker(\varphi)$$

   $\Rightarrow xy^{-1} = e \Rightarrow x = y$

□

Satz 2.4.5.

a) Sind $\varphi : G \to H, \quad \psi : H \to K$ Gruppenhomomorphismen, so ist auch $\psi \circ \varphi : G \to K$ ein Gruppenhomomorphismus.

b) Ist $\varphi : G \to H$ ein Isomorphismus, so ist $\varphi^{-1} : H \to G$ auch ein Isomorphismus.

Beweis.

zu (a): Behauptung: $\psi \circ \varphi : G \to K$ ist ein Homomorphismus

$$\varphi : G \to H \text{ ist ein Homomorphismus}$$
$$\Rightarrow \varphi(x * y) = \varphi(x) \cdot \varphi(y) \text{ für alle } x, y \in G \qquad (1)$$

$$\psi : H \to K \text{ ist ein Homomorphismus}$$
$$\Rightarrow \psi(u \cdot v) = \psi(u) \bullet \psi(v) \text{ für alle } u, v \in H \qquad (2)$$

Betrachten:$(\psi \circ \varphi)(x * y)$

$$= \psi(\varphi(x * y)) \overset{(1)}{=} \psi(\varphi(x) \cdot \varphi(y))$$
$$\overset{(2)}{=} \psi(\varphi(x)) \bullet \psi(\varphi(y)) = (\psi \circ \varphi)(x) \bullet (\psi \circ \varphi)(y)$$
$$\Rightarrow \psi \text{ ist ein Homomorphismus von } G \to K$$

zu (b): $\varphi : G \to H$ ist ein Isomorphismus
Behauptung: $\varphi^{-1} : H \to G$ ist auch ein Isomorphismus
φ hat die Eigenschaften eines Homomorphismus und ist zusätzlich bijektiv
$\Rightarrow \quad \varphi^{-1}$ ist bijektiv
$\Rightarrow$ Behauptung

□

Satz 2.4.6. *Sei $G = \langle a \rangle$ eine zyklische Gruppe, dann gilt:*
Ist $|G| = \infty \Rightarrow G \cong (\mathbb{Z}, +)$
Ist $|G| = m < +\infty \Rightarrow G \cong (\mathbb{Z}_m, +)$

Beweis. 1. Sei $|G| = \infty$, d.h $G = \{a^k\}_{k \in \mathbb{Z}}$
Setzen: $\varphi : G \to \mathbb{Z}$ mit $\varphi(a^k) = k$
Wegen $\varphi(a^k \cdot a^l) = \varphi(a^{k+l}) = k + l = \varphi(a^k) + \varphi(a^l)$ ist φ ein Homomorphismus.
Offenbar ist φ bijektiv $\Rightarrow G \cong \mathbb{Z}$

2. Sei $|G| = m < \infty \Rightarrow G = \{e, a, a^2, \ldots, a^{m-1}\}$
Setzen: $\varphi : G \to \mathbb{Z}_m$ mit $\varphi(a^k) = \overline{k} \qquad (k = 0, \ldots, m-1)$
Wegen
$$a^k \cdot a^l = \begin{cases} a^{k+l} & ; \quad k + l < m \\ a^{k+l-m} & ; \quad k + l \geq m \end{cases}$$
Dann gilt: $\varphi(a^k \cdot a^l) = \varphi(a^{k+l}) = \overline{k+l} = \overline{k} + \overline{l} = \varphi(a^k) + \varphi(a^l)$
φ ist ein Homomorphismus und bijektiv
$\Rightarrow$ Behauptung

□

2.5 Normalteiler, Faktorgruppen, Isomorphiesätze

Definition 2.5.1. *Eine Untergruppe N von G heißt Normalteiler von G (kurz: $N \trianglelefteq G$) wenn gilt:*

$$aNa^{-1} \subseteq N \textit{ für alle } a \in G$$

Beispiel 2.5.2.

1. *In jeder abel'schen Gruppe ist jede Untergruppe Normalteiler*
2. $G, \{e\}$ *sind Normalteiler von* G
3. *Das Zentrum* $Z(G) := \{x \in G : xy = yx$ *für alle* $y \in G\}$ *der Gruppe* G *ist Normalteiler von* G
4. *Jede Untergruppe* $U \leq G$ *mit* $[G : U] = 2$ *ist Normalteiler von* G

Satz 2.5.3. *Sei* $N \leq G$*. Dann sind folgende Aussagen äquivalent:*

(a) N *ist Normalteiler von* G

(b) $aNa^{-1} = N$ *für alle* $a \in G$

(c) $aN = Na$ *für alle* $a \in G$

(d) $aN \subseteq Na$ *für alle* $a \in G$

(e) $xy^{-1} \in N \Leftrightarrow x^{-1}y \in N$

Beweis.

(a) $\Rightarrow$ (b) : Sei $N \trianglelefteq G$, d.h. $aNa^{-1} \subseteq N$ für alle $a \in G$.
wir ersetzen a durch a^{-1}: $aNa^{-1} \subseteq N$, da $a^{-1}N(a^{-1})^{-1} \subseteq N$
$\Rightarrow N = aa^{-1}Naa^{-1} = a(a^{-1}Na)a^{-1} \subseteq aNa^{-1} \subseteq N$
$\Rightarrow N = aNa^{-1}$

(b) $\Rightarrow$ (c) :

$$\begin{aligned} N &= aNa^{-1} \\ Na &= aNa^{-1}a \\ \Rightarrow Na &= aNe = aN \end{aligned}$$

c) $\Rightarrow$ d) : trivial

(c) $\Rightarrow$ (e) : Sei $xy^{-1} \in N$ und $aN = Na$ für alle $a \in G$
Zeigen: $x^{-1}y \in N$
Setzen:$n := xy^{-1}$
$\Rightarrow ny = x \Rightarrow x \in Ny = yN$
$\Rightarrow$ es existiert ein $n' \in N : x = yn' \quad |x^{-1}\cdot, \cdot n'^{-1}$
$\Rightarrow x^{-1}y = n'^{-1} \in N$
Analog zeigt man die Umkehrung.

(e) $\Rightarrow$ (a) : Sei $b = ana^{-1}, \quad n \in N, \quad a \in G$
$\Rightarrow n = a^{-1}(ba) \in N \overset{(e)}{\Rightarrow} n' := a(ba^{-1}) \in N \Rightarrow n' = aa^{n-1}b^{-1} = b^{-1} \in N$
$\overset{\text{UG}}{\Rightarrow} b \in N$

$$aNa^{-1} \subseteq N \Rightarrow \text{ Behauptung}$$

□

Beispiel 2.5.4.

1. *Aus $N \trianglelefteq G$, $N \leq U \leq G \Rightarrow N \trianglelefteq U$*
2. *Sei $G(n, \mathbb{R})$ eine Gruppe der invertierbaren Matrizen aus $M(n \times n, \mathbb{R})$. Dann ist $S(n, \mathbb{R}) = \{A \in M(n \times n, \mathbb{R}) : det(A) = 1\}$ ein Normalteiler in $G(n, \mathbb{R})$. (folgt aus $det(BAB^{-1}) = det(A)$).*
3. *Sei $\varphi : G \to H$ ein Gruppenhomomorphismus. Dann ist der $ker(\varphi)$ ein Normalteiler von G.*

Satz 2.5.5. *Sei $U \leq G$ eine Untergruppe von G, dann ist die Äquivalenzrelation "$\overset{r}{\sim}$" ("$\overset{l}{\sim}$") (Definition $(2.3 - 1)$) genau dann vertäglich mit der Gruppenoperation von G, wenn U ein Normalteiler von G ist.*

Beweis.

1. Sei $U \trianglelefteq G$ und $x_i \overset{r}{\sim} y_i \quad mod(U) \quad (i = 1, 2)$, d.h. $u_i := x_i y_i^{-1} \in U \Rightarrow x_i = u_i y_i \quad (i = 1, 2)$
$\Rightarrow x_1 x_2 = u_1(y_1 u_2)y_2$. Nun ist $y_1 y_2 \in y_1 U \overset{\text{NT}}{=} U y_1 \Rightarrow$ es existiert ein $u \in U : y_1 u = u y_1$
$\Rightarrow x_1 x_2 = u_1 u y_1 y_2 \Rightarrow (x_1 x_2)(y_1 y_2)^{-1} = u_1 u \in U$
$\Rightarrow x_1 x_2 \overset{r}{\sim} y_1 y_2 \Rightarrow$ Behauptung
2. Sei $a \in G, \quad u \in U$
$\Rightarrow a \overset{r}{\sim} a, u \overset{r}{\sim} e \Rightarrow au \overset{r}{\sim} ae = a$
$\Rightarrow aua^{-1} \in U \Rightarrow$ Behauptung

□

Satz 2.5.6.

1. *Ist N Normalteiler der Gruppe G, so ist $G/N := \{aN : a \in G\}$ mit der Operation $(aN)(bN) := (ab)N$ die Gruppe, die die Faktorgruppe von G nach N enthält.*
2. $|G/N| = [G : N]$

3. *Die Abbildung $\pi : G \to G/N$ mit $\pi(g) = gN$ ist der Gruppenhomomorphismus mit $ker(\pi) = N \subseteq G$*

Beweis.

zu 1) : Satz $(2.5-5) \Rightarrow$ "$\overset{r}{\sim}$" verträglich mit der Operation
Satz $(1.3-3) \Rightarrow$ Operation auf G/N wohldefiniert
Wegen Satz $(1.3-4)$ ist G/N Halbgruppe mit $\mathbf{1}$-Element eN. Außerdem ist aN durch $a^{-1}N$ in G/N invertierbar.
$\Rightarrow G/N$ ist eine Gruppe.

zu 2) : folgt aus Definition $(2.3-5)$

zu 3) : folgt aus Satz $(1.3-3)$

□

Folgerung 2.5.7. *Ist $N \trianglelefteq G$ und sind je zwei der Gruppen N, G und G/N endlich, so auch die dritte. Gruppe und es gilt:*

$$|G/N| = \frac{|G|}{|N|}$$

Beweis. folgt aus Satz $(2.3-7)$ □

Folgerung 2.5.8. *Ein Komplex U der Gruppe G ist genau dann ein Normalteiler von G, wenn $U = ker(\varphi)$ der Kern eines Gruppenhomomorphismus $\varphi : G \to H$ ist.*

Satz 2.5.9. *Sei $\varphi : G \to H$ ein Gruppenhomomorphismus, $N_1 \trianglelefteq G$ und $N_2 \trianglelefteq H$. Dann ist $\varphi^{-1}(N_2) \trianglelefteq G$ und wenn φ zusätzlich surjektiv ist (d.h., φ ist Epimorphismus), so ist $\varphi(N_1) \trianglelefteq H$.*

Beweis.

1. Seien $x, y \in \varphi^{-1}(N_2) \Rightarrow \varphi(x), \varphi(y) \in N_2 \Rightarrow \varphi(xy^{-1}) = \varphi(x)[\varphi(y)]^{-1} \in N_2$, da $N_2 \leq H \Rightarrow \varphi^{-1}(N_2) \leq G$
   Weiterhin gilt für beliebige $a \in G$: $\varphi(axa^{-1}) = \varphi(a)\varphi(x)[\varphi(a)]^{-1} \in N_2$
   $\Rightarrow axa^{-1} \in \varphi^{-1}(N_2) \Rightarrow \varphi^{-1}(N_2) \trianglelefteq G$

2. Sei $\varphi : G \to H$ surjektiv, $\tilde{x}, \tilde{y} \in \varphi(N_1) \qquad (+)$

   Zeigen: $\tilde{x}\tilde{y}^{-1} \in \varphi(N_1)$

   $\overset{(+)}{\Rightarrow}$ es existieren $x, y \in N_1 : \tilde{x} = \varphi(x), \tilde{y} = \varphi(y)$
   $\Rightarrow xy^{-1} \in N_1$, da $N_1 \leq G$

$\Rightarrow \varphi(xy^{-1}) \in \varphi(N_1)$, d.h. $\varphi(x)[\varphi(y)]^{-1} \in \varphi(N_1) \Rightarrow \varphi(N_1) \leq H$

Zeigen: $\varphi(N_1)$ ist Normalteiler

Sei $a \in H$ beliebig und $\tilde{x} \in \varphi(N_1)$, d.h. $\tilde{x} = \varphi(x)$ mit $x \in N_1$. Da φ surjektiv ist, existiert ein $b \in G : a = \varphi(b)$. Betrachten wir $a\tilde{x}a^{-1} = \varphi(b)\varphi(x)\varphi(b^{-1}) \subset \varphi(N_1)$, da $b \times b^{-1} \in N_1$ (Normalteiler-Eigenschaft)
$\Rightarrow$ Behauptung

□

Definition 2.5.10. *Die Gruppe G heißt einfach, wenn nur triviale Untergruppen Normalteiler in G sind.*

Satz 2.5.11. *Sei $\varphi : G \to H$ ein nichttrivialer Homomorphismus, d.h. $\varphi(a) \neq \{e'\}$.*
Ist G einfach, so ist φ injektiv.

Beweis. Da $ker(\varphi) \trianglelefteq G \Rightarrow ker(\varphi) = \{e\}$ oder $\ker(\varphi) = G$

1. $\Rightarrow$ injektiv
2. $\Rightarrow \varphi(G) = \{e'\}$ Widerspruch

□

Satz 2.5.12 (Homomorphiesatz). *Ist $\varphi : G \to H$ ein Gruppenhomomorphismus, dann existiert genau ein Gruppenkomplement $\Phi : G/ker(\varphi) \to H$ mit $\varphi = \Phi \circ \pi$, wobei $\pi : G \to G/ker(\varphi)$ der kanonische Homomorphismus ist.*

Beweis. Anwendung von Satz $(1.3 - 11)$:
Dort war die Äquivalenzrelation die Relation "$Rel(\varphi)$", d.h. $xRel(\varphi)y \Leftrightarrow \varphi(x) = \varphi(y) \Rightarrow e' = \varphi(x)\varphi(y)^{-1} = \varphi(xy^{-1})$
$\Leftrightarrow xy^{-1} \in ker(\varphi) \Leftrightarrow x \overset{r}{\sim} y \quad mod(ker(\varphi))$
$\Leftrightarrow G/Rel(\varphi) = G/ker(\varphi)$
$\overset{S(1.3-11)}{\Rightarrow}$ Behauptung □

Folgerung 2.5.13. *Ist $\varphi : G \to H$ ein Gruppenhomomorphismus, so gilt:*

$$G/ker(\varphi) \cong \varphi(G)$$

Beweis. Folgerung $(1.3 - 12)$ □

Satz 2.5.14 (1. Isomorphiesatz). *Sei G ein Gruppe, $U \leq G$ und $N \trianglelefteq G$, dann gilt:*

1. $UN \leq G$
2. $U \cap N \trianglelefteq U$
3. $UN/N \cong U/(U \cap N)$

Beweis.

1. Da N Normalteiler von G ist, folgt $aN = Na$ für alle $a \in G$
   $\Rightarrow UN = \bigcup_{u \in U}(uN) = \bigcup_{u \in U}(Nu) = NU$

   Zeigen: $UN \leq G$
   $(UN)(UN) = U(NU)N = UUNN = UN$
   $(UN)^{-1} = N^{-1}U^{-1} = NU = UN$

2. Offenbar ist $N \trianglelefteq UN \qquad (2.5 - 4(1))$

   Sei $\pi : G \to G/N$ der kanonische Homomorphismus und $\pi_0 : U \to G/N$ die Einschränkung von π auf U, d.h. $\pi_0(u) = \pi(u) = uN$ für alle $u \in U$

   π_0 ist ein Homomorphismus.
   Wir bestimmen den Kern von π_0:
   Sei $u \in U$ mit $u \in ker(\pi_0) \Leftrightarrow \pi_0(u) = eN = N$
   $\Leftrightarrow uN = N \Leftrightarrow u \in N \Leftrightarrow ker(\pi_0) = U \cap N \Rightarrow U \cap N \trianglelefteq U$

3. Bestimmung von $\pi_0(U)$:
   $\pi_0(U) = \{uN : u \in U\}$. Wegen $vN = N$ für alle $v \in N$
   $\Rightarrow \pi_0(U) = \{(uv)N : uv \in UN\} = UN/N$
   Aus der Folgerung $(2.5 - 13)$ folgt
   $U/U \cap N = U/ker(\pi_0) \cong \pi_0(U) = UN/N$

□

Folgerung 2.5.15. *Ist $U \leq G, N \trianglelefteq G$ und $|UN| < \infty$, so gilt:*

$$|UN| = \frac{|U||N|}{|U \cap N|}$$

Beweis. $\frac{|UN|}{|N|} = [UN : N] = |UN/N| = |U/U \cap N| = [U : U \cap N] = \frac{|U|}{|U \cap N|}$ □

Satz 2.5.16 (2. Isomorphiesatz). *Sei G eine Gruppe und U, V Normalteiler mit $U \subseteq V$. Dann ist V/U Normalteiler von G/U und es gilt:*

$$(G/U)/(V/U) \cong G/V$$

Beweis. Setzen $\varphi : G/U \to G/V$ mit $\varphi(gU) = gV$.
Zeigen: φ ist wohldefiniert

Sei $gU = hU \Rightarrow gh^{-1} \in U \subseteq V \Rightarrow gV = hV \Rightarrow \varphi$ korrekt definiert.

Offenbar ist φ ein Homomorphismus mit dem Bild G/V

Bestimmen $ker(\varphi)$:
$ker(\varphi) = \{gU : gV = V\} = \{gU : g \in V\} = V/U$
Aus der Folgerung $(2.5 - 13)$:
$(G/U)/(V/U) = (G/U)/ker(\varphi) \cong \varphi(G/U) = G/V$ □

Beispiel 2.5.17.

