

Benjamin Hill, zunächst Thomas Kahle (3x VL, 1x Ü)

Übungsbücher auf Homepage der Veranstaltung; verlinkt unter

"Teaching" / Thomas Kahle (ab morgen)

→ Übungsbücher in der ersten Übung abgeben ~~(12. April)~~ (12. April)

## Inhalt

### 1.1 Grundlagen von Halbgruppen zu Gruppen

Algebra ist Abstraktion von Strukturen wie z.B. -Mengen  $X, Y, Z$ ,

- Relationen, z.B. Äquivalenzrelationen  $\rightarrow \begin{cases} (x, x) \in R \\ (x, y) \in R \Rightarrow (y, x) \in R \\ (x, y) \in R \text{ und} \\ (y, z) \in R \Rightarrow (x, z) \in R \end{cases}$   
Allgemein:  $R \subseteq X \times X$
- Abbildungen:  $f: X \rightarrow Y$   
Abbildungen definieren Äquivalenzrelationen  
(weil Elemente werden auf derselben  
Abbildung abgebildet)  
V.a.:  $x_1 \sim_f x_2 (\Rightarrow f(x_1) = f(x_2) \quad \forall x_1, x_2 \in X)$

gilt Relativsymbol "in der Mitte":  
 $x \sim y (\Leftrightarrow (x, y) \in R)$

Jede Äquivalenzrelation ist von dieser Form: (Also: Es gibt eine passende Abbildung.)

Sei  $\sim$  eine Äquivalenzrelation auf  $X$ . ~~Die Äquivalenzklasse~~ eines ~~ist~~

$x \in X$  ist definiert als  $A_x := \{x' \in X \mid x' \sim x\}$

Die Menge aller Äquivalenzklassen wird mit  $X/\sim$  bezeichnet.

Wir haben eine kanonische Abbildung  $\pi: X \rightarrow X/\sim$   
(Projektion)  $x \mapsto A_x$

Jede Abbildung kann mit Hilfe dieser Konstruktion in "natürliche Teile" zerlegt werden: Sei  $f: X \rightarrow Y$  beliebig. ~~Betrachte~~  $X \xrightarrow{f_1} X/\sim \xrightarrow{f_2} f(X) \xrightarrow{f_3} Y$

~~Betrachte~~ wobei  $f_1$  die kanonische Projektion  
 $f_2$  die Abbildung der Äquivalenzklasse mit  $f$   
 $f_3$  Inklusion von  $f(X) \subseteq Y$ .

Bild von  $f$   
( $\subseteq Y$ )

Genauso:  $X \xrightarrow{f_1} X/\sim \xrightarrow{f_2} f(X) \xrightarrow{f_3} Y$

$X \xrightarrow{f_1} A_x \xrightarrow{f_2} f(x) \xrightarrow{f_3} f(x)$   
ist eindeutig  
bijektiv

$f_1$ : surjektiv  
 $f_2$ : bijektiv  
 $f_3$ : injektiv  
(nach oben)

Def.: Die Zerlegung  $f = f_3 \circ f_2 \circ f_1$  heißt kanonische Zerlegung von  $f$ .  
(erleicht die Frage, ob  $f$  injektiv ist.)

$\uparrow$  (Faktorisierung)

enthält absolute Grundbegriffe

Bemerkung: In der abstrakten Algebra nutzen wir gerne Diagramme, um

Verzweigungen von Abbildungen zu visualisieren:

Man sagt: ein Diagramm kommutiert,

falls jede Komposition entlang geschweifter

Pfeile zwischen den gleichen Mengen die gleiche Abbildung ergibt.

Nun zu algebraischen Strukturen auf Mengen und Abbildungen.

Sie kennen Gruppen, Ringe, Körper, Vektorräume, Modelle.

Wir definieren hier mit Halbgruppen, die "entstehen", falls man

in der Definition einer Gruppe Inverse und das Neutralelement weglässt.

Def.: Eine Halbgruppe  $H$  ist eine Menge zusammen mit einer assoziativen Verknüpfung  $\circ$  auf  $H$ . D.h.

$$\circ : H \times H \rightarrow H \quad \text{mit} \quad (g \circ h) \circ k = g \circ (h \circ k) \quad \forall g, h, k \in H.$$

Bemerkung: Der Punkt  $\circ$  wird gerne weggelassen, d.h.  $g(hk) = (gh)k$  usw.

- Es gibt auch die additive Notation mit " $+$ " als Operation.

- In multiplikativer Notation schreibt man auch:  $\overbrace{h \cdots h}^n := h \cdot h \cdot \dots \cdot h$ ,  $n \in \mathbb{N}$   
- additiv:  $\underbrace{n h}_{n\text{-mal}} = \underbrace{h + h + \dots + h}_{n\text{-mal}}$  ( $n \neq 0$ )

Definition: Sei  $(H, \circ)$  eine Halbgruppe.