1. *Sei* $m, n \geq 1$ *natürliche Zahlen und* $\varphi : (m\mathbb{Z}, +) \to (\mathbb{Z}n, +)$ *mit* $\varphi(m\mathbb{Z}) = \overline{z} \in \mathbb{Z}n$ *(Restklasse* $mod(n)$*)*
   φ *ist ein Epimorphismus mit* $ker(\varphi) = mn\mathbb{Z}$
   ($\varphi(mz) = \overline{0} \Rightarrow \overline{z} = \overline{0} \Rightarrow z \in \mathbb{Z} \Rightarrow mz \in m\mathbb{Z}$*)*
   Aus der Folgerung $(2.5 - 13)$ *folgt:*

$$m\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}n$$

2. *Seien* $m, n \geq 1$ *natürliche Zahlen mit* $m = rn, r \in \mathbb{Z} \Rightarrow m\mathbb{Z} \leq n\mathbb{Z}$
   Da $(\mathbb{Z}, +)$ *abgeschlossen ist, sind beide Untergruppen Normalteiler von* $\mathbb{Z}$*.*
   Nach Satz ($2.5 - 16$*) folgt:*

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

Kapitel 3

Strukturs̈atze

3.1 Operationen von Gruppen auf Mengen

Definition 3.1.1. *Sei G eine Gruppe und $X \neq \emptyset$ eine beliebige Menge. Man sagt, G operiert auf X, wenn eine äußere Verknüpfung "$\circ$" auf $G \times X \to X$ mit dem Operationsbereich G existiert und es gilt:*

1. $(gh) \circ x = g \circ (h \circ x)$ *für alle* $g, h \in G$ *und* $x \in X$
2. $e \circ x = x$ *(e ist das* **1***-Element von G)*

Satz 3.1.2. *Eine Gruppe G operiert genau dann auf einer Menge $X \neq \emptyset$, wenn es einen Gruppenhomomorphismus $\Phi : G \to S(X)$ von G in eine symetrische Gruppe $S(X)$ gibt.*
($S(X) = \{f : X \to X | f$ bijektiv$\}$ mit $(f \circ g)(x) = f(g(x))$)

Beweis. 1. Sei $\Phi : G \to S(X)$ ein Homomorphismus, d.h. $\Phi(g) : X \to X$ ist bijektiv. Wir setzen $g \circ x := \Phi(g)(x)$ für alle $g \in G$ und für alle $x \in X$.

Zeigen: Diese Verknüpfung erfüllt Definition $(3.1 - 1(1))$ und $(3.1 - 1(2))$.

Betrachten: $(gh) \circ x = \Phi(gh)(x) \overset{\Phi \text{ ist Hom.}}{=} (\Phi(g) \circ \Phi(h))(x)$

$$= \Phi(g)(\Phi(h)(x)) = g \circ (h \circ x) \Rightarrow \quad (1)$$
$$e \circ x = \Phi(e)(x) = id_x(x) = x \Rightarrow \quad (2)$$
$$\Rightarrow \text{ G operiert auf } X$$

2. Seien die Bedingungen aus Definition $(3.1 - 1)$ erfüllt

Setzen:$\varphi_g : X \to X$ mit $\varphi_g(x) = g \circ x$ für alle $g \in G$ und für alle $x \in X$

Zeigen: φ_g ist bijektiv

Betrachten:

$$\begin{aligned}(\varphi_g \circ \varphi_{g^{-1}})(x) &= \varphi_g(\varphi_{g^{-1}}(x)) = \varphi_g(g^{-1} \circ x) \\ &= g \circ (g^{-1} \circ x) = (gg^{-1}) \circ x = e \circ x = x \\ &\Rightarrow \varphi_g \circ \Phi_{g^{-1}} = id_x(x) \Rightarrow \varphi_g \text{ ist surjektiv} \\ g \circlearrowleft g^{-1} \qquad &\varphi_{g^{-1}} \circ \varphi_g = id_x \Rightarrow \varphi_g \text{ ist injektiv} \\ &\Rightarrow \varphi_g \text{ ist bijektiv, also } \varphi_g \in S(X)\end{aligned}$$

Setzen: $\Phi : G \to S(X)$ mit $\Phi(g) = \varphi_g$

Zeigen: Φ ist ein Gruppenhomomorphismus:

Betrachten:

$$\begin{aligned}\Phi(gh)(x) = \varphi_{gh}(x) &= (gh) \circ x = g \circ (h \circ x) \\ &= \varphi_g(\varphi_h(x)) = \Phi(g)(\Phi(h)(x)) = \Phi(g) \circ \Phi(h)(x) \\ &\Rightarrow \Phi(gh) = \Phi(g) \circ \Phi(h) \Rightarrow \Phi \text{ ist ein Homomorphismus}\end{aligned}$$

□

Beispiel 3.1.3. *Sei G eine endliche Gruppe; $U \lneqq G$; $\quad X = \{gU : g \in G\}$ ist die Menge aller Linksnebenklassen bezüglich U.*
Wir setzen für $a \in G$ und $gU \in X$:

$$a \cdot gU = (ag)U$$

Vermöge dieser Verknüpfung operiert G auf X.
Für $a, b \in G$ gilt:

$$(ab)gU = (abg)U = a(bgU) = a(b \cdot gU)$$

$$e \cdot gU = (eg)U = gU$$

Lemma 3.1.4. *Seien G, U, X wie in Beispiel $(3.1 - 3)$.*

Ist $|G|$ kein Teiler von $([G : U])$!, dann besitzt U einen echten Normalteiler von G.

Beweis. Sei $S(X)$ wie in Satz $(3.1 - 2)$.
Da $|X| = [G : U] < +\infty \Rightarrow |S(X)| = ([G : U])$!

Aus Beispiel $(3.1-3)$ und Satz $(3.1-2)$ folgt, dass ein Homomorphismus Φ existiert, mit

$$\Phi : G \to S(X) \Rightarrow im(\Phi) \leq S(X) \overset{\text{Lagrange}}{\Longrightarrow} |im(\varphi)| \text{ teilt } |S(X)|$$

Außerdem gilt nach dem Homomorphisatz: $im(\Phi) \cong G/ker(\Phi)$
Wenn der $ker(\Phi) = \{e\} \Rightarrow G \cong im(\Phi)$

$$\begin{aligned} &\Rightarrow |G| = |im(\Phi)| \text{ teilt } |S(X)| \Rightarrow \text{ Widerspruch zu Voraussetzung} \\ &\Rightarrow ker\Phi \neq \{e\} \\ &ker(\Phi) \text{ ist Normalteiler von } G \end{aligned}$$

Analysiert man die Basis von Satz $(3.1-2)$, so sieht man, dass $ker(\Phi) \leq U$. □

Satz 3.1.5. *Wenn eine Gruppe G auf X operiert, so ist die Relation $x \overset{G}{\sim} y \Leftrightarrow$ es existiert ein $g \in G : g \cdot x = y$ eine Äquivalenzrelation auf X.*

Beweis.

1. $x \sim x$ gilt, da $ex = x$ für alle $x \in X$ gilt
2. Sei $x \sim y$, d.h. $g \cdot x = y$
   Betrachten: $g^{-1}y = g^{-1}(g \cdot x) = (g^{-1} \cdot g) \cdot x = ex = x \Rightarrow y \sim x$
3. $x \sim y, \quad y \sim z$, d.h. es existieren $g, h \in G$ mit $g \cdot x = y, h \cdot y = z$
   $\Rightarrow (hg)x = h \cdot (g \cdot x) = hy = z \Rightarrow x \sim z$

□

Bemerkung 3.1.6.

1. *Die Äquivalenzklassen $[x] := \{y \in X : x \overset{G}{\sim} y\}$ heißen Orbits (Bahnen) von G in X. Es gilt:*

$$[x] = \{y \in X : \text{ es existiert } g \in G : g \cdot x = y\} = \{g \cdot x : g \in G\} =: G \cdot x$$

2. *Weiter gilt:*
   (a) $X = \bigcup_{x \in X} G \cdot x$
   (b) $G \cdot x = G \cdot y \Leftrightarrow$ *es existiert* $g \in G : gx = y$

Beispiel : Sei G ein Gruppe, $U \leq G$
U operiert auf G vermöge der Abbildung:
$U \times G \to G$ mit $u \cdot g = ug$ für alle $u \in U$ und $g \in G$
Nachweis:

(a) $(uv)g = (uv) \cdot g = u \cdot (v \cdot g)$

(b) $e \cdot g = eg = g$ *für alle* $g \in G$

Orbits hier: $[g] = U \cdot g = Ug$ *Rechtsnebenklassen bezüglich* U

Definition 3.1.7. *Wenn die Gruppe G auf X operiert, so heißt die Menge*

$$G_x := \{g \in G : g \cdot x = x\}$$

der Stabilisator des Elementes $x \in X$ in G.

Satz 3.1.8. *G operiere auf X, dann ist für jedes Element $x \in X$ der Stabilisator G_x eine Untergruppe von G und es gilt:*

$$|G \cdot x| = [G : G_x]$$

Beweis. Sei $h \in G_x$ ($x \in X$ beliebig aber fix)
Zeigen: $h^{-1} \in G$

$h^{-1} \cdot x = h^{-1}(h \cdot x) = (h^{-1} \cdot h) \cdot x = x$
Sei weiter $g \in G_x$
Zeigen: $gh \in G_x$

$(gh) \cdot x = g \cdot (hx) = gx = x$
$\Rightarrow G_x \leq G$

Kostruieren die Bijektion: $f : G \cdot x \to \{$ Linksnebenklassen von G_x bezüglich $G\}$
Setzen für $g \cdot x \in G \cdot x$ folgendes:

$$f(g \cdot x) = gGx$$

Zeigen: f ist wohldefiniert und bijektiv

Sei $h \in G$ mit $g \cdot x = h \cdot x \Rightarrow (h^{-1} \cdot g) \cdot x = h^{-1}(gx) = h^{-1}(hx) = (h^{-1}h) \cdot x = x$
$\Rightarrow h^{-1}g \in G_x \Rightarrow hG_x = gG_x$
$\Rightarrow f$ ist wohldefiniert und surjektiv
Zeigen: f ist injektiv

$f(g \cdot x) = f(h \cdot x) \Rightarrow hG_x = gG_x \Leftrightarrow gx = hx$ (wie oben) □

Folgerung 3.1.9. *Ist $|G| \leq +\infty$, so ist $|G \cdot x|$ Teiler von $|G|$.*

Beweis. Satz von Lagrange

$$|G| = |G_x| \cdot [G : G_x] = |G_x| \cdot |G \cdot x|$$

Bezeichnung: Die Menge $V \subseteq X$ heißt Vertretersystem der Orbits, wenn gilt:

1. Für alle $x \in X$ existiert ein $v \in V$: $\quad G \cdot x = G \cdot v$
2. Aus $v_{1/2} \in V$ mit $v_1 \neq v_2 \Rightarrow G \cdot v_1 \neq G \cdot v_2$

□

Satz 3.1.10. *Wenn eine Gruppe G auf X operiert und $V \subseteq X$ ein Vertretersystem der Orbits ist, so gilt:*

$$|X| = \sum_{v \in V} [G : G_v]$$

Beweis.

$$X = \bigcup_{v \in V} G \cdot v$$

□

Definition 3.1.11. *Operiere die Gruppe G auf X, so wird das Element $\mathbf{x} \in X$ Fixpunkt unter der Gruppenoperation genannt, wenn gilt:*

$$g \cdot \mathbf{x} = \mathbf{x} \qquad \textit{für alle } g \in G$$

Die Gesamtheit dieser Elemente sei $Fix_G(X)$

Bemerkung 3.1.12.

1. *Es gilt: $x \in Fix_G(X) \Leftrightarrow Gx = \{x\} \Leftrightarrow Gx = G \Leftrightarrow [G : G_x] = 1$*
2. *für jedes Untersystem V der Orbits gilt: $Fix_G(X) \subseteq V$*
3. $|X| = |Fix_G(X)| + \sum_{v \in V \textit{ mit } [G:G_v]>1} [G : G_v]$

Satz 3.1.13 (Fixpunktsatz). *Sei G eine Gruppe der Ordnung p^r wobei p eine Primzahl ist (d.h. $|G| = p^r \quad (r \geq 1)$). Wenn G auf einer endlichen Menge X operiert, dann gilt:*

$$|X| \equiv |Fix_G(X) \quad | \quad mod(p)$$

Insbesondere gibt es wenigstens einen Fixpunkt, wenn $|X|, p$ teilerfremd sind.

Beweis. Bemerkung $(3.1-12(1)) \Rightarrow |X| - |Fix_G(X)| = \sum_{v\in V}[G:G_v]$
Nach dem Satz von Lagrange ist $[G:G_v]$ ein Teiler von $|G| = p^r$. Da $[G:G_v] > 1 \Rightarrow$
$[G:G_v] = p^{l(r)} \quad (l(r) \geq 1)$.
$\Rightarrow p| \sum_{v\in V}[G:G_v] = |X| - |Fix_G(X)| \Rightarrow$ Behauptung
$\Rightarrow$ Wenn der $ggT(p,|X|) = 1 \Rightarrow p \nmid |X| \Rightarrow |Fix_G(X)| > 0$ □

Beispiel 3.1.14. *Sei G eine Gruppe und $\emptyset \neq X \subseteq G$ und* $\Gamma := \{gXg^{-1} : g \in G\}$.
(gXg^{-1} heißt eine zu X konjungierte Teilmenge)

Für $h \in G$ und $Y \in \Gamma$ setzen wir hYh^{-1}.
Vermöge dieser Verknüpfung operiert G auf Γ.

$$\left(eYe^{-1} = Y, (h_1,h_2)Y = (h_1,h_2)Y(h_1,h_2)^{-1} = h_1(h_2Yh_2^{-1})h_1^{-1} = h_1(h_2Y)\right)$$

Da $X \in \Gamma$ können wir den Stabilisator zu X aufschreiben

$$G_x = \{g \in G : g \cdot X = X\} = \{g \in G : gXg^{-1} = X\} = \{g \in G : gX = Xg\} =: N(X)$$

(Normalisator von X)
Für $Y \in \Gamma$ betrachten wir den Orbit

$$G \cdot Y = \{h \cdot y : h \in G\} = \{hYh^{-1} : h \in G\}$$

$$\overset{(\exists y\in G: gXg^{-1}=Y)}{=} \{h(gXg^{-1})h^{-1} : h \in G\} = \{(hg)X(hg)^{-1} : h \in G\}$$

wenn h die Gruppe durchläuft, so auch (hg)
$\Rightarrow G \cdot Y = \Gamma$
Nach Satz $(3.1-8)$ gilt dann:

$$|\Gamma| = |GY| = [G:G_y]$$

Insbesondere $|\Gamma| = [G:G_x] = [G:N(X)]$
Wenn wir in diesem Beispiel X durch eine Untergruppe $U \subseteq G$ ersetzen, ergibt sich

Satz 3.1.15. *Die Anzahl verschiedener, konjungierter Untergruppen $gUg^{-1} \quad (g \in G)$ der Untergruppe U ist gleich dem Index des Normalisators von U in G.*

Beispiel 3.1.16. *Sei G ein Gruppe und $X = G$. Setzen wir für $g \in G$ und $x \in X = G$:*

$$g \cdot x := gxg^{-1}$$

Offenbar operiert vermöge dieser Verknüpfung die Gruppe G auf sich selbst (per Konjugation),

Orbits : $G \cdot h = \{ghg^{-1} : g \in G\}$ *(der zu h konjungierten Elemente)*
Stabilisator : $G_x := \{g \in G : g \cdot x = x\} = \{g \in G : gxg^{-1} = x\} = \{g \in G : gx = xg\} = N(X)$

$$\begin{aligned} Fix_G(X) = Fix_G(G) &= \{x \in G = X : gx = x \text{ für alle } g \in G\} \\ &= \{x \in G : gxg^{-1} = x \text{ für alle } g \in G\} \\ &= \{x \in G : gx = xg \text{ für alle } g \in G\} \\ &= Z(G) \quad (\text{Zentrum von } G) \end{aligned}$$

Mit der Bemerkung $(3.1 - 12(3))$ *gilt:*

$$|G| = |Z(G) + \sum_{v \in V} [G : N(X)] \qquad (*)$$

Hieraus folgt:

Satz 3.1.17. *Ist G eine Gruppe mit $|G| = p^r$ (p ist prim mit $r \geq 1$), dann hat G ein nichttriviales Zentrum, d.h. $Z(G) \neq \{e\}$.*

Beweis. Da $Z(G) \leq G \Rightarrow |Z(G)| = p^k$ mit $0 \leq k \leq r$
Aus $(*)$ und wi in Beweis von Satz $(3.1 - 13)$ folgt:
$p||G| - \sum_{v \in V} |G : N(V)| = |Z(G)| \Rightarrow |Z(G)| > 1 \Rightarrow$ Behauptung □

Definition 3.1.18. *Die Gruppe G mit $|G| = p^r$ (p prim, $r \geq 1$) heißt p-Gruppe.*

3.2 Die Sylow'schen Sätze

Lemma 3.2.1. *Sei p Primzahl, $m \in \mathbb{N}$ mit $ggT(m, p) = 1$ und $n = p^r \cdot m \quad (r \geq 1)$, dann gilt:*

$$p^{r-s+1} \nmid \binom{n}{p^r} \text{ für alle } s \text{ mit } 1 \leq s \leq r$$

Beweis. Es ist

$$\binom{n}{p^s} = \frac{n!}{p^s!(n-p^s)!} = \frac{n(n-1)(n-2)\cdot \ldots \cdot (n-p^s+1)}{1 \cdot 2 \cdot \ldots \cdot p^s} = mp^{r-s} \prod_{i=1}^{p^s-1} \frac{mp^r - i}{i}$$

Wir wollen in jedem Faktor aus $\prod_{i=1}^{p^s-1} \frac{mp^r-i}{i} = \binom{n-1}{p^s-1}$, welches eine ganze Zahl ist, die mögliche p-Potenzen kürzen. Wir erhalten dann ein Produkt $\prod \frac{mp^{r_j}-j}{j}$ über gewisse j, die nicht mehr durch p teilbar sind. Nehmen wir an, dass p ein Teiler dieses Produktes sei, dann ist p erst recht Teiler des Produktes der Zähler. Da p eine Primzahl ist, teilt p wenigstens einen Faktor, sagen wir $p \mid mp^{r_k} - k$. Da wir wegen $1 \leq i \leq p^s - 1$ in den Faktoren $\frac{mp^r-i}{i}$ eine kleinere p-Potenz als p^s gekürzt haben, sind die verbleibenden Exponenten r_j sämtlich größer 0. Damit folgt aus $p \mid mp^{r_k} - k$, dass p ein Teiler von k ist. Das widerspricht aber der Tatsachen, dass der $ggT(k, p) = 1$ ist. Also ist p kein Teiler des obigen Produktes und p^{r-s} ist die höchste p-Potenz, in die $\binom{n}{p^s}$ aufgeht. □

Satz 3.2.2 (1. Sylow'scher Satz). *Es gelten die Voraussetzungen wie in Lemma* $(3.2 - 1)$
Ist G eine Gruppe mit $|G| = n = p^r m$, so existiert zu jedem s mit $1 \leq s \leq r$ eine Untergruppe $U \leq G$ mit $|U| = p^s$.

Beweis. Sei $1 \leq s \leq r$ fix und $\Gamma := \{A \subseteq G : |A| = p^s\}$
Bekanntlich gilt: $|\Gamma| = \binom{n}{p^s}$
Wir setzen für $g \in G$ und $A \in \Gamma$:

$$g \cdot A = gA.$$

Da $|gA| = A \Rightarrow gA \in \Gamma$
Vermöge dieser Verknüpfung operiert G auf Γ. (da $e \cdot A = eA = A$, $(gh) \cdot A = (gh)A = g(hA) = g \cdot (hA)$)
Die Orbits sind $G \cdot A$ und für ein Vertretersystem $\mathcal{V}$ der Orbits gilt dann $\Gamma = \bigcup_{V \in \mathcal{V}} G \cdot V$. Aus Satz $(3.1 - 10)$ folgt:

$$\binom{n}{p^s} = |\Gamma| = \sum_{V \in \mathcal{V}} [G : G_V]$$

Aus Lemma $(3.2 - 1)$ folgt: $p^{r-s+1} \nmid \binom{n}{p^s}$
$\Rightarrow$ es existiert $B \in \mathcal{V} : p^{r-s+1} \nmid [G : G_B] =: i$
$\Rightarrow r - s \geq max\{k : p^k \text{ teilt } i\}$

Wegen $p^r m = |G| = i \cdot [G : G_B]$ kommt p in $i|G_B|$ als Faktor r-mal vor, jedoch höchstens $(r - s)$-mal in i.
$\Rightarrow p$ ist in $|G_B|$ mindestens s-mal enthalten
$\Rightarrow p^s$ teilt $|G_B|$
$\Rightarrow |G_B| \geq p^s$

Zeigen: $|G_B| \leq p^s$

$G_B = \{g \in G : g \cdot B = B\}$ (Stabilisator)
Für $g \in G_B$ gilt also: $B = g \cdot B = gB$
$\Rightarrow B = G_B B \Rightarrow$ für $b \in B$ ist $G_B b \subseteq B$.
Nun ist $|G_B| = |G_B b| \leq |B| = p^s$, da $B \in \Gamma$
$\Rightarrow |G_B| = p^s$ und bekanntlich ist $G_B \subseteq G$ □

Folgerung 3.2.3 (Satz von Cauchy). *Sei G eine endliche Gruppe und p eine Primzahl. Wenn p $|G|$ teilt, so existiert ein $g \in G$ mit $ord(g) = p$.*

Beweis. Nach 1. Sylow'schen Satz existiert $U \subseteq G$ mit $|U| = p$
$\Rightarrow U$ zyklisch
$\Rightarrow$ es existiert $g \in U$, so dass $U = \langle g \rangle$

$$\Big(\Rightarrow ord(g) = |U| = p\Big)$$

□

Definition 3.2.4. *Sei $U \leq G$ eine Untergruppe von G. U heißt p-Sylow-Gruppe von G, wenn gilt:*

1. *U ist p-Untergruppe von G (d.h. $|U| = p^a$)*
2. *Ist H eine p-Untergruppe von G mit $U \subseteq H$, so ist $U = H$.*

Bemerkung 3.2.5.

1. *Die p-Sylow-Gruppen sind wegen Def. $(3.2 - 4(2))$ max. unter den p-Untergruppen von G.*
2. *Jede p-Gruppe ist gleich ihrer einzigen p-Sylow-Gruppe.*

Satz 3.2.6. *Sei G wie in Satz $(3.2 - 2)$, (d.h. $|G| = p^r m$) dann ist jede Untergruppe $U \leq G$ mit $|U| = p^r$ eine p-Sylow-Gruppe von G.*

Beweis. Nach Satz $(3.2 - 2)$ existiert eine Untergruppe $U \leq G$ mit $|U| = p^r \Rightarrow U$ ist p-Untergruppe von G.
Sei $H \leq G$ mit $U \leq H$ und $|H| = p^l$.
Nach Satz von Lagrange gilt : $p^l \mid p^r m \Rightarrow l \leq r$
$\Rightarrow |H| \leq |U| \Rightarrow H = U$ □

Folgerung 3.2.7. *G sei wie in Satz $(3.2 - 2) \Rightarrow |U| = p^r$*

Lemma 3.2.8. *Ist U eine p-Untergruppe (bzw. eine p-Sylow-Gruppe) der Gruppe G, so sind alle konjugierten Untergruppen $gUg^{-1} \quad (g \in G)$ eine p-Gruppe (bzw. p-Sylow-Gruppe) in G.*

Beweis. Sei $U \subseteq G$ mit $|U| = p^a \quad (a \geq 1)$. Offenbar ist $|gUg^{-1}| = |U|$
$\Rightarrow |gUg^{-1}| = p^a \Rightarrow gUg^{-1}$ ist eine p-Untergruppe von G.
Sei nun $U \leq G$ eine p-Sylow-Gruppe.

Ann.: gUg^{-1} sei keine p-Sylow-Gruppe
$\Rightarrow$ es existiert eine p-Sylow-Gruppe H von G mit $gUg^{-1} \subsetneq H$
$\Rightarrow U \subsetneq g^{-1}Hg = (g^{-1})H(g^{-1})^{-1}$
Dies ist ein Widerspruch zur Behauptung □

Satz 3.2.9 (2. Sylow'scher Satz). *Sei G wie in Satz $(3.2 - 2)$ (d.h. $|G| = p^r m$) und sei P eine p-Sylow-Gruppe von G.*
Zu jeder p-Untergruppe U von G existiert ein Element $a \in G : aUa^{-1} \subseteq P$.

Beweis. Sei zunächst $|P| = p^r$ erfüllt: (nach Folgerung $(3.2-7)$ ist dies möglich)
Betrachten:

$\Gamma := \{gP : g \in G\}$ (Linksnebenklasse) und $U \leq G$ mit $|U| = p^l \quad (l \leq r)$
Vermöge der Abbildung
$u \cdot gP = (ug)P \quad (u \in U, gP \in X)$ operiert U auf Γ.
Die Orbits sind $U \cdot gP = UgP$
Für ein Vertretersystem $\mathcal{V}$ der Orbits gilt:

$$\Gamma = \bigcup_{vP \in \Gamma} UvP$$

Wegen $|\Gamma| = [G : P] = \dfrac{|G|}{|P|} = \dfrac{p^r m}{p^r} = m \Rightarrow p \nmid |\Gamma|$
$\Rightarrow$ es existiert ein $U\tilde{v}P \quad (\tilde{v}P \in \mathcal{V}) : \quad p \nmid |U\tilde{v}P| = |U \cdot \tilde{v}P|$
Nach Satz $(3.1-8)$ gilt:$|U \cdot \tilde{v}P| \mid |U| \Rightarrow p^l = |U| = k \cdot |U \cdot \tilde{v}P| \Rightarrow |U \cdot \tilde{v}P| = 1$
$\overset{\text{Bem.}(3.1-10)}{\Rightarrow} \tilde{v}P \in Fix_U(\Gamma)$, d.h.

$u \cdot \tilde{v}P = \tilde{v}P$ für alle $u \in U,$ also
$(u\tilde{v})P = \tilde{v}P$ für alle $u \in U$
$\Rightarrow \tilde{v}u\tilde{v}P = P$ für alle $u \in U$
$\Rightarrow aUa^{-1} \subseteq P$ (wobei $a = \tilde{v}^{-1}$)

Sei nun P' eine beliebige p-Sylow-Gruppe von P. Da also insbsondere P' eine p-Gruppe ist, folgt aus Teil des Beweises (U durch P' ersetzen)

$$\text{Es existiert ein } b \text{ mit } bP'b^{-1} \subseteq P \quad (|P| = p^r)$$

Nach Lemma $(3.2-8)$ ist $bP'b^{-1}$ selbst eine p-Sylow-Gruppe.
$\overset{\text{Def.}(3.2-2)}{\Rightarrow} bP'b^{-1} = P \Rightarrow |P'| = |P| = p^r \Rightarrow$ Behauptung $\square$

Folgerung 3.2.10. *Je zwei p-Sylow-Gruppen der Gruppe G (mit $|G| = p^r m$) sind konjugiert zueinander, also damit isomorph zueinander, und die Anzahl der Elemente dieser Gruppen ist gleich p^r.*

Folgerung 3.2.11. *Eine p-Sylow-Gruppe P von G (mit $|G| = p^r m$) ist ein Normalteiler in $G \Leftrightarrow P$ ist die einzige p-Sylow-Gruppe von G.*

Beweis. "$\Rightarrow$" Sei P ein Normalteiler in G und (Annahme) P' eine p-Sylow-Gruppe von $G \overset{\text{Folg.}(3.2-10)}{\Rightarrow}$ es existiert ein $x \in G : P' = xPx^{-1} = P \Rightarrow P_1$ ist einzige p-Sylow-Gruppe in G.

"$\Leftarrow$" Sei P einzige p-Sylow-Gruppe von G. Nach Lemma $(3.2-8)$ ist gPg^{-1} für alle $g \in G$ eine p-Sylow-Gruppe in $G \Rightarrow P = gPg^{-1}$ für alle $g \in G \Rightarrow P$ ist ein Normalteiler. $\square$

Folgerung 3.2.12. *Zu jeder abel'schen Gruppe G ($|G| = p^r m$) gibt es genau eine p-Sylow-Gruppe.*

Satz 3.2.13 (3.Sylow'scher Satz). *Sei G eine endliche Gruppe, p eine Primzahl, $m \in \mathbb{N}$ mit dem $ggT(m,p) = 1$. Wenn $|G| = p^r m \quad (r \geq 1)$ so ist die Anzahl s_p der p-Sylow-Gruppen zu G Teiler von m und von der Form $1 + kp \quad (k \geq 0)$ und es gilt:*

1. *$s_p \mid m$ und*
2. *es existiert ein $k \geq 0 = s_p = 1 - kp$*

Zum Beweis benötigen wir Folgendes:

Lemma 3.2.14. *Sei $U \leq G$ und $N(U) = \{x \in G : xU = Ux\}$ Normalisator von U. Dann gilt: $N(U)$ ist die größte Untergruppe von G, in der U Normalteiler ist.*

Beweis. Übung □

Lemma 3.2.15. *Ist $P \leq G$ eine p-Sylow-Gruppe von G und $\overline{a} \in N(P)/P$ mit $ord(\overline{a}) = p^l$ $(l \geq 1)$, so ist $\overline{a} = \overline{e}$ ($\mathbf{1}$-Element von $N(P)/P$) d.h, $a \in P$.*

Beweis. Sei $ord(\overline{a}) = p^l \Rightarrow |\langle \overline{a} \rangle| = p^l$, d.h. $V := \langle \overline{a} \rangle$ ist eine p-Gruppe.
Sei $\pi : N(P) \to N(P)/P$ der harmonische Homomorphismus
$\Rightarrow U := \pi^{-1}(v) \leq N(P)$ und $P \subseteq U$
Weiterhin gilt:

$$V = U/P \qquad (\pi(U) = \pi(\pi^{-1}(V)) = V)$$

Wegen $|U| = |U/P| \cdot |P| = p^k \Rightarrow U$ ist eine p-Gruppe $\Rightarrow P = U$
$\Rightarrow V = P/P = \{e\} = \langle \overline{a} \rangle \Rightarrow \overline{a} = \overline{e} \Rightarrow a \in P$ □

Lemma 3.2.16. *Sei $P \leq G$ eine p-Sylow-Gruppe von G und $a \in G$ mit $ord(a) = p^l \quad (l \geq 1)$. Wenn $aPa^{-1} = P$, so ist $a \in P$.*

Beweis. Wegen $aP = Pa$ ist $a \in N(P) \Rightarrow \pi(a) = \overline{a} \in N(P)/P$ mit $(\overline{a})^{p^l} = (\overline{a^{p^l}}) = \overline{e} = ord(\overline{a}) = p^l$
$\Rightarrow a \in P$ □

Beweis zu Satz $(3.2 - 13)$. Sei $\Gamma = \{P, P_1, \ldots, P_{r-1}\}$ die Menge der verschiedenen p-Sylow-Gruppen zu G. ($|P| = p^r$). Nach Folgerung $(3.2 - 10)$ ist $\Gamma = \{gPg^{-1} : g \in G\}$. Nach Satz $(3.1 - 15) \Rightarrow |\Gamma| = [G : N(P)] = \frac{|G|}{|N(P)|}$ und es folgt

$$|G| = |\Gamma||N(P)|$$

$\Rightarrow p^r m = |G| = |\Gamma||P|[N(P) : P] = |\Gamma| \cdot p^r \cdot k \Rightarrow m = |\Gamma| \cdot k$
$s_p = |\Gamma|$ teilt m. Vermöge der Abbildung $h \cdot X = hXh^{-1} \quad (h \in P, X \in \Gamma)$ operiert P auf X (als Übung). Wenn $\mathcal{V} \subseteq \Gamma$ ein Vertretersystem der Orbits ist, so folgt aus Satz $(3.1 - 10)$

$$|\Gamma| = \sum_{x \in \mathcal{V}} [P : P_x]$$

wobei $P_x = \{g \in P : g \cdot X = X\}$ der Stabilisator zu X ist.
konkret:$P_x = \{g \in P : gXg^{-1} = X\}$. Für $X = P \Rightarrow P_p = \{g \in P : gPg^{-1} = P\} \Rightarrow P_p = P$
Ist nun $[P : P_x] = 1 \Rightarrow X$ ist ein Fixpunkt, d.h. $g \cdot X = X$ für alle $g \in P. \Rightarrow gXg^{-1} = X$ für alle $g \in P$. Nun ist $ord(g) = p^{lg}$ (da $g \in P$) und X eine p-Sylow-Gruppe mit $gXg^{-1} \Rightarrow P \subseteq X \Rightarrow P = X$
Nun gilt für $X = P$: $\quad [P : P_x] = 1, \quad |\Gamma| = 1 \sum_{x \in \mathcal{V}} [P : P_x]$
Da $[P : P_x] \mid |P| \Rightarrow$ es existiert ein $i_x \in \mathbb{N} : [P : P_x] = p^{i_x} \quad (i_x \geq 1, x \neq p)$
$\Rightarrow |\Gamma| = 1 + p \sum_{x \in \mathcal{V}} p^{i_x - 1} \qquad s_p = |\Gamma| = 1 + p \cdot k \quad (k \geq 0)$ □

Folgerung 3.2.17. *Sei $|G| = p^r m \quad (r \geq 1, p$ prim$)$. Wenn $m < p$, so besitzt G genau eine p-Sylow-Gruppe, die Normalteiler in G ist. (d.h. G ist nicht einfach)*

Beweis. Zeigen: $s_p = 1$
Annahme: $s_p > 1 \Rightarrow s_p = 1 + kp$ mit $k \geq 1 \Rightarrow s_p \geq 1 + p > m$
Nun gilt aber: $s_p \mid m \Rightarrow$ Widerspruch
$\Rightarrow$ Behauptung □

Folgerung 3.2.18. *Seien p, q Primzahlen mit $q < p, p \neq 3$ und G eine Gruppe mit $|G| = p^r q \quad (r \geq 1)$.*
Dann besitzt G genau eine p-Sylow-Gruppe.

Beweis. zeigen: $s_p = 1$
Da $s_p \mid q^2 (= m) \Rightarrow s_p = 1$ oder $s_p = q$ oder $s_p = q^2$.
Sei $s_p = q \Rightarrow q = 1 + kp \quad (k \geq 1) \Rightarrow q \geq 1 + p > p$
$\Rightarrow$ Widerspruch
Sei $s_p = q^2 \Rightarrow q^2 = 1 + kp \quad (k \geq 1) \Rightarrow kp = q^2 - 1 = (q+1)(q-1) \Rightarrow p \mid (q+1)$ oder $p \mid (q-1)$.

$$\left.\begin{array}{l} \text{Da } q - 1 < q < p \Rightarrow p \mid (q+1) \\ \text{Da } p \neq 3 \Rightarrow p \geq q \end{array}\right\} \text{ Widerspruch } \Rightarrow s_p = 1$$

□

Folgerung 3.2.19. *Seien p, q prim mit $q < p$ und sei G eine Gruppe mit $|G| = pq$, dann gilt:*

1. *Es gibt genau eine p-Sylow-Gruppe*
2. *Ist $p \in \{1 + kp : k \geq 1\}$, so ist G zyklisch*

Beweis.

1. folgt aus Folgerung $(3.2-17)$ für $r=1, \quad m=q$

2. s_q ist die Anzahl der q-Sylow-Gruppen
   Da $s_q \mid p \Rightarrow s_q = 1$ oder $s_q = p$
   Wenn $p = s_q \Rightarrow p = 1 + kq \quad (q \geq 1)$ Widerspruch
   $\Rightarrow s_q = 1$

   $\Rightarrow$ Es existiert genau eine Untergruppe U_p mit $|U_p| = p$ und
   es existiert genau eine Untergruppe U_q mit $|U_q| = q$
   $\Rightarrow$ sind die einzigen p- bzw. q-Sylow-Gruppen zu G.
   $\Rightarrow U_p, U_q$ sind Normalteiler und außerdem sind diese zyklisch.
   Man kann zeigen:
   $$G \cong \mathbb{Z}_p \times \mathbb{Z}_q \cong \mathbb{Z}_{pq} \Rightarrow \text{ Behauptung}$$

□

Satz 3.2.20. *Jede Gruppe G mit $|G| = p^r \quad (r \geq 1, \quad p$ prim$)$ hat einen Normalteiler N mit $|N| = p^{r-1}$*

Beweis. Wir beweisen diesen Satz per vollständiger Induktion.