- neutrales Element  
ist, falls existet,  
einzig  
(wurde es  $e_1, e_2$ ,  
wenn es  $\neq e_2$ ?)} }  
a) Die Ordnung von  $H$  ist  $|H|$  (die Kardinalität der Menge)  
b)  $H$  ist abelsch (bzw. Kommutativ), falls gilt:  $gh = hg \quad \forall g, h \in H$ .  
c) Ein  $e \in H$  heißt neutrales Element von  $H$ , falls  $e \circ h = h \circ e = h$  gilt.  
d)  $H$  heißt Monoid, falls  $H$  ein neutrales Element besitzt.

Bemerkung: Neutrale Elemente werden gerne mit " $1$ " in multiplikativer und " $0$ " in additiver Notation bezeichnet.

Beispiele:

1) Für jede Menge  $X$  ist  $T_X := \{ f: X \rightarrow X \}$  ein Monoid (mit  $\circ$ ).  
Halbgruppe, da  $\circ$  assoziativ. (Selbstabbildungen)  
 $\text{id}_X$  ist neutrales Element:  $\text{id}_X: X \rightarrow X$ .

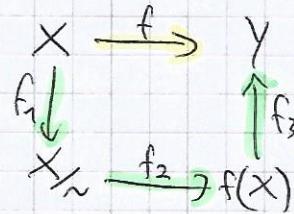
$$x \mapsto x$$

2)  $\{0, 1, 2, \dots\}$  mit  $+$  (wobei  $\infty$  jeden Überlauf absorbiert,  $\infty$  absonderndes Element kann es in einer Gruppe nicht geben) ist ein Monoid (Körper der rationalen Zahlen,  $\mathbb{Q}$ ).

3)  $\{0, 1, 2, 3\}$  mit  $+$  und der Verkürzung  $4=1, 5=2, \dots$  ist kein Monoid. ( $\notin \text{Modul}\Omega$ )  $\{1, 2, 3\}$  ist eine Untergruppe, die ein anderes neutrales Element (nämlich 3) besitzt ( $x+3=x$ ).

Viele Erstaufen über Gruppen gelten schon in Monoiden, z.B.

Lemma: Jedes Monoid hat genau ein Neutralelement.



Beweis: falls  $e, e'$  neutral:  $e = e \cdot e' = e'$ .  $\square$

Auch für Halbgruppen kann man eine Verknüpfungstafel aufstellen:

$h_1$	$h_2$	$\dots$	Elemente von Halbgruppe in fixierter Nummerierung
$h_1$	$h_1 h_1$	$h_1 h_2$	$\dots$
$h_2$	$h_2 h_1$	$h_2 h_2$	$\dots$
$\vdots$	$\vdots$	$\ddots$	Halbgruppen haben Unterhalbgruppen, d.h. Teilmengen, die unter der induzierten Operation wieder Halbgruppen sind.

Ein Untermonoid ist eine Unterhalbgruppe, die neutrales Element  $\xrightarrow{\text{des neutr. El. des Monoids}}$

eine Untergruppe einer Halbgruppe ist eine Teilmenge, die eine Gruppe bildet. (Hier ist ein anderes Neutralelement möglich, siehe Beispiel).

Definition: Sei  $(M, \cdot)$  ein Monoid. Ein Element  $a \in M$  heißt invertierbar, falls ein  $b \in M$  existiert mit  $ab = ba = e$  (ist Neutrallement). Einheit

Tablet: Ein solches  $b$  ist eindeutig, denn falls  $b'$  auch  $ab' = b'a = e$  erfüllt, gilt:  $b = be = b'(ab') = (ba)b' = eb' = b'$ .  $\square$

Daher ist die Notation  $a^{-1}$  respektive  $-a$  für das Inverse von  $a$  gebräuchlich.

Achsenp. Aus der Existenz eines  $b$  mit  $ab = e$  (falls es existiert) folgt zweit  $ba = e$  für dieses  $b$  ( $ab = e$  und  $ba = e$  müssen beide gelten!).

Ein Element  $b$ , das  $\frac{ab}{ba} = \frac{e}{e} = 1$  erfüllt, heißt Rechts-Inverses von  $a$ .

Beispiel:  $T_X =$  Monoid der Abbildungen  $X \rightarrow X$ . Einheiten in  $T_X$ : bijektive Abbildungen jede surjektive Abbildung  $f: X \rightarrow X$  hat ein Rechtseinv.  $g: X \rightarrow X$  mit  $\text{id}_X = f \circ g$ . Jede injektive Abb.  $f: X \rightarrow X$  hat ein Linkseinv.  $g: X \rightarrow X$  mit  $\text{id}_X = g \circ f$ .