Ind.-Ann.: $r = 1; |G| = p \Rightarrow G$ ist zyklisch $\Rightarrow N = \{e\}$ Normalteiler zu G mit $p^0 = 1$

Ind.-Vor.: Behauptung gilt für jede Gruppe mit p^{r-1} Elementen

Ind.-Bew.: Sei $r > 1$. Nach Satz $(3.1-17)$ ist $|Z(G)| > 1$
Da $Z(G) \leq G \Rightarrow |Z(G)| = p^r \Rightarrow |Z(G)| = p^l \quad (l \geq 1)$

Nach Satz $(3.2-2)$ existiert $N \leq Z(G)$ mit$|N| = p$
Da $Z(G)$ Normalteiler zu G ist und $N \leq Z(G) \Rightarrow N \trianglelefteq G$
$\Rightarrow |G/N| = \dfrac{|G|}{|N|} = \dfrac{p^r}{p} = p^{r-1}$
Nach der Ind.-Vor. (angewandt auf G/N) besitzt G/N einen Normalteiler $\overline{U}$ mit $\overline{U} = p^{r-2}$
Sei $\pi : G \to G/N$ der kanon. Homomorphismus $\Rightarrow U = \pi^{-1}(\overline{U}) \geq N$
Nach Satz $(2.5-9)$ ist $U \trianglelefteq G$ und $\overline{U} = U/N$

□

Folgerung 3.2.21. *Sei G wie in Satz $(3.2-20)$. Dann gibt es eine steigende Folge $\{U_i\}_{i=0}^{r}$ mit $|U_i| = p^i \quad (i = 0, \ldots, r)$, wobei zusätzlich gilt:*

$$U_i \triangleleft U_{i\neq 1} \quad (i = 0, \ldots r-1)$$

Beweis. Siehe Blatt □

Bemerkung 3.2.22. *1. Mit ähnlichen Methoden zeigt man:*
Ist G einfach, mit $60 < |G| < 168$, so ist $|G|$ eine Primzahl, d.h. $|G|$ ist zyklisch.

2. $A_5 \subset S_5$ einfach mit $|A_5| = 60$. Es gibt einfache Gruppen mit 168 Elementen.

3. $30 = 2 \cdot 3 \cdot 5$

$$\begin{aligned} & s_5 \mid 10 \text{ und } s_3 = 1 + 3k \quad (k \geq 0) \\ \Rightarrow & s_5 \in \{1, 2, 5, 10\} \Rightarrow s_3 \in \{1, 10\} \\ Ann. : & s_5 = 6, s_3 = 10 \text{ Seien } U, V \text{ verschiedene p-Sylow-Gruppen} \\ \Rightarrow & |U| = |V| = 5 \Rightarrow U, V \text{ zyklisch } \Rightarrow U \cap V = \{1\} \\ \Rightarrow & \text{Es existieren Elemente der Ordnung } 5. \\ & s_3 = 10 \text{ liefert 20 Elemente der Ordnung } 3. \end{aligned}$$

Satz:
Sei G eine Gruppe mit $|G| < 60$. Ist $|G|$ keine Primzahl, so besitzt G echte Normalteiler, d.h. G ist nicht einfach.

Zum Beweis für zusammengesetzte Ordnungen $|G|$ die folgende Tabelle:

$1 < \|G\| \leq 20$	Folg
$04 = 2^2$	E
$06 = 2 \cdot 3$	19,17
$08 = 2^3$	E
$09 = 3^2$	E
$10 = 2 \cdot 5$	19,17
$12 = 2^2 \cdot 3$	a
$14 = 2 \cdot 7$	19,17
$15 = 3 \cdot 5$	19,17
$16 = 2^4$	E
$18 = 3^2 \cdot 2$	17
$20 = 2^2 \cdot 5$	18

$20 < \|G\| \leq 40$	Folg
$21 = 3 \cdot 7$	19,17
$22 = 2 \cdot 11$	19,17
$24 = 2^3 \cdot 3$	b
$25 = 5^2$	E
$26 = 2 \cdot 13$	19,17
$27 = 3^3$	E
$28 = 2^2 \cdot 7$	18
$30 = 2 \cdot 3 \cdot 5$	c
$32 = 2^5$	E
$33 = 3 \cdot 11$	19,17
$34 = 2 \cdot 17$	19,17
$35 = 5 \cdot 7$	19,17
$36 = 2^2 \cdot 3^2$	d
$38 = 2 \cdot 19$	19,17
$39 = 3 \cdot 13$	19,17
$40 = 2^3 \cdot 5$	e

$40 < \|G\| < 60$	Folg
$42 = 2^3 \cdot 5$	17
$44 = 2^2 \cdot 11$	17,18
$45 = 3^2 \cdot 5$	18
$46 = 2 \cdot 23$	17,19
$48 = 2^4 \cdot 3$	f
$49 = 7^2$	E
$50 = 2 \cdot 5^2$	17
$51 = 3 \cdot 17$	17
$52 = 2^2 \cdot 13$	18
$54 = 2 \cdot 3^3$	17
$55 = 5 \cdot 11$	17,19
$56 = 2^3 \cdot 7$	g
$57 = 3 \cdot 19$	17,19
$58 = 2 \cdot 29$	17,19

Fall a $12 = 2^2 \cdot 3 \Longrightarrow G$ besitzt 2 - Sylow - Gruppen, 3 - Sylow - Gruppen $\Longrightarrow 12 = 2^2 \cdot m_2 \Longrightarrow s_2 \mid 3$ und $s_2 \in \{1 + k \cdot 2\}_{k \geq 0} \Longrightarrow s_2 \in \{1, 3\}$ Analog : $s_3 \in \{1, 4\}$. Wenn $s_3 = 1 \Longrightarrow$ Behauptung. Sei $s_3 = 4$. Seien $H_{1/4}$ die 3 - Sylow - Gruppen $\Longrightarrow |H_i| = 3 \Longrightarrow H_i$ zyklisch. $\Longrightarrow H_i \cap H_j = \{e\} \ \ (i \neq j) \Longrightarrow |\bigcup_{i=1}^{4} H_i| = 9$

Annahme: $s_2 = 3$ und $P_{1/2/3}$ die 2- Sylow - Gruppen $\Longrightarrow |P_j| = 4$. Wäre $P_j \cap H_i =< e > \quad \forall \ i, j \Longrightarrow$ In P_j existieren drei Elemente $\neq e$, die nicht in $\bigcup H_i$ liegen . Da $P_j \neq P_i$ existieren mindestens 4 Elemente $\neq e$, die nicht in $\bigcup H_i$ liegen. Widerspruch $9 + 4 = 13 > 12 \Longrightarrow \exists \ i, j, \ x \neq e \mid x \in P_i \cap H_i \Longrightarrow ord \ (x) = 3$, da $x \in H_i$ Widerspruch zu $3 \nmid 4 = |P_j|$.

Fälle b, d und f ergeben sich aus Lemma 3.1-4 : $|G| = 24 = 2^3 \cdot 3 : G$ besitzt eine 2 - Sylow - Gruppe H mit $|H| = 2^3 \Longrightarrow |G : H| = 3$. Nun ist $24 \nmid 3! = 6 \Longrightarrow$ Behauptung. $36 = 2^2 \cdot 3^3 \Longrightarrow \exists$ 3 - Sylow - Gruppe H mit $|H| = 3^2 \Longrightarrow |G : H| = 4$ und $36 \nmid 4$! $48 = 2^4 \cdot 3 \Longrightarrow \exists$ 2 - Sylow - Gruppe H mit $|H| = 2^4 \Longrightarrow |G : H| = 3$ und $48 \nmid 3$!

Fall c $30 = 2 \cdot 3 \cdot 5$, s_3 teilt 10 und $s_3 = 1 + 3k \ \ (k \geq 0)$, $s_3 \in \{1, 2, 5, 10\} \Longrightarrow s_3 \in \{1, 10\}$, s_5 teilt 6 und $s_5 = \{1 + 5k\} \ \ (k \geq 0)$, $s_5 \in \{1, 2, 3, 6\} \Longrightarrow s_5 \in \{1, 6\}$. Annahme : $s_3 = 10, \ s_5 = 6$ Seien U, V zwei verschiedene 5 - Sylow - Gruppen. $\Longrightarrow U \cap V = \{1\} \Longrightarrow s_5 = 6 \Longrightarrow 24$ verschiedene Elemente der Ord. 5, enstprechend $s_3 = 10$ liefert 20 verschiedene Elemente der Ord. 3. Widerspruch zu $|G| = 30. \Longrightarrow s_3 = 1$ oder $s_5 = 1 \Longrightarrow$ Behauptung.

Fall e $40 = 2^3 \cdot 5$, s_5 teilt 8 und $s_5 = 1 + 5k \ \ (k \geq 0) \Longrightarrow s_5 \in \{1, 2, 4, 8\}$. $s_5 = 1$, 5 - Sylow - Gruppe ist normal. $\Longrightarrow$ Behauptung.

Fall g $56 = 2^3 \cdot 7$, s_7 teilt 8 und $s_7 = \{1 + 7k\}$ $(k \geq 0)$. Annahme : $s_7 = 8$ wie in (c) liefert die $8 \cdot 7 + 1$ verschiedene Elemente. Sei U eine 2 - Sylow - Gruppe $\Longrightarrow |U| = 8$ Sei H eine 7 - Sylow - Gruppe $\Longrightarrow H \cap U = \{1\}$. $\Longrightarrow s_2 = 1 \Longrightarrow$ Behauptung

Fall E In diesem Fall ist $|G| = p^r \quad r \geq 2$ also Primzahlpotenz. Falls G abelsch ist, so existiert nach dem 1. Sylowschen Satz ein $U \leq G$ mit $|U| = p$, ist G nicht abelsch, so folgt, daß $Z(G)$ Normalteiler ist. (Beachte: $Z(G) \neq \langle e \rangle$ Satz 3.1-17)

Kapitel 4

Konstruktion mit Zirkel und Lineal

4.1 Definitionen

Definition 4.1.1. *Sei $R \neq \emptyset$ eine beliebige Menge und "$+$" sowie "$\cdot$" zwei Operationen auf R. $(R, +, \cdot)$ heißt Ring, wenn gilt:*

1. *$(R, +)$ ist eine abel'sche Gruppe ($\mathbf{1}$-Element sei 0)*
2. *$(R, \cdot)$ ist eine Halbgruppe mit $\mathbf{1}$-Element*
3. $$\left.\begin{array}{l} a \cdot (b + c) = a \cdot b + a \cdot c \\ (a + b) \cdot c = a \cdot c + b \cdot c \end{array}\right\} \textit{Distributivgesetze}$$

Definition 4.1.2. *Ein Ring $(R, +, \cdot)$ heißt kommutativ, wenn gilt:*

$$a \cdot b = b \cdot a \qquad \textit{für alle } a, b \in R$$

Beispiel 4.1.3. 1. *$(\mathbb{Z}, +, \cdot)$ ist der Ring der ganzen Zahlen*
2. *$M_n(\mathbb{Z}) = M(n \times n, \mathbb{Z}) = \mathbb{Z}^{n \times n}$ ist der Ring der $n \times n$-Matrizen $A = (a_{ik})_{i,k=1}^{n}$, wobei $a_{ik} \in \mathbb{Z}$*

Definition 4.1.4. *Ein Ring heißt Schiefkörper, wenn $\mathbf{1} \neq 0$, d.h., $|R| \geq 2$ und alle Elemente $x \neq 0$ in $(R, \cdot)$ invertierbar sind.*
Ein kommutativer Schiefkörper heißt ein Körper.
($(1), (2)$ aus Beispiel $(4.1 - 3)$ sind keine Körper !)

Beispiel 4.1.5. 1. *$\mathbb{Q}, \mathbb{R}, \mathbb{C}$ sind Körper*

2. $\mathbb{F}_2 = \{0, 1\}$

   $\mathbb{F}_2 = (\mathbb{Z}_2, +, \cdot)$ *ist ein Körper*

3. *Quaternionen:*

$$1, i, j, k \qquad i^2 = j^2 = k^2 = 1$$
$$x = \xi_0 + \xi_1 \cdot i + \xi_2 \cdot j + \xi_3 \cdot k$$

   Sei $z, w \in \mathbb{C}, \quad M(z,w) = \begin{pmatrix} z & w \\ \overline{z} & \overline{w} \end{pmatrix}$
   $|H| = \{M(z,w) : z, w \in \mathbb{C}\}$ *ist die Menge der Quaternionen.*

   Operation: Matrixmultiplikation und -addition

   Einselement: $I = M(1,0)$ $M(z,w)$ *ist invertierbar in* $M_2(\mathbb{C})$
   $\Leftrightarrow det(M(z,w)) \neq 0$
   $\Leftrightarrow z\overline{z} + w\overline{w} \neq 0$ *(d.h.* $|z^2| + |w^2| \neq 0$*)*
   $\Leftrightarrow M(z,w) \neq 0$

   Für die Inverse gilt:

$$M(z,w)^{-1} = M(\alpha\overline{z} - \alpha w) \text{ mit } \alpha = \frac{1}{|z^2| + |w^2|}$$

   $M(z,w)$ *ist nicht kommutativ, denn*

$$\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}$$

   $\Rightarrow$ *echter Schiefkörper*

4.2 Der Körper der konstruierbaren Zahlen

Definition 4.2.1. *Sei* $(K, +, \cdot)$ *ein Körper. Die Teilmenge* $\emptyset \neq k \subseteq K$ *heißt Teilkörper zu* K*, wenn* $(k, +, \cdot)$ *selbst ein Körper ist.*

Satz 4.2.2. *Sei* k *ein Körper und* $k \subseteq K$ *mit* $|k| \geq 2$*, dann sind folgende Aussagen äquivalent:*

1. k *ist ein Teilkörper von* K

2. *Aus* $a, b \in k$ *folgt:* $a + b \in k, a \cdot b \in k, (-a) \in k, a^{-1} \in k$ *für* $a \neq 0$

Beweis Übung. □

Bemerkung 4.2.3. *Ist* k *ein Teilkörper von* K*, so ist* $\mathbf{1}$*-Element von* K *auch das* $\mathbf{1}$*-Element von* k*.*

Beweis. Sei $a \in k$ mit $a \neq 0 \Rightarrow a^{-1} \in k \Rightarrow a \cdot a^{-1} = \mathbf{1} \in k$. □

Definition 4.2.4. *Der Teilkörper* k *des Körpers* K *heißt abgeschlossen unter Quadratwurzeln, wenn aus* $a \in K$ *und* $a^2 \in k$ *stets* $a \in k$ *folgt.*

Der Rest dieses Kapitels ist auf der Kopie mit den "Klassischen Problemen der griechischen Mathematik" sehr schön dargestellt.

4.3 Der Polynomring in einer Unbestimmten

Sei R ein kommutativer Ring mit $\mathbf{1}$-Element $\neq 0$

Definition 4.3.1. *Die Folge* $(a_i)_{i \geq 0}^{\infty}$ *von Elementen* $a_i \in R \quad (i \geq 0)$ *heißt finit (oder finite Folge), wenn ein Index* i_0 *existiert, mit* $a_i = 0$ *für alle* $i \geq i_0$*.*
Mit $R[X]$ *bezeichnen wir die Menge aller finiten Folgen aus* R*.*
Wir finden die Operationen "$+$*" und "*$\cdot$*", so dass* $R[X]$ *ein Ring wird.*
Seien $(a_i), (b_j) \in R[X]$*.*
Setzen:

$$(a_i) + (b_j) := (a_i + b_j) \text{ (Addition)}$$
$$(a_i) \cdot (b_j) := (c_k), \text{ wobei } c_k = \sum_{i+j=k} a_i b_j \text{ (Multiplikation)}$$

Satz 4.3.2. *Mit dieser Verknüpfung "*$+$*", "*$\cdot$*" wird* $R[X]$ *zu einem kommutativen Ring mit* $\mathbf{1}$*-Element.*

Beweis Übung. □

Bedeutung von X in $R[X]$:

Setzen: $X = (0, 1, 0, 0, \ldots)$
$$X^2 = X \cdot X = (0, 0, 1, 0, 0, \ldots)$$
$$X^n = (\delta_{in})_i \geq 0 \qquad \left(\delta_{in} = \begin{cases} 1 & ; \quad i = n \\ 0 & ; \quad i \neq n \end{cases} \right)$$
Setzen: $X^0 := (1, 0, 0, \ldots)$

Wir identifizieren:
$a_0 \in R$ mit $(a_0, 0, 0, \ldots)$
$\Rightarrow$ Für $a \in R \Rightarrow aX^i = (0, 0, \ldots, \overset{i-te}{a}, 0, 0 \ldots)$
$\Rightarrow (a_0, a_1, \ldots, a_n, 0, 0, \ldots) = \sum_{i=0}^{n}(a_i X^i)$
Damit ist also $R[X]$ der Ring des Polynoms $\sum_{i\geq 0} a_i X^i$ in der Unbestimmten X.

$$\sum a_i X^i + \sum b_i X^i = \sum (a_i + b_i) X^i$$
$$\sum_{i\geq 0} a_i X^i \cdot \sum_{j\geq 0} b_j X^j = \sum_{i,j\geq 0} a_i b_j X^{i+j}$$

Definition 4.3.3. *Sei* $f = \sum_{i\geq 0} a_i X^i \in R[X]$ *mit* $a_n \neq 0 \quad (n \geq 0)$ *sowie* $a_{n+j} = 0$ *für alle* $j \geq 1$

$$a_n - \textit{ höchster Koeffizient in } f$$
$$n = deg(f) - \textit{Grad von } f$$
$$f \textit{ heißt normiert, wenn } a_n = 1$$

Die Polynome vom Grade 0 *sind alle Elemente aus* $R/\{0\}$. *Das Nullpolynom hat keinen Grad*

Bemerkung 4.3.4. *Sei* $f = \sum_{i=0}^{n} a_i X^i \in R[X]$ *fix.*
Wir setzen:

$$\varphi_f : R \to R \textit{ mit } \varphi_f(r) = \sum_{i=0}^{n} a_i r^i = f(r)$$

Achtung: Das Polynom f *und die Funktion* φ_f *sind wesentlich verschiedene Objekte.*

Beispiel:

$R = \mathbb{F}_2 := \{0, 1\}$
Da $\{0, 1\} = R$ *endlich ist, existieren auch nur endlich viele Funktionen von* $R \to R$,
Aber: In $\mathbb{F}_2[X]$ *liegen unendlich viele Polynome.*
konkret: $f = X^2 - X \Rightarrow \varphi_f(r) = 0 \Rightarrow \varphi_f = 0$
$f = X^3 - X \Rightarrow \varphi_f(r) = 0 \Rightarrow \varphi_f = 0$

Definition 4.3.5. *Ein kommutativer, nullfreier Ring mit* $\mathbf{1}$*-Element* $\neq 0$ *heißt Integritätsbereich.*
(nullteilerfrei: Aus $xy = 0 \Rightarrow x = 0$ *oder* $y = 0$*)*

Satz 4.3.6. *Es gilt:*

$$R[X] \textit{ Integritätsbereich} \Rightarrow R \textit{ Integritätsbereich}$$

Beweis Übung. □

Folgerung 4.3.7. *Seien $f, g \in R[X]/\{0\}$, dann gilt:*

1. *Entweder $f \cdot g = 0$ oder $deg(f \cdot g) \leq deg(f) + deg(g)$*
2. *Wenn R Integritätsbereich ist, so gilt:*
$$deg(f \cdot g) = deg(f) + deg(g)$$
3. $$deg(f + g) \leq max(deg(f), deg(g))$$

Satz 4.3.8. *Sei R der Integritätsbereich und $f = \sum_{i \geq 0} a_i X^i \in R[X]$, dann gilt:*

$$f \text{ in } R \text{ invertierbar } \Leftrightarrow f = a_0, \quad a_0 \text{ invertierbar}$$

(d.h. $R^* = (R[X])^*$)

Beweis. 1. Sei f invertierbar, d.h. $g \in R[X]$ mit $f \cdot g = \mathbf{1}$

$$\begin{aligned} \overset{\text{Folg. } (4.3-1)}{\Rightarrow} \; & 0 = deg(\mathbf{1}) = deg(f \cdot g) = deg(f) + deg(g) \\ & \Rightarrow deg(f) = 0 = deg(g) \Rightarrow f = a_0, g = b_0 \\ & \mathbf{1} = a_0 b_0 \Rightarrow a_0 \text{ ist invertierbar in } R \end{aligned}$$

2. Die Umkehrung ist trivial

□

Satz 4.3.9 (Division mit Rest). *Sei R ein kommutativer Ring mit $\mathbf{1} \neq 0$ und $f = \sum_{i=0}^{n} a_i X^i$, $g = \sum_{j=0}^{m} b_j X^j \in R[X]/\{0\}$ mit $n = deg(f)$ und $m = deg(g)$.*
Wenn a_n in R invertierbar ist, so existieren eindeutig bestimmte Polynome $q, r \in R[X]$ mit $g = q \cdot f + r$, wobei $r = 0$ oder $deg(r) < deg(f)$.

Beweis. (Eindeutigkeit)
Sei $q' \cdot f + r', r' = 0$ oder $deg(r') < deg(f)$

$$\Rightarrow qf + r = q'f + r' \Rightarrow (q' - q)f = r - r'$$

Wäre $q = q' \Rightarrow r = r' \Rightarrow$ Behauptung
Sei also $q \neq q'$
Annahme: $r \neq r' \Rightarrow (q' - q)f \neq 0$
Da a_n invertierbar ist $\Rightarrow deg(r - r') = deg(q' - q) + deg(f)$
Hieraus folgt mit Folgerung $(4.3 - 7)$:

$$deg(f) \leq deg(r - r') \leq max(deg(r), deg(r')) < deg(f)$$

Dies ist ein Widerspruch
$\Rightarrow r = r'$
$\Rightarrow (q' - q)f = 0$ Da a_n invertierbar ist, so ist f kein Nullteiler (hier nicht bewiesen)
$\Rightarrow q = q' \Rightarrow$ Eindeutigkeit

Existenz von q, r: Induktion nach $m = deg(g)$
Sei $deg(g) = 0$, d.h $g = b_0$.
Ist $f = a_0 \quad (a_0 \in \mathbb{R})$ Voraussetzung $\Rightarrow a_0$ ist invertierbar
Setzen:
$q = a_0^{-1} b_0, \quad r = 0$
$\Rightarrow b_0 = a_0^{-1} b_0 a_0 + r$

Ist $deg(f) > deg(g)$, setzen $q = 0$, $r = g$
Sei nun $deg(g) \geq deg(f) \geq 1$

Setzen:

$$\begin{aligned} g_1 &= g - a_n^{-1} b_m X^{m-n} \cdot f = b_m X^m + \ldots + b_0 - a_n^{-1} b_m X^{m-n} \cdot q_n X^n - \ldots \\ &= b_m X^m - b_m X^n + \ldots \Rightarrow g_1 = 0 \text{ oder } deg(g_1) < m - deg(g) \end{aligned}$$

Nach der Induktionsvoraussetzung (für $(m-1)$ gilt die Aussage)$\Rightarrow$ Es existieren $q_1, r_1 \in R[X]$ mit $g_1 = q_1 \cdot f + r_1$, wobei $r_1 = 0$ oder $deg(r_1) < deg(f)$

$$\Rightarrow g = (q_1 + a_n^{-1} b_m X^{m-n}) f + r_1$$

(denn $q_1 f + a_n^{-1} b_m X^{m-n} f + r_1 = q_1 + a_n^{-1} b_m X^{m-n} f = g$)
$\Rightarrow$ Behauptung □

Folgerung 4.3.10. *Sei R ein kommutativer Ring mit $\mathbf{1} \neq 0$ und $a \in R$. Dann sind folgende Aussagen äquivalent:*

1. *a ist Nullstelle von f, d.h. $f(a) = 0$*
2. *Es existiert ein $q \in R[X] : f = (X - a)q$*

Beweis.

$2 \Rightarrow 1$: $f(a) = (a - a)q(a) = 0$

$1 \Rightarrow 2$: Aus dem Satz "Division mit Rest" folgt:
Es existieren $q, r \in R[X]$ mit $f = (X - a)q + r$, wobei $r = 0$ oder
$deg(r) < deg(X - a) = 1$

Ann.: Sei $r \neq 0 \Rightarrow deg(r) = 0 \Rightarrow r = r_0 \in R \Rightarrow 0 = f(a)$

□

Folgerung 4.3.11. *Sei $f \in R[X]/\{0\}$ mit $n = deg(f)$, dann gilt:*
f hat in R höchstens n Nullstellen.

Definition 4.3.12. *Sei R der Integritätsbereich und $a, b \in R$. a heißt Teiler von b ($a \mid b$), wenn gilt:*

$$\text{Es existiert ein } c \in R : b = a \cdot c$$

Satz 4.3.13 (Rechenregeln für Teiler). *Es gilt:*

1. $\mathbf{1} \mid a, a \mid 0, a \mid a$ *für alle* $a \in R$
2. $a \mid \mathbf{1} \Leftrightarrow a$ *ist invertierbar* ($a \in R^*$), (a *heißt Einheit*)
3. $a \mid b_i \quad (i = 1, 2) \Rightarrow a \mid r_1 a_1 + r_2 a_2$ *für alle* $r_i \in R \quad (i = 1, 2)$
4. $a \mid b$ *und* $b \mid c \Rightarrow a \mid c$
5. $a \mid b$ *und* $b \mid a \Leftrightarrow$ *es existiert ein* $u \in R : a = bu$

Beweis Übung. □

Definition 4.3.14.

1. *Die Elemente $a, b \in R$ heißen assoziiert, wenn ein $u \in R^*$ existiert mit $a = bu$.*
2. *Der Teiler $t \in R$ von $a \in R$ heißt echter Teiler von a, wenn t nicht invertierbar und t nicht assoziiert zu a ist.*
3. *Sei $q \in R/(R^* \cup \{0\})$. q heißt irreduzibel oder unzerlegbar, wenn aus $q = a \cdot b \quad (a, b \in R)$ stets folgt: a oder b ist invertierbar.*

Beispiel 4.3.15.

1. $f = X - a \in \mathbb{Z}[X]$ *ist irreduzibel*
2. $f = X^2 + 1 \in R[X]$ *ist irreduzibel, aber* $f \in \mathbb{C}[X]$ *ist zerlegbar, da* $X^2 + 1 = (X - i)(X + i)$

Definition 4.3.16.
1. *Das Element $t \in R$ heißt gemeinsamer Teiler der Elemente $a, b \in R$, wenn gilt: $t \mid a$ und $t \mid b$.*
2. *$a \neq b$ sind teilerfremd, wenn jeder gemeinsame Teiler von a und b eine Einheit ist.*

3. *Das Element $d \in R$ heißt größter gemeinsamer Teiler (ggT) der Elemente $a, b \in R$, wenn d gemeinsamer Teiler von a und b ist und wenn jeder gemeinsame Teiler dieser 2 Elemente auch Teiler von d ist.*

Folgerung 4.3.17.

1. *Sind $d, d' \in R$ zwei ggT von $a, b \in R$, so ist d assoziiert zu d' ($d = ud', u \in R^*$)*
2. *$a \neq b$ teilerfremd $\Leftrightarrow ggT = 1$*

Aufgaben 4.3.18. *Sei $a = bq + r$ und d ggT von a, b. Man zeige:*
d ist ggT von b, r und umgekehrt

Satz 4.3.19 (Existenz und Darstellung eines ggT). *Sei K ein Körper und $f, g \in K[X]/\{0\}$. Dann besitzen f und g einen ggT $h \in K[X]/\{0\}$ und es existieren Polynome $p, q \in K[X]$ mit*

$$h = pf + qg$$

Beweis. O.B.d.A sei $deg(f) \leq deg(g)$ (Ind. nach $deg(f)$)

IA : Sei $deg(f) = 0$, d.h. $f = a_0 + 0 \quad (a_0 \in K)$
$\Rightarrow$ es existiert $a_0^{-1} \in K \Rightarrow$ es existiert ein Polynom $f^{-1} \in K[X] \Rightarrow \mathbf{1} = ggT(f, g)$ mit $\mathbf{1} = a_0^{-1} f + 0g$

IV : Sei $deg(f) = n + 1 > 0$ und es gelte die Behauptung für Polynome $\overline{f}$ mit $deg(\overline{f}) \leq n$

IB : Aus dem Satz über die "Division mit Rest" folgt die Existenz der Elemente $q, r \in K[X]$ mit $g = fq + r \quad (*)$, wobei $r = 0$ oder $deg(r) < deg(f) = n + 1$.

- Wenn $r = 0 \Rightarrow f = ggT(f, g)$ und $f = f \cdot 1 + g \cdot 0$
- $r \neq 0 \Leftrightarrow deg(r) \leq n$, können IV auf r, g anwenden, d.h. r, g besitzen den ggT h und es exisistieren $p_1, q_1 \in K[X]$ mit

$$h = p_1 r + q_1 g \overset{(*)}{\Rightarrow} \begin{array}{rcl} h & = & p_1(g - fq) + q_1 g \\ & = & pf(-p_1 q) + (q_1 + q_1)g \end{array}$$

Wegen Aufgabe $(4.3 - 18)$ ist dieses h auch $ggT(f, g)$.

□

Definition 4.3.20. *Sei $f \in R[X]$ normiert und $deg(f) \geq 1$. Das Polynom f heißt reduzibel (zerlegbar), wenn Polynome $g, h \in R[X]$ existieren mit $f = g \cdot h$ und $deg(g), deg(h) < deg(f)$. (sonst heißt f irreduzibel).*

Ist $f \in K[X]$ irreduzibel, so setzen wir voraus, dass f normiert ist.

Folgerung 4.3.21. *Seien $f_{1/2} \in K[X]$ mit $f_1 \neq f_2$*

1. *Wenn f_1, f_2 irreduzibel, so sind sie teilerfremd*
2. *Wenn $f \in K[X]$ irreduzibel, so folgt aus $f \mid g \cdot h \quad (g, h \in K[X])$ stets $f \mid g$ oder $f \mid h$.*

Beweis zu 2). Sei f irreduzibel, $f \mid g \cdot h$ und $f \nmid g$

$$\Rightarrow 1 \quad ggT(f,g) \overset{\text{Satz}(4.3-19)}{\Rightarrow} \text{ es existieren } p, q \in K[X] \text{ mit } 1 = pf + qg$$
$$\Rightarrow h = pfh + qgh \Rightarrow f \mid h$$

□

Bemerkung 4.3.22. *2) ist die Eigenschaft eines Primelementes*

Satz 4.3.23 (Satz über die Primfaktorzerlegung). *Jedes nicht-konstante Polynom $f \in K[X]$ lässt sich als Produkt*

$$f = \varepsilon p_1 p_2 \cdots p_m$$

mit $\varepsilon \in K[X]/\{0\}$ und irreduzibelen Polynomen $p_1, \ldots, p_m$ schreiben.
Dabei sind die Polynome $p_1, \ldots, p_m$ bis auf ihre Reihenfolge eindeutig bestimmt.

Lemma 4.3.24 (Gauß). *Wenn $f \in \mathbb{Z}[X]$ in $\mathbb{Z}[X]$ irreduzibel ist, so ist f auch in $\mathbb{Q}[X]$ irreduzibel.*

Beweis. Sei $f \in \mathbb{Z}[X]$ irreduzibel.

Ann.: Sei f in $\mathbb{Q}[X]$ reduzibel.
$\Rightarrow$ Es existiert ein $g = \sum_{i=0}^{r} \alpha_i X^i \in \mathbb{Q}[X], \quad h = \sum_{j=0}^{s} \beta_j X^j \in \mathbb{Q}[X]$ mit
$f = g \cdot h$, sei $\alpha > 0$ der Hauptnenner aller $\alpha_i, \beta_j \Rightarrow \alpha f = g' \cdot h'$ mit $g', h' \in \mathbb{Z}[X]$,
$g' = \sum_{i=0}^{r} a_i X^i, \quad h' = \sum_{j=1}^{s} b_j X^j \quad (a_i, b_j \in \mathbb{Z})$

Zeigen: $\alpha \mid g' \cdot h'$ in $\mathbb{Z}[X]$

Sei p Primteiler von α.
Zeigen: $p \mid a_i$ für alle $i = 0, \ldots, r$ oder $p \mid b_j$ für alle $j = 0, \ldots, s \quad (*)$

Ann.: $(*)$ gilt nicht
$\Rightarrow$ es existieren $i, j : p \nmid a_i$ und $p \nmid b_j$
Setzen: $i_0 = min\{i : p \nmid a_i\}$, $j_0 = min\{j : p \nmid b_j\}$
Betrachten:

$$c_{i_0+j_0} := \sum_{i+j=i_0+j_0} a_i b_j = a_{i_0} b_{j_0} + \sum_{\substack{i+j=i_0+j_0 \\ i \neq i_0}}{}' a_i b_j$$

$$\text{Für} \quad \left.\begin{array}{lll} i < i_0 & :\Rightarrow & p \mid a_i \Rightarrow p \mid a_i b_j \\ i > i_0 & :\Rightarrow & j < j_0 \Rightarrow p \mid b_j \Rightarrow p \mid a_i b_j \end{array}\right\} p \mid \sum{}'$$

Da $p \mid \alpha f = g' \cdot h' \Rightarrow p \mid c_{i_0+j_0} \Rightarrow p \mid a_{i_0} \cdot b_{j_0} = c_{i_0+j_0} - \sum{}'$
Da p eine Primzahl ist folgt $p \mid a_{i_0}$ oder $p \mid b_{j_0}$ Dies ist Widerspruch
$\overset{O.B.d.A.}{\Rightarrow} p \mid g' \Rightarrow g'' = \frac{1}{p} g' \in \mathbb{Z}[X]$ mit $deg(g') = deg(g'') \Rightarrow g' \cdot h' = pg''h' = \alpha f \Rightarrow \frac{\alpha}{p} \cdot f = g'' \cdot h'$
Setzen wir das Verfahren über alle Primteiler von α fort, liefert dies Polynome $\hat{g}, \hat{h} \in \mathbb{Z}[X]$ mit $deg(\hat{g}) = deg(g)$ bzw. $deg(\hat{h}) = deg(h)$ sowie $f = \hat{g} \cdot \hat{h}$. $\Rightarrow f \in \mathbb{Z}[X]$ ist reduzibel. Dies ist ein Widerspruch zur 1. Behauptung

□

Satz 4.3.25 (Eisensteinkriterium). *Sei $f = \sum_{k=0}^{n} c_k X^k \in \mathbb{Z}[X]/\mathbb{Z}, c_k \neq 0$ ein normiertes Polynom und $n = deg(f) \geq 2$ (Für $n = 1$ trivial). Wenn eine Primzahl $p \in \mathbb{N}$ existiert mit $p \mid c_k$ für alle $k = 0, 1, \ldots, n-1$ und $p^2 \nmid c_0$, so ist f in $\mathbb{Z}[X]$ und damit in $\mathbb{Q}[X]$ irreduzibel.*

Beweis. Sei f irreduzibel in $\mathbb{Z}[X]$, d.h. es existieren Polynome $g, h \in \mathbb{Z}[X]$ mit $f = g \cdot h$ und $deg(g), deg(h) < deg(f)$.

$$g = \sum_{i=0}^{r} a_i X^i, \quad h = \sum_{j=0}^{s} b_j X^j \quad (a_i, b_j \in \mathbb{Z})$$
$$r = deg(g), \quad s = deg(h)$$

Da $p \mid c_0 = a_0 b_0 \Rightarrow p \mid a_0$ oder $p \mid b_0$. Falls beides eintritt, so gilt $p^2 \mid c_0^2$. Dies ist Widerspruch
$\Rightarrow$ O.B.d.A. sei $p \mid a_0 \Rightarrow p \nmid b_0$
Da $1 = c_n = a_r b_s \Rightarrow a_r = b_s = \pm 1 \Rightarrow p \nmid a_r$
Setzen:

$$k = min\{i \in \{0, \ldots, r\} : p \nmid a_i\} \Rightarrow 0 < k \leq r < n$$

Betrachten: $c_k = \sum_{i=0}^{k} a_i b_{k-i}$ Für $0 \leq i < k$ gilt: $p \mid a_i \Rightarrow p \mid a_i b_{k-i}$ für alle $i = 0, \ldots, k-1$.
Da $k < n \Rightarrow p \mid c_k \Rightarrow p \mid c_i - \sum_{i=0}^{k-1} a_i b_{k-i} = a_i b_0 \Rightarrow p \mid a_k$ oder $p \mid b_0$
Da $p \nmid b_0 \Rightarrow p \mid a_k$ Dies ist Widerspruch zur Definition zu k
$\Rightarrow$ Behauptung □

Beispiel 4.3.26.

1. $f = X^4 + 25X^2 + 5X + 10$
   $p = 5 \Rightarrow f$ *irreduzibel in* $\mathbb{Z}[X] \quad (\mathbb{Q}[X])$

1') *Auf* $f = X^3 + 28X^2 - 15X + 6$ *ist das Kriterium nicht anwendbar.*

2. $f = X^n - a \in \mathbb{Z}[X]$ *mit* $|a| \neq 1$ *(Warum?) und* a *ist quadratfrei (d.h.* $a = \prod_{i=1}^{\infty} p_i^{\alpha_i}$ *mit* $\alpha_i = 0$ *oder* $\alpha_i = 1$*) ist irreduzibel über* $\mathbb{Q}$*.*
konkret:

$f_1 = X^4 - 30 \quad 30 = 2 \cdot 3 \cdot 5$ *irreduzibel*
$f_2 = X^4 - 9 \quad q$ *nicht quadratfrei, da* $f_2 = (X^2 - 3)(X^2 + 3)$
$f_3 = X^4 - 28 \quad 28 = 2^2 \cdot 7$ *nicht quadratfrei, aber Kriterium für* $p = 7$ *anwendbar*
$\Rightarrow f_3$ *irreduzibel*

3. *Sei* p *eine Primzahl. Dann ist* $f = \sum_{i=0}^{p-1} X^i \in \mathbb{Z}[X]$ *über* $\mathbb{Q}$ *irreduzibel.*
Übung !!!

4.4 Endliche Körpererweiterungen

Definition 4.4.1. *Ist* K *ein Teilkörper von* L $(K \subseteq L)$*, so heißt* L *Körpererweiterung von* K *oder Körpererweiterung über* K*. Wir schreiben dafür* $L : K$*.*
Ein Körper M *heißt Zwischenkörper der Erweiterung* $L : K$*, wenn* M *Teilkörper* L *ist mit* $K \subseteq M \subseteq L$*.*

Beispiel 4.4.2. $\mathbb{C} : \mathbb{Q}$ *ist eine Körpererweiterung und* $\mathbb{R}$ *ein Zwischenkörper*

Bemerkung 4.4.3. *Sei* $L : K$ *eine Körpererweiterung, dann ist* L *natürlicherweise ein Vektorraum über* K*. Dann ist* $(L, +)$ *eine abel'sche Gruppe und durch* $k \cdot l \quad (k \in K, l \in L)$ *ist "skalare" Multiplikation mit den Elementen aus* K *erklärt. Aus den Körperaxiomen folgen dann die des Vektorraums.*

Definition 4.4.4. *Sei* $L : K$ *eine Erweiterung*

1. *Die Dimension* $dim_K L$ *des Vektorraums* L *über* K *heißt der Grad der Erweiterung* $L : K$ *(kurz:* $dim_k L = [L : K] = Grad(L : K)$*)*
2. *Die Erweiterung* $L : K$ *heißt endliche Körpererweiterung, wenn der* $Grad(L : K) < \infty$

Beispiel 4.4.5.

1. $[\mathbb{C} : \mathbb{R}] = 2$ *(Basis:* $1, i$ *mit* $z = x \cdot 1 + y \cdot i$*)*
2. $[\mathbb{R} : \mathbb{Q}] = \infty$

Beweis. Ann.: $[\mathbb{R} : \mathbb{Q}] = n < \infty$
$\Rightarrow$ es existiert eine Basis $\{b_1, \ldots, b_n\}$
$\Rightarrow$ für alle $r \in \mathbb{R}$ gilt: $r = \sum_{i=1}^{n} \lambda_i b_i$
mit abzählbar vielen $\lambda_i \in \mathbb{Q}$ und endlich vielen b_i (nämlich genau n), weshalb die Summe abzählbar ist. Dies ist ein Widerspruch zu $r \in \mathbb{R}$ mit $\mathbb{R}$ überabzählbar. $\Rightarrow$ Vermutung $\square$

3. $\mathbb{Q}[\sqrt{2}] = \{r_1 + r_2\sqrt{2} \mid r_1, r_2 \in \mathbb{Q}\} \supset \mathbb{Q}$
   $[\mathbb{Q}[\sqrt{2}] : \mathbb{Q}] = 2$

4. $[L : K] = 1 \Rightarrow L = K$

Satz 4.4.6 (Gradsatz). *Ist M ein Zwischenkörper der Erweiterung $L : K$, so gilt:*

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

Beweis. Seien $X = \{x_\alpha\}_{\alpha \in A}, Y = \{y_\beta\}_{\beta \in B}$ Basen der Erweiterung $M : K$ bzw. $L : M$.
Zeigen: $Z = \{x_\alpha y_\beta : (\alpha, \beta) \in A \times B\}$ ist Basis der Erweiterung $L : K$
Da Y Basis des M-Vektorraums $L : K$, gilt:
für alle $x \in L$ existiert ein $m_\beta \in M : x = \sum_\beta m_\beta y_\beta$
(wobei $m_\beta = 0$ für fast alle β)
Da X Basis des K-Vektorraums M ist, gilt:
für alle m_β existiert ein $k_{\beta\alpha} \in K : m_\beta = \sum_\beta = \sum_\alpha k_{\beta\alpha} x_\alpha \quad (k_{\beta\alpha} = 0$ für fast alle $\alpha)$

$\Rightarrow x = \sum_{\alpha,\beta} k_{\beta\alpha} x_\alpha y_\beta \Rightarrow Z$ erzeugt einen K-Vektorraum L.

Sei $0 = \sum_{\alpha,\beta} \xi_{\alpha\beta} \cdot x_\alpha \dot{y}_\beta \qquad (\xi_{\alpha\beta} \in K)$
$\Rightarrow 0 = \sum_\beta (\sum_\alpha \xi_{\alpha\beta} x_\alpha) y_\beta$
Da Y eine Basis ist, folgt: $0 = \sum_\alpha \xi_{\alpha\beta} x_\alpha$ für alle β.
Da X eine Basis ist, folgt weiterhin: $\xi_{\alpha\beta} = 0$ für alle $\alpha, \beta \Rightarrow Z$ ist eine Basis

$$[L : K] = dim_K L = |Z| = |A \times B| = |A||B| = dim_K M \cdot dim_K L = [M : K] \cdot [L : M]$$

□

Folgerung 4.4.7.

1. *Ist M ein Zwischenkörper der endlichen Körpererweiterung $L : K$, so sind die Zahlen $[L : M]$ und $[M : K]$ Teiler der Zahl $[L : K]$*

2. *Ist $[L : K] = p$, p ist eine Primzahl, so besitzt die Erweiterung $[L : K]$ keinen echten Zwischenkörper. (z.B $|\mathbb{C} : \mathbb{R}| = 2$)*

3. *Sei M ein Zwischenkörper von $L : K$. Dann gilt:*

$$L = M \Leftrightarrow [L : K] = [M : K]$$

4. *Für einen Körperturm $K_1 \subseteq K_2 \subseteq \ldots \subseteq K_n$ (d.h. eine Folge $(K_{i+1} : K_i)_{i=1}^{n-1}$ von Körpererweiterungen)*
   gilt:

$$[K_n : K_1] = \prod_{i=1}^{n-1} [K_{i+1} : K_i]$$

Definition 4.4.8. *Sei $L : K$ eine Körpererweiterung, dann gilt:*

1. *Das Element $a \in L$ heißt algebraisch über K, wenn eine Polynom $f \in K[X]/\{0\}$ existiert mit $f(a) = 0$*
2. *Ein normiertes Polynom $f \in K[X]$ mit $f(a) = 0$ und minimalem Grade heißt Minimalpolynom des Elementes $a \in L$ über K.*
3. *$a \in L$ heißt transzendent über K, wenn aus $f \in K[X]$ mit $f(a) = 0$ stets $f = 0$ folgt.*

Beispiel 4.4.9.

1. *$k \in K$ ist algebraisch über K, da k Nullstelle zu $X - k \in K[X]$ ist.*
2. *$i \in \mathbb{C}$ algebraisch über $\mathbb{Q}$, da i Nullstelle von $f = X^2 + 1 \in \mathbb{Q}[X]$ ist.*
3. *$\sqrt[3]{2} \in \mathbb{R}$ algebraisch über $\mathbb{Q}$*
4. *$X \in K[X]$ transzendent über K*
5. *$\pi, e \in \mathbb{R}$ transzendent über $\mathbb{Q}$*

Satz 4.4.10. *Sei $L : K$ eine Körpererweiterung und $a \in L$ algebraisch über K.*

1. *Das Minimalpolynom $f \in K[X]$ von a über K ist eindeutig bestimmt und irreduzibel (über K).*
2. *Ist $g \in K[X]$ ein normiertes, irreduzibles Polynom über K mit $g(a) = 0$, so ist $g = f$ das Minimalpolynom.*

Beweis. 1. Seien $f_{1/2} \in K[X]$ das Minimalpolynom von a.
Ann.: $f_1 \neq f_2$
$\Rightarrow deg(f_1 - f_2) < deg(f_1)$
Nun gilt: $(f_1 - f_2)(a) = f_1(a) - f_2(a) = 0$ dies ist ein Widerspruch
$\Rightarrow f$ eindeutig bestimmt

Ann.: f ist reduzibel $\Rightarrow f = f_1 + f_2$ mit $1 \leq deg(f_{1/2}) \leq deg(f)$
Da $f(a) = 0 \Rightarrow f_1(a) = 0$ oder $f_2(a) = 0$ Widerspruch zu (Minimal-Grad)

2. Sei g normiert, irreduzibel mit $g(a) = 0$ und f das Minimalpolynom zu a.
Aus dem Satz über die Division mit Rest folgt, dass $q, r \in K[X] : g = f \cdot q + r$ existieren mit $r = 0$ oder $deg(r) < deg(f)$
$\Rightarrow r(a) = (g - (f \cdot q)(a)) = g(a) - f(a) \cdot q(a) = 0$
Wenn $r \neq 0$ Widerspruch wegen Minimalpolynom
$r = 0 \Rightarrow g = f \cdot q$

Da g irreduzibel ist, so ist $f \notin K \Rightarrow q \in K$
Da beide normiert sind $\Rightarrow q = 1 \Rightarrow q = f$

□

Zunächst:

Lemma 4.4.11. *Sei R ein Integritätsbereich und K Körper mit $K \subseteq R$ (K als Teilring). Wenn $dim_K R < \infty$, so ist R ein Körper.*

Beweis. Sei $r \in R/\{0\}$. Wir zeigen, dass r invertierbar (in R) ist.
Betrachten die Abbildung $\mu_r : R \to R$ mit $\mu_r(s) = rs (s \in R)$. Offenbar ist μ_r K-linear.
Weiter folgt aus $\mu_r(s) = 0 = rs \Rightarrow s = 0$ (nullteilerfrei)$\Rightarrow$ μ_r ist injektiv.
$\Rightarrow$ Da $\mathbf{1} \in R$ ist, existiert ein $s' \in R$ mit $\mathbf{1} = \mu_r(s') = rs'$
$\Rightarrow$ r invertierbar. □

Satz 4.4.12. *Sei $L : K$ eine Körpererweiterung; $a \in L$ algebraisch über K und $f \in K[X]$ das Minimalpolynom. Wenn a existiert mit $a = deg(f)$, dann gilt:*

1. *Die Elemente $\mathbf{1}, a, a^2, \ldots, a^{n-1}$ über K sind linear unabhängig.*

2. $K(a) := \left\{ \sum_{i=0}^{n-1} \lambda_i a^i : \lambda_i \in K \right\}$ *ist der kleinste Teilkörper von L, der a und K umfasst (d.h. $[K(a) : K] = n$)*

Beweis. zu 1) : $\sum \lambda_i a^i = 0 \quad (\lambda_i \in K)$
Betrachten $g = \sum_{i=0}^{n-1} \lambda_i X^i \in K[X]$
$\Rightarrow deg(g) \leq n - 1 < n$ und $g(a) = 0 \Rightarrow g = 0 \Rightarrow \lambda_i = 0$ für alle $i = 0, \ldots, n-1$

zu 2) : Offenbar ist $K(a)$ ein K-Vektorraum mit $dim_K K(a) = n$ und $K \subseteq K(a)$
Zeigen: $K(a)$ ist kommutativer, nullteilerfreier Ring,

$$x = \sum_{i=0}^{n-1} \lambda_i a^i, \quad y = \sum_{j=0}^{n-1} \mu_j a^j \in K(a)$$

Ist $xy \in K(a)$?
Wo liegen die Elemente a^k für $k \geq n$?
Betrachten: a^n. Sei $f = X^n + \sum_{i=0}^{n-1} v_i X^i$ das Minimalpolynom von a über K.

$$\Rightarrow 0 = f(a) = a^n + \sum v_i a^i$$
$$\Rightarrow a^n = -\sum_{i=0}^{n-1} v_i a^i \in K(a)$$
$$\Rightarrow a^n \in K(a)$$
per Induktion: $a^{n+1} \in K(a)$ für alle $i \geq 0$
$$\Rightarrow xy \in K(a)$$

Da offenbar $K(a) \in L$, ist $K(a)$ nullteilerfrei.
$K(a)$ ist der Integrationsbereich mit $K \subseteq K(a)$
wegen Lemma $(4.4 - 11) \Rightarrow K(a)$ ist Körper mit $K \subseteq K(a) \subseteq L$
Sei M kleinster Teilkörper von L, der K und a umfasst.

$$K \subseteq M \subseteq L$$

Da $a \in M$ und $K \subseteq M \Rightarrow a^i \in M, \lambda_i \in M \Rightarrow \sum \lambda_i a^i \in M$
$\Rightarrow K(a) \subseteq M \Rightarrow K(a) = M$

□

Satz 4.4.13. *Sei $L : K$ eine Körpererweiterung und $a \in L$, dann gilt:*
a ist genau dann algebraisch über K, wenn ein Körperturm $K \subseteq M \subseteq L$ existiert mit $a \in M$ und $[M : K] < \infty$

Beweis. "⇒" Setzen $M := K(a)$
$\Rightarrow [M : K] = deg(f) < +\infty$ (f ist Minimalpolynom)

"⇐" Sei $n = [M : K] < +\infty \Rightarrow \mathbf{1}, a, a^2, \ldots, a^n$ sind linear unabhängig
$\Rightarrow$ es existieren $\lambda_0, \lambda_1, \ldots, \lambda_n \in K : \sum_{i=0}^{n} \lambda_i a^i = 0$ mit mindestens einem $\lambda_i \neq 0$
Setzen $g = \sum_{i=0}^{n} \lambda_i X^i \in K[X]$ mit $g \neq 0$.
Außerdem ist
$g(a) = 0 \Rightarrow a$ ist algebraisch über K

□

Satz 4.4.14. *Sei $L : K$ eine Körpererweiterung und $a, b \in L$ algebraisch über K. Dann sind die Elemente $-a, a + b, ab$ und $a^{-1} \quad (a \neq 0)$ algebraisch über K.*

Beweis. Wir setzen $K(a, b) := K(a)(b)$
Es existiert ein Körperturm $K \subseteq K(a) \subseteq K(a, b) \subseteq L$, wobei die obigen Elemente alle in $K(a, b)$ liegen.

Zeigen: $[K(a,b):K] < \infty$
Sei f bzw. g das Minimalpolynom von a bzw. b über K mit:

$$deg(f) = n, \qquad deg(g) = m$$

$\Rightarrow [K(a):K] = n$
Da $K \subseteq K(a)$ ist, so ist auch $g \in K(a)[X]$ mit $g(b) = 0 \Rightarrow b$ ist algebraisch über $K(a)$.
$\Rightarrow deg($Minimalpolynom von b über $K(a) \leq m$
$\Rightarrow [K(a,b):K(a)] \leq m$
Gradsatz $\Rightarrow [K(a,b):K] = [K(a):K] \cdot [K(a,b):K(a)] < n \cdot m \leq \infty$
$\overset{\text{Satz } (4.4-13)}{\Rightarrow}$ Behauptung □

Satz 4.4.15 (Hauptsatz). *Sei $\mathcal{P}$ der Körper der konstruierbaren Zahlen (Satz $(4.2-5)$) und $z \in \mathcal{P}$.*
Dann gibt es einen Körperturm

$$\mathbb{Q} = K_0 \subset K_1 \subset \ldots \subset K_n = L \quad (\subset \mathbb{C})$$

mit $z \in K_n = L$ mit $[K_i : K_{i-1}] = 2$ für alle $i = 1, \ldots, n$

Beweis. Wir führen den Beweis nach der Anzahl der Kostruktionsschritte.
Keine Konstruktionsschritte: $1, 0 \in \mathbb{Q}$
Sei k ein Teilkörper von $\mathbb{C}$ und $p, q, r \in k, |qr| \in k$
Die Geradengleichung, die die Gerade durch p, q beschreibt, hat einen Koeffizienten aus k, die Kreisgleichung, die den Kreis um p mit dem Radius $|qr|$ beschreibt, hat ebenfalls einen Koeffizienten aus k.
$\Rightarrow$ Die Schnittpunkte dieser Objekte sind Nullstellen von Polynomen mit dem Grade 2.
$\Rightarrow$ Man erhält echte Körpererweiterungen mit dem Grade$= 2$. □

Folgerung 4.4.16. *Jede konstruierbare Zahl $z \in \mathcal{P}$ ist algebraisch über $\mathbb{Q}$ und der Grad des Minimalpolynoms von z über $\mathbb{Q}$ ist eine Zweierpotenz $(2^i, i \geq 0)$.*

Beweis. Sei $z \in \mathcal{P} \Rightarrow$ es existiert eine Körpererweiterung $K : \mathbb{Q}$ mit $z \in K$ und $[K : \mathbb{Q}] = 2^n$.
$\Rightarrow z$ ist algebraisch über $\mathbb{Q}$ mit $deg(f) = l$.
$\Rightarrow [\mathbb{Q}(z) : \mathbb{Q}] = l$
Nun ist $\mathbb{Q} \subset \mathbb{Q}(z) \subseteq K$ und wegen dem Gradsatz folgt:

$$2^n = [K : \mathbb{Q}] = [\mathbb{Q}(z) : \mathbb{Q}] \cdot [K : \mathbb{Q}(z)] = l \cdot k$$

□

Satz 4.4.17. *Sei $z \in \mathbb{C}$. Wenn ein Körperturm $\mathbb{Q} = K_0 \subset K_1 \subset \ldots \subset K_n = K \quad (\subset \mathbb{C})$ mit $z \in K$ und $[K_i : K_{i-1}] = 2 \quad (i = 1, \ldots n)$ existiert, so ist $z \in \mathcal{P}$.*

Beweis. Sei $[K_i : K_{i-1}] = 2$. Wir zeigen: Es existieren $\omega_i \notin K_{i-1}$ mit $K_i = K_{i-1}(\omega_i)$ und $\omega_i^2 \in K_{i-1}$

Sei $a \in K_i/K_{i-1}$ (Da $[K_i : K_{i-1}] = 2$ ist, so ist $1, a$ Basis zu K_i über K_{i-1}), dann sind die Elemente $\mathbf{1}, a, a^2$ linear unabhängig.

$\Rightarrow$ es existieren $p, q \in K_{i-1} : a^2 + pa + q = 0$
Setzen:$\omega_i = a + \frac{p}{2} \Rightarrow \omega_i \notin K_{i-1}$

$$\omega_i^2 = a^2 + pa + \frac{p^2}{4} = -pa - q + pa + \frac{p^2}{4} = \frac{p^2}{4} - q \in K_{i-1}$$

Nun ist $K_{i-1} \subset K_{i-1}(\omega_i) \subseteq K_i$. Da 2 eine Primzahl ist folgt mit der Folgerung $(4.4 - 7(2))$, dass $K_i = K_{i-1}(\omega_i)$
Induktion: $\mathbb{Q} = K_0 \subset \mathcal{P}$, sei $K_{i-1} \subset \mathcal{P} \Rightarrow \omega_i^2 \in \mathcal{P}$
$\mathcal{P}$ ist algebraisch unter der Quadratwurzel $\Rightarrow \omega_i \in \mathcal{P}$

$$\Rightarrow K_i = K_{i-1}(\omega_i) \subset \mathcal{P} \Rightarrow \text{ Behauptung}$$

□

4.5 Zu den klassischen Problemen

1. Delisches Problem: Verdoppelung eines Würfels

   $a \in \mathbb{R}$ und $a = \sqrt[3]{2} \in \mathcal{P}$?

   $f = X^3 - 2 \in \mathbb{Q}[X]$
   $f(a) = 0$. Nach Eisenstein $(p = 2)$ ist f irreduzibel $\Rightarrow f$ ist das Minimalpolynom von a
   $\Rightarrow deg(f) = 3$ ist keine 2-er Potenz
   $\Rightarrow \sqrt[3]{2} \notin \mathcal{P}$

2. Quadratur des Kreises:

   Es existiert ein $a \in \mathcal{P} \cap \mathbb{R} : a^2 = \pi$
   Ann.: Es existiert ein $a \in \mathcal{P} : a^2 = \pi \Rightarrow \pi \in \mathcal{P}$
   $\Rightarrow \pi$ ist algebraisch über $\mathbb{Q}$. Dies steht im Widerspruch zur Transzendenz von π

3. Winkeldreiteilung:
   Bemerkung:

   1) α ist konstruierbar $\Leftrightarrow \cos\alpha \in \mathcal{P}$

2) $\cos\alpha$ nicht konstruierbar $\Leftrightarrow$ 3α auch nicht konstruierbar

Zeigen: $\cos 20^\circ \notin \mathcal{P} \Leftrightarrow 3\alpha = 60$ nicht dreiteilbar
Satz von Moivre:

$$\begin{aligned}\cos 3\alpha + i\sin 3\alpha &= (\cos\alpha + i\sin\alpha)^3 \\ &= \cos^3\alpha + 3\cos\ 2\ \alpha\ isin\ \alpha + 3\cos\alpha i^2\sin^2\alpha + i^3\sin^3\alpha\end{aligned}$$

$$\begin{aligned}\cos 3\alpha &= \cos^3\alpha - 3\cos\alpha\sin^2\alpha \\ \cos 3\alpha &= 4\cos^3\alpha - 3\cos\alpha \\ a &= \cos 20^\circ \quad (\alpha = 20^\circ) \\ \frac{1}{2} &= 4a^3 - 3a \Rightarrow a \text{ ist eine Nullstelle von } h = 8X^3 - 6X - 1 \\ h(\frac{y+1}{2}) &= y^3 + 3y^2 - 3 \\ p = 3 &\overset{\text{Einstein}}{\Longrightarrow} h(\frac{y+1}{2}) \text{ ist irreduzibel} \\ \Rightarrow f = \frac{1}{8}h(X) &\text{ ist irreduzibel } \Rightarrow f \text{ ist Minimalpolynom von } a \\ deg(f) = 3 &\text{ (keine Zweierpotenzen) } \Rightarrow a \notin \mathcal{P}\end{aligned}$$

4. Konstruktion regelmäßiger n-Ecke:

Für welche $n \in \mathbb{N}$ ist der Eckpunkt eines regelmäßigen n-Eckes konstruierbar?

$e^{i\frac{2\pi}{n}} \in \mathcal{P}?$ $\quad \cos\frac{2\pi}{n} \in \mathcal{P}?$

Fall $n = 7, a = \cos\frac{2\pi}{7}$. Das Minimalpolynom von a ist $f : X^3 + X^2 - 2X - 1$ über $\mathbb{Q}$,
$deg(f) = 3$
$\Rightarrow a \notin \mathcal{P} \Rightarrow 7 -$ Eck ist nicht konstruierbar

Kapitel 5

Einige Fakten zur Körpertheorie

5.1 Ringe und maximale Ideale

Definition 5.1.1. *Sei R ein Ring mit dem $\mathbf{1}$-Element. Eine Untergruppe $I \subset (R, +)$ heißt Ideal in R (über R), wenn gilt:*

$$rx, xr \in I \text{ für alle } r \in R, \text{ für alle } x \in I$$

Beispiel 5.1.2.

1. $R = \mathbb{Z}, I = 2\mathbb{Z}$
2. $R = C[0,1], \emptyset \neq F \subseteq [0,1]$
   $I_F := \{x \in R : x(t) = 0 \text{ für alle } t \in F\}$
3. *Sei K ein Körper,* $R = K[X], f \in R$ *fix* , $I = f \circ K[X]$

Bemerkung 5.1.3. *Das Ideal ist im Allgemeinen kein Unterring von R, da i. allg. $\mathbf{1} \notin I$.*

Definition 5.1.4. *Seien R, S Ringe mit $\mathbf{1}$-Element.*

1. *Die Funktion $f : R \to S$ heißt (Ring-)Homomorphismus, wenn gilt:*

$$\begin{aligned} f(r_1 + r_2) &= f(r_1) + f(r_2) \qquad \text{für alle } r_{1,2} \in R \\ f(r_1 \cdot r_2) &= f(r_1) f(r_2) \\ f(\mathbf{1}_R) &= \mathbf{1}_S \end{aligned}$$

2. *Ist f zusätzlich bijektiv, so heißt f Isomorphismus*

Bemerkung 5.1.5. *Sei $f : R \to S$ ein Homomorphismus, dann gilt:*

1. $im(f) := \{f(r) : r \in R\}$ *ist ein Unterring von* S
2. $ker(f) := \{r \in R : f(r) = 0\}$ *ist das Ideal in* R

Satz 5.1.6. *Sei* R *ein Ring mit* $\mathbf{1}$*-Element und* I *ein Ideal.*

1. *Die Relation "*$x \overset{I}{\sim} y$*"* $\overset{def.}{\Longleftrightarrow}$ $x - y \in I$ *ist eine Äquivalenzrelation auf* R
2. *Die Nebenklasse bezüglich "*$\overset{I}{\sim}$*" habe die Gestalt*

$$\overline{r} = r + I = \{r - i, i \in I\}$$

3. *Durch folgende Operationen wird der Faktorring* R/I *erklärt:*

$$\begin{array}{rcl} \overline{r_1} + \overline{r_2} & := & \overline{r_1 + r_2} \\ \overline{r_1} \cdot \overline{r_2} & := & \overline{r_1 \cdot r_2} \end{array} \quad \textit{für alle } r_{1,2} \in R/I$$

4. *die kanonische Abbildung* $\pi : R \to R/I$ *mit* $\pi(r) = \overline{r} \quad (r \in \overline{r})$ *ist ein surjektiver Ring-Homorphismus mit* $ker(\pi) = I$

Beweis Übung. □

Folgerung 5.1.7. *Sei* $f : R \to S$ *ein Homomorphismus, dann gilt:*

$$R/ker(\pi) \cong im(f)$$

Definition 5.1.8. *Das Ideal* $M \subset R$ *des Rings* R *heißt maximales Ideal, wenn gilt:*

1. $M \neq R$
2. *für jedes Ideal* $I \neq R$ *mit* $M \subseteq I$ *ist* $M = I$

Satz 5.1.9. *Das Ideal* $I \subset R$ *ist genau dann maximal, wenn der Faktorring* $R/I \neq \{\overline{0}\}$ *und* R/I *als auch* $\{\overline{0}\}$ *die einzigen Ideale in* R/I *sind.*

Folgerung 5.1.10. *Ein kanonischer Ring* R *ist genau dann ein Körper, wenn* $R \neq \{0\}$ *und in* R *nur* R *und* $\{0\}$ *die einzigen Ideale sind.*

Beweis. "⇒" Sei R ein Körper und $I \subseteq R$ ein Ideal mit $I \neq \{0\}$
⇒ es existiert ein $x \in I/\{0\}$ $\overset{\text{Körper}}{\Rightarrow}$ es existieren $x^{-1} \in R : x^{-1}x = \mathbf{1}$ $\overset{\text{Ideal}}{\Rightarrow}$ $\mathbf{1} \in I$ $\overset{\text{Übung}7.3/4}{\Longrightarrow}$ $R = I$

"⇐" Sei die Bedingung erfüllt. Sei $x \in R/\{0\}$
Zeigen: Es existiert ein $x^{-1} \in R$
Setzen: $I := xR = \{xr : r \in R\} = \langle x \rangle$.
Offenbar ist I ein Ideal in R mit $x \in I$ (d.h. $I \neq \{0\}$).
$\Rightarrow I = R \Rightarrow \mathbf{1} \in I$
$\Rightarrow$ es existiert ein $r \in R : \mathbf{1} = xr \Rightarrow x$ ist invertierbar $\Rightarrow$ Behauptung

□

Folgerung 5.1.11. *Sei R ein kommutativer Ring, $I \subseteq R$ ein Ideal von R, so gilt:*
I ist in R maximales Ideal $\Leftrightarrow$ R/I ist ein Körper

Beispiel 5.1.12. 1. $R = \mathbb{Z}, \quad m\mathbb{Z}$ *ist maximal* $\Leftrightarrow \mathbb{Z}/\mathbb{Z}m$ *ist ein Körper, wenn m eine Primzahl ist.*

2. $R = C[0,1], \quad t_0 \in [0,1]$
$M = \{x \in R : x(t_0) = 0\}$
$f : R \to \mathbb{R}$ *mit* $f(x) = x(t_0)$
Offenbar ist f ein Homomorphismus.
$ker(f) = M, \quad im(f) = \mathbb{R}$
$\mathbb{R} = im(f) \cong R/ker(f) = R/M$
$\Rightarrow M$ *ist maximales Ideal ($\mathbb{R}$ ist ein Körper, R/M auch)*

Bezeichnung 5.1.13. *Sei p eine Primzahl, so wird der Körper $\mathbb{F}_p$ wie folgt dargestellt:*

$$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$$

Satz 5.1.14. *Sei K ein Körper und $R = K[X]$.*

1. *Jedes Ideal in R hat die Form $f \cdot K[X] = \langle f \rangle := \{f \cdot g : g \in K[X]\}$ für gewisse Polynome $f \in K[X]$ (Hauptideal)*

2. *$\langle f \rangle = f \cdot K[X]$ ist genau dann maximales Ideal in $K[X]$, wenn f irreduzibel ist.*
Insbesondere gilt:
Ist $f \in K[X]$ irreduzibel, so ist $K[X]/\langle f \rangle$ ein Körper.

Beweis. zu 1) Sei $I \neq \{0\}$ ein Ideal in R. Wir wählen ein $f \in I/\{0\}$ mit dem mit minimalem Grad $\Rightarrow f \cdot K[X] \subseteq I$
Sei $g \in I/\{0\}$. Mit dem Satz über die Division mit Rest folgt:
Es existieren $q, r \in R : g = q \cdot f + r$, wobei $r = 0$ ist oder $deg(r) < deg(f)$.

$$\Rightarrow r = g - q \cdot f \in I \Rightarrow r = 0$$

$$\Rightarrow g = q \cdot f \in f \cdot K[X] \Rightarrow \text{ Behauptung}$$

zu 2) Für $f_{1/2} \in K[X]$ gilt:

$$f_1 \mid f_2 \Leftrightarrow f_2 \cdot K[X] \subseteq f_1 \cdot K[X]$$

Hieraus folgt:

$$f \text{ irreduzibel} \Leftrightarrow f \cdot K[X] \text{ maximal}$$

□

Satz 5.1.15. *Sei K ein Körper und $K^* = (K/\{0\}, \cdot)$, dann gilt:*
Jede Untergruppe $G \subseteq K^*$ ist zyklisch

Beweis. setzen:

$$\begin{aligned} n_i &= ord(g_i) \quad (g_i \in G, i = 1, \ldots, r) \\ n &= kgV(n_1, \ldots, n_r) \Rightarrow n = k_i n_i \quad (i = 1, \ldots, r) \\ &\Rightarrow (g_i)^n = \mathbf{1} \text{ für alle } g_i \in G \end{aligned}$$

Sei $f = X^n - 1 \in K[X] \Rightarrow f(g_i) = 0$
Da $f \in K$ höchstens n Nullstellen besitzt, folgt: $|G| = r \leq n$.
Seien nun $p_1 < p_2 < \ldots < p_t$ Primzahlen in der Darstellung von n:

$$n = p_1^{l_1} \cdot p_2^{l_2} \cdot \ldots \cdot p_t^{l_t}$$

Zu jedem Faktor $p_s^{l_s}$ existieren n_{i_s} mit $p_s^{l_s} \mid n_{i_s}$.
Wir ordnen desen Faktoren $p_s^{l_s}$ das Element g_{i_s} zu
$\Rightarrow ord(g_{i_s}) = p_s^{l_s} \cdot m_s$, wobei der $ggT(m_s, p_s^{l_s}) = 1 \quad (s = 1, \ldots, l)$
$\Rightarrow ord(g_{i_s}^{m_s}) = p_s^{l_s}$ (Übung $6/2$)
Setzen: $g := g_{i_1}^{m_1} \cdot g_{i_2}^{m_2} \cdot \ldots \cdot g_{i_z}^{m_z} \Rightarrow ord(g) = p_1^{l_1} \cdot \ldots \cdot p_z^{l_z} = n$
$\Rightarrow |G| \geq n, \quad |\langle g \rangle| = n \Rightarrow |G| = n$, da $\langle g \rangle \subseteq G \Rightarrow G = \langle g \rangle$ □

Beispiel 5.1.16. *Sei p eine Primzahl und $\mathbb{F}_p$ ein endlicher Körper. Daraus folgt, dass $(\mathbb{F}_p^*, \cdot)$ eine endliche Gruppe ist und mit Satz $(5.1 - 16)$ gilt:*
$\mathbb{F}_p$ ist zyklisch, d.h. es existiert ein $g \in \mathbb{Z} : \mathbb{F}_p^* := \{\overline{\mathbf{1}}, \overline{g}, \overline{g^2}, \ldots, \overline{g^{p-2}}\}$, was bedeutet, dass für alle $x \in \{1, \ldots, p-1\}$ genau ein $i \in \{0, \ldots, p-2\}$ existiert mit $x = g^i$ mod(p)
g heißt Primitivzahl (-wurzel) mod(p)
konkret:

$$\begin{aligned} &p = 5, \quad g = 2 \\ &1 \leq 2^0, \quad 2 \equiv 2^1, \quad 3 \equiv 2^3, \quad 4 \equiv 2^2 \end{aligned}$$

Bemerkung 5.1.17. *Ist G eine zyklische Gruppe mit $|G| = n$, so ist die Anzahl der Elemente in G mit der Ordnung n gleich φ_n (Eulersche Funktion)*

5.2 Zerfällungskörper

Sei K ein Körper und $f \in K[X]$.

Problem: Gesucht ist der Körper L, über den f in Linearfaktoren zerfällt.

Satz 5.2.1 (Kronecker). *Sei K ein Körper mit einem über K irreduziblen Polynom $p \in K[X]$, dann gibt es eine Körpererweiterung $L : K$ mit $[L : K] = deg(p)$, so dass p in L eine Nullstelle besitzt.*

Beweis. Sei p irreduzibel über $K \Rightarrow \langle p\rangle = pK[X]$ ist maximales Ideal in $K[X] =: R$
$\Rightarrow L = R/\langle p\rangle$ ist ein Körper. Sei $\pi : R \to L$ der kanonische Homomorphismus und $\hat{\pi} = \pi/K : K \to L$.
Zeigen, dass $\hat{\pi}$ injektiv ist:
Sei $ker(\hat{\pi}) \neq \{0\}$. Da $\hat{\pi}$ ein Homomorphismus ist, ist $ker(\hat{\pi})$ ein Ideal im Körper K (Übung $7/3$)
$\Rightarrow ker(\hat{\pi}) = K \Rightarrow \hat{\pi}(\mathbf{1}) = \overline{0} \in L \Rightarrow \pi(\mathbf{1}) = \overline{0}$
Da $ker(\pi) = \langle p\rangle$ folgt, dass $\mathbf{1} \in \langle p\rangle \overset{\text{Ü.7/3}}{\Rightarrow} K[X] = \langle p\rangle \Rightarrow p =$constant
Dies ist ein Widerspruch zur Irreduzibilität von $p \Rightarrow ker(\hat{\pi}) = \{0\} \Rightarrow \hat{\pi}$ ist injektiv

Wir können nun die Elemente von K und von $\hat{\pi}(K)$ identifizieren, d.h. $K \ni k \Leftrightarrow \hat{\pi}(k) \in \hat{\pi}(K) \subset L$
$\Rightarrow K$ ist als Teilkörper von L zu interpretieren $\Rightarrow L : K$ ist eine Körpererweiterung
Sei $a : \overline{X} \in L$ (Restklasse des Polynoms $f = X$)
Für

$$p = \sum_{i=0}^{r} k_i X^i \Rightarrow p(a) = \sum_{i=0}^{r} k_i (X + \langle p\rangle)^i$$
$$= \sum_{i=0}^{r} k_i X^i + \langle p\rangle = p + \langle p\rangle = \langle p\rangle = \overline{0}$$
$$\Rightarrow a \in L \text{ ist eine Nullstelle von } p$$

Da p irreduzibel ist, ist p das Minimal-Polynom von a über K.
Nach Satz $(4.4 - 12/13)$ ist $L = K(a)$ und $[L : K] = deg(p)$ □

Folgerung 5.2.2. *Ist K ein Körper und $f \in K[X]/K$, dann gibt es einen Erweiterung $L : K$ mit $[L : K] \leq deg(f)$ und f hat in L Nullstellen.*

Beispiel 5.2.3.

$$p = \sum_{i=1}^{n} X^i \in \mathbb{Q}[X] \textit{ irreduzibel}$$
$$L = \mathbb{Q}[X]/\langle p\rangle, \quad [L : \mathbb{Q}] = 4 \qquad \overline{\mathbf{1}}, \overline{X}, \overline{X^2}, \overline{X^3}$$

Beweis.

$$p = (X - \overline{X})(X - \overline{X^2})(X - \overline{X^3})(X - \overline{X^4}) \text{ (nachrechnen)}$$

□

Definition 5.2.4. *Sei K ein Körper und das Polynom $f \in K[X]/K$. Die Körpererweiterung $L : K$ (und damit L) heißt Zerfällungskörper von f, wenn gilt:*

1. *es existieren $a_1, \ldots, a_r$, $c \in K$:*

$$f = c \prod_{i=1}^{r} (X - a_i)$$

2. *$L = K(a_1, \ldots, a_r)$*

Bemerkung 5.2.5. *a)*

1) bedeutet : f zerfällt über L in Linearfaktoren, d.h. alle Nullstellen (Wurzeln) von f liegen in L.

2) bedeutet : L ist minimal mit dieser Eigenschaft 1)

b) Die Elemente $a_1, \ldots, a_r$ sind algebraisch über K und damit ist $[L : K] = [K(a_1, \ldots, a_r) : K] < \infty$

Beispiel 5.2.6. *1. $\mathbb{Q}(\sqrt{2})$ ist der Zerfällungskörper von $f = X^2 - 2$,*
denn $f = (X - 2)(X + 2)$, $\quad \pm\sqrt{2} \in \mathbb{Q}(\sqrt{2})$, $\quad \mathbb{Q}(-\sqrt{2}, \sqrt{2}) = \mathbb{Q}(\sqrt{2})$

2. *Das Polynom $X^4 - 2X^3 - 3X^2 + 4X + 2 = (X \pm \sqrt{2})(X - (1 \pm \sqrt{2}))$ hat auch $\mathbb{Q}(\sqrt{2})$ als Zerfallskörper.*

3. *Das Polynom $(X^2 - 1)(X^2 + 1)$ hat in $\mathbb{Q}(\sqrt{2})$ eine Nullstelle aber zerfällt nicht in Linearfaktoren, sondern in $\mathbb{Q}(\sqrt{2}, i)$*

4. *Sei L ein Zerfällungskörper von $f \in K[X]$ über K und M ein Zwischenkörper von $L : K$, so ist L auch Zerfällungskörper von f über M.*

5. *Sei $L : K$ ein Zerfällungskörper von $f \in K[X]$ mit $f = c \prod_{i=1}^{r} (X - a_i)$, $L = K(a_1, \ldots, a_r)$. Sei nun $a \in N$ mit $N \supset L \supset K$.*
Wir betrachten $f \in K[X] \Rightarrow f$ zerfällt über $L(a)$ in Linearfaktoren (wie oben) mit $L(a) = K(a_1, \ldots, a_r)(a) = K(a)(a_1, \ldots, a_r) \Rightarrow L(a)$ ist Zerfällungskörper von f über $K(a)$.

5.3 Kreisteilung

Definition 5.3.1. *Sei K ein Körper. Der Durchschnitt aller Teilkörper von K heißt Primkörper von K.*

Definition 5.3.2. *Sei K ein Körper, P ein Primkörper von K und $n \in \mathbb{N}/\{0\}$.*
Jede Wurzel des Polynoms $X^n - 1 \in P[X]$ heißt $n-te$ Einheitswurzel über K.
Der Zerfällungskörper $P_n : P$ dieses Polynoms heißt $n-ter$ Kreisteilungskörper über P.

Bemerkung 5.3.3. *1. Jede Einheitswurzel ist algebraisch über einen Primkörper P zu K.*

2. *Sei $E_n : E_n(P)$ die Menge der n-ten Einheitswurzeln über P im Kreisteilungskörper P_n, dann gilt:*

   (a) $|E_n| \leq n$

   (b) $E_n \subseteq E_{nm} \qquad (n, m \neq 0)$

   (c) $E_m \subset E_n$ *für alle positiven Teiler* m *von* n

   (d) Aus $m \mid n \Rightarrow P_m \subset P_n$

Definition 5.3.4. *Sei K ein Körper. Für $n \geq 1$ und $\mathbf{1} \in K$ sei*

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

Die Zahl

$$Char(K) := \begin{cases} 0 & , \text{ wenn } \quad n\mathbf{1} \neq 0 \text{ für alle } n \geq 1 \\ min\{n \geq 1 : n\mathbf{1} = 0\} & , \text{ wenn } \quad n \in \mathbb{N} \text{ existiert, mit } n\mathbf{1} = 0 \end{cases}$$

heißt Charakteristik von K.
Man kann zeigen:

(a) Wenn $Char(K) \neq 0$, dann ist $Char(K) = p^2$, mit p, einer Primzahl.

(b) Wenn $P \subseteq K$ ein Primkörper von K ist, dann gilt:

$$Char(K) = Char(P)$$

Satz 5.3.5. *Es gilt:*

(a) E_n ist eine zyklische Untergruppe von $P_n^* = (P_n/\{0\}, \cdot)$

(b) Ist $Char(P) = p \neq 0$, so ist $E_n = E_{np}$ für alle $n \geq 1$

(c) Wenn $Char(P) = 0$ ist, oder dieser kein Teiler von n, so ist $|E_n| = n$

Beweis. zu (a) : Seien $a, b \in E_n$, d.h. $a^n = 1 = b^n$.
$(a \cdot b^{-1})^n = a^n \cdot (b^{-1})^n = \mathbf{1} \cdot \mathbf{1} = \mathbf{1}$
$\Rightarrow (ab^{-1}) \in E_n \Rightarrow E_n \leq P_n^*$
Da E_n endlich ist, ist E_n zyklisch.

zu (b) : Sei $Char(K) = Char(P) = p \neq 0$

$$(a^n - 1)^p = \sum_{k=0}^{p} \binom{p}{k} (a^n)^k (-1)^{p-k} = a^{np} - 1 + \underbrace{\sum_{k=0}^{p-1} p \cdot l(a^n)^k}_{=0}$$

$\Rightarrow a^n - 1 = 0 \Leftrightarrow a^{np} - 1 = 0$
$\Rightarrow$ Behauptung

zu (c) : Ist $Char(K) = 0$ oder $p \nmid n$ mit $Char(K) = p \Rightarrow X^n - 1$ besitzt nur einfache Wurzeln in K.

□

Generell gilt nun: Sei $Char(P) = p \neq 0$ und $n \in \mathbb{N}$ so gewählt, dass $p \nmid n$ ist.

Satz 5.3.6. *Mit dieser Voraussetzung $p \nmid n$ ist E_n eine zyklische Gruppe.*
Jedes erzeugende Element $\xi \in E_n$ der Gruppe E_n heißt dann primitive Einheitswurzel, d.h. $E_n = \{\mathbf{1}, \xi, \xi^2, \ldots, \xi^{n-1}\}$.

Satz 5.3.7. *Für jede primitive $n-te$ Einheitswurzel $\xi \in E_n$ gilt:*

$$P_n = P(\xi)$$

Satz 5.3.8. *Für $F_n : \{\xi \in E_n : E_n = \langle \xi \rangle\}$ gilt:*

$$|F_n| = \varphi_n \qquad \textit{Eulersche } \varphi - \textit{Funktion}$$

Satz 5.3.9. *Es gilt:*

(a) $F_n \cap F_m = \emptyset$ *für alle* $n \neq m$

(b) $E_n = \bigcup_{d|n} F_d \qquad (d > 0)$

Beweis. zu (a) : $\xi \in F_n \cap F_m \Rightarrow n = |\langle \xi \rangle| = m \Rightarrow m = n$ Widerspruch zu $n \neq m$

zu (b) : Sei $n = dm \overset{Bem.:(5.3-3(2c))}{\Longrightarrow} E_d \subseteq E_n$
$\Rightarrow F_d \subseteq E_n \Rightarrow \bigcup_{d|n} F_d \subset E_n$ mit $d > 0$
Sei ξ n-te primitive Einheitswurzel, d.h. $E_n = \langle \xi \rangle$.
Für $a \in E_n$ gilt:

Es existiert ein k mit $a = \xi^k$

$\Rightarrow ord(a) = ord(\xi^k) = \frac{n}{\text{ggT}\,(n,k)} := d$
$\Rightarrow a^d = \mathbf{1} \Rightarrow a$ ist d-te Einheitswurzel
$\Rightarrow a \in E_d$, da $ord(a) = d \Rightarrow \langle a \rangle = E_d$
$\Rightarrow a \in F_d \Rightarrow E_n \subseteq \bigcup_{d|n} F_d$ für $d > 0$.
$\Rightarrow$ Behauptung

□

Folgerung 5.3.10. *Es gilt:*

$$n = \sum_{d|n} \varphi(d) \qquad (d > 0)$$

Bemerkung 5.3.11. *Sei $F_n = \{\xi_1, \ldots, \xi_{\varphi(n)}\}$, dann gilt:*

(a) $E_n = \langle \xi_i \rangle$ *für alle* $i = 1, \ldots, \varphi(n)$.

(b) Für fixe $\xi \in F_n$ *ist*

$$F_n = \{\xi^k : ggT(k,n) = 1, 1 \leq k \leq n\}$$

Definition 5.3.12. *Das Polynom*

$$\Phi_n = \prod_{i=1}^{\varphi(n)} (X - \xi_i) = \prod_{\xi \in F_n} (X - \xi_i)$$

heißt das n-te Kreisteilungspolynom über P.

Satz 5.3.13. *Es gilt:*

$$X^n - 1 = \prod_{d|n} \Phi_d(X) \qquad (d > 0)$$

Beweis. Da P_n ein Zerfällungskörper von $X^n - 1$ ist, d.h. $X^n - 1$ zerfällt in P_n in Linearfaktoren, d.h. $X^n - q = \prod_{\xi \in E_n} (X - \xi)$.
Nun ist $E_n = \bigcup_{d|n} F_d \qquad (d > 0)$
$\Rightarrow X^n - 1 = \prod_{d|n} (\prod_{\xi \in E_n} (X - \xi)) = \prod_{d|n} \Phi_d(X) \qquad (d > 0)$ □

Folgerung 5.3.14. *Für jede Primzahl p gilt:*

$$\Phi_p(X) = \sum_{n=0}^{p-1} X^n$$

Beweis.

$$\Phi_1(X) = X - 1$$
$$X^p - 1 = \Phi_1(X) \cdot \Phi_p(X)$$
$$\Rightarrow \Phi_p(X) = \frac{X^p - 1}{X - 1}$$

□

Beispiel 5.3.15. *Berechnung von* Φ_6*:*

$$\begin{aligned} X^6 - 1 &= \Phi_1 \cdot \Phi_2 \cdot \Phi_3 \cdot \Phi_6 \\ &= (X-1)(X+1)(X^2+X+1)\Phi_6 \\ \Phi_6 &= X^2 - X + 1 \end{aligned}$$

Satz 5.3.16. *Für jedes* $n \geq 1$ *gilt:* $\Phi_n \in P[X]$*. Im Fall* $P = \mathbb{Q}$ *ist* $\mathbb{Q} \in \mathbb{Z}[X]$*.*

Beweis. Induktion nach n

IA.: $n = 1, \Phi_1 = X - 1 \in P[X] \quad (\in \mathbb{Z}[X])$

IV.: $\Phi_k \in P[X] \quad (\in \mathbb{Z}[X])$ für alle $k < n$

IB.: Für $g := \prod_{d|n} \Phi_d \in P[X] \quad (\in \mathbb{Z}[X]) \quad (0 < d < n)$
Da g normiert ist, folgt nach dem Satz über die "Division mit Rest":
Es existieren genau ein $q, r \in P[X] : X^n - 1 = qg + r \quad (*)$, wobei $r = 0$ oder $deg(r) < deg(g)$ ist.
Da $P \subset P_n \quad (\mathbb{Z} \subset \mathbb{Q} \subset P_n)$, ist auch $(*)$ eine Zerlegung über $P_n[X]$.
Nach Satz $(5.3 - 13)$ ist aber dort $X^n - 1 = g \cdot \Phi_n \Rightarrow r = 0, q = \Phi_n \Rightarrow \Phi_n \in P[X]$ $(\in \mathbb{Z}[X])$.

□

Bemerkung 5.3.17. *Sei* R *der Integritätsbereich (mit* $\mathbf{1}$*) und*

$$f = \sum_{i=1}^{n} a_i X^i, \text{ sowie } f' = \sum_{i=1}^{n} i a_i X^{i-1}$$

Dann gilt: Aus $u, f \in R[X]$ *mit* $u^2 \mid f \Rightarrow u \mid f'$
(klar: $f' = (u^2 v)' = (u(uv))' = u'(uv) + u(uv)' = u((uv) + (uv)')$*)*

Satz 5.3.18. *Für jedes* $n \geq 1$ *ist* Φ_n *über* $\mathbb{Q}$ *irreduzibel.*

Bemerkung 5.3.19. *Der Satz wird für den Fall* $Char(\mathcal{P}) \neq 0$ *falsch, z.B. über* $\mathbb{Z}_5 = \mathbb{F}_5$ *ist*

$$\Phi_{1,2} = X^4 - X^2 + 1 = (X^2 - 2X - 1)(X^2 + 2X - 1)$$

Folgerung 5.3.20.

1. Φ_n *ist das Minimalpolynom jeder primitiven* $n - ten$ *Einheitswurzel* $\xi \in \mathbb{F}_n$ *über* $\mathbb{Q}$

2. *Der Grad der Körpererweiterung* $[\mathbb{Q}(\xi) : \mathbb{Q}] = \varphi(n)$ *für alle* $\xi \in \mathbb{F}_n$ *(für* $\mathcal{P} = \mathbb{Q}$*)*

Definition 5.3.21. *Eine ungerade Primzahl* p *heißt Fermat'sche Primzahl, wenn ein* $m \in \mathbb{N}$ *existiert mit* $p = 2^m + 1$.

(Man zeigt: $p = 2^m + 1$ *ist eine Fermat'sche Primzahl, wenn* $m = 2^k \quad (k \geq 0)$*)*

Beispiel:

$$2^1 + 1 = 3, \quad 2^2 + 1 = 5, \quad 2^4 + 1 = 17, \quad 2^8 + 1 = 257$$
$$2^16 + 1 = 65537, \quad 2^{32} + 1 = 4.294.967.297 = 641 \cdot 67.004.117$$

Wenn p *eine Primzahl mit* $p < 10^{40000}$ *ist, so ist* p *eine Fermat'sche Primzahl, wenn* $p \in \{3, 5, 17, 257, 65537\}$

Satz 5.3.22 (Gauß). *Ein regelmäßiges* n*-Eck ist genau dann mit Zirkel und Lineal konstruierbar, wenn* n *von der Form*

$$n = 2^k p_1 \cdot p_2 \cdot \ldots \cdot p_r \quad (k \geq 0),$$

wobei die p_i *paarweise verschiedene Fermat'sche Primzahlen sind.*

Beweis.

Notwendigkeit: Sei ein n-Eck konstruierbar $\Leftrightarrow$ die n-te prime Einheitswurzel ξ ist konstruierbar.
Sei $\xi \in \mathbb{F}_n$ konstruierbar $\Leftrightarrow \xi \in \mathcal{P} \Rightarrow$ Grad des Minimalpolynoms zu ξ ist eine 2er-Potenz.
$\Rightarrow \varphi(n) = deg\Phi_n = 2^\alpha \quad (\alpha \geq 0)$
Sei $n = 2^k p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_r^{k_r}$ die Primfaktorzerlegung zu $n \quad (p_i \neq p_j, \quad i \neq j)$.

Nun gilt: $\varphi(n) = \varphi(2^k)\varphi(p_1^{k_1}) \cdot \ldots \cdot \varphi(p_r^{k_r})$
(Mit p eine Primzahl $\Rightarrow \varphi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1)$)
$\Rightarrow 2^\alpha = \varphi(n) = 2^{k-1} \prod_{i=1}^r p_i^{k_i - 1}(p_i - 1)$
Wäre z.B. $k_1 - 1 \neq 0 \Rightarrow p_1 \mid 2$
Dies ist ein Widerspruch zu $p_1 > 2$ prim
$\Rightarrow k_i - 1 = 0$ für alle $i = 1, \ldots, r$
$\Rightarrow 2^\alpha = 2^{k-1} \prod_{i=1}^r (p_i - 1) \Rightarrow p_i - 1 = 2^{l_i} \quad (i = 1, \ldots, r)$
$\Rightarrow p_i = 2^{l_i} + 1 \Rightarrow p_i$ ist eine Fermat'sche Primzahl und

$$n = 2^k p_1 p_2 \cdots p_r$$

□

Beispiel 5.3.23.

(a) *konstruierbar sind* $2^k \cdot 5, \quad 2^k \cdot 17$

(b) *nicht konstruierbar sind* $7, 9, 11, \ldots, 19$