Konkret:  $f: \mathbb{N} \rightarrow \mathbb{N}$  mit  $g: \mathbb{N} \rightarrow \mathbb{N}$  gilt  $f \circ g = \text{id}_{\mathbb{N}}$ .  
 $k \mapsto \begin{cases} k/2 & \text{falls } k \text{ gerade} \\ 1 & \text{falls } k \text{ ungerade} \end{cases}$   $k \mapsto 2k$

Definition: Die Menge der invertierbaren Elemente eines Monoids  $M$  heißt Einheitsgruppe von  $M$  und wird mit  $U(M) := \{a \in M \mid a \text{ invertierbar}\}$  (eine Unterguppe) mit  $U$  bezeichnet.

Bemerkung:  $M^*, M^\times$  sind auch gebräuchliche Notationen für  $U(M)$ .

Beispiele:  $-(\mathbb{Z}, \circ)$  ist ein Monoid mit Einheitsgruppe  $\{-1, 1\}$ .

- Für jeden Körper gilt:  $U(k) = k \setminus \{0\}$

-  $U(T_X) = S_X$  sind die Permutationen von  $X$  (Permutationsgruppe)

-  $U(\text{Matr. } n \times n) = \text{GL}_n(k)$  ist die allgemeine lineare Gruppe (reguläre  $n \times n$ -Matr.)

Def: Eine Gruppe ist ein Monoid  $G$ , für das gilt:  $U(G) = G$ .

Übung: Prüfen, dass das die bekannte Definition ist.

Proposition: Für jedes Monoid  $M$  ist  $U(M)$  eine Gruppe.

Beweis:  $U(M)$  ist eine Halbgruppe da falls  $a, b$  invertierbar auch  $ab$  invertierbar (Inverses:  $b^{-1}a^{-1}$ );  $ee \in U(M) \Rightarrow$  Monoid.  $U(U(M)) = U(M)$ , da falls  $a$  invertierbar mit Inversem  $a^{-1}$ , dann ist  $a^{-1}$  invertierbar mit Inversem  $a$ .

(www.math.orgu.de / Algebra.html)

Def. Sei  $G$  eine Gruppe und  $x \in G$ . Die Ordnung von  $x$  ist die kleinste positive ganze Zahl  $n$  s.d. gilt  $x^n = 1$ , falls eine solche Zahl existiert und  $+ \infty$  andernfalls. (Wir schreiben  $|x|$  für die Ordnung von  $x$ ).  $\left( \begin{array}{l} x^n : \underbrace{x \cdot x \cdot \dots \cdot x}_{n-\text{Mal}} \\ |x| \text{ neutr. El. in } G \end{array} \right)$

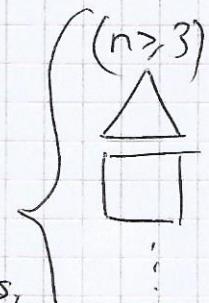
## 1.2 Diedergruppen

Eine wichtige Klasse von Gruppen sind Symmetriegruppen von geometrischen Objekten. Ihre Elemente sind Transformationen, die ein geometrisches Objekt (als Ganzes) in sich selbst überführen.

Wir betrachten hier exemplarisch das reguläre  $n$ -Eck in der Ebene. (Winkel jeweils an jeder Ecke gleich)

Bezeichne mit  $D_{2n}$  die Menge der Symmetrioperatoren des regulären  $n$ -Ecks, d.h. Operationen, die man mit einem  $n$ -Eck aus Holz in 3D ausführen kann, s.d. es danach wieder deckungsgleich zu liegen kommt.

Diese Vorschrift bedeutet insbesondere, dass Ecken auf Ecken zu liegen kommen. Seien dazu die Ecken konsekutiv mit  $1, \dots, n$  nummeriert.  
 $\Rightarrow$  Jede Symmetrie gibt eine Bijektion  $\{1, \dots, n\}$  (eine Permutation).



(\*) Bsp.: Drehung um den Winkel  $\frac{2\pi}{n}$  gibt die Bijektion  $i \mapsto i+1$  (Konvention  $n+1=1$ )

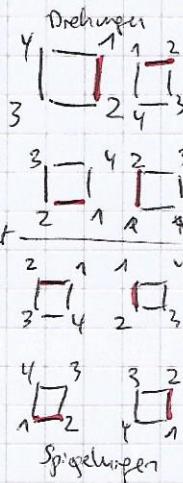
$D_{2n}$  ist eine Gruppe mit Komposition als Operation: assoziativ als Funktionskomposition, die Identität (totale Symmetrie) ist das neutrale Element. Inverse sind klar (Symmetrie rückgängig machen).

Behauptung:  $|D_{2n}| = 2n$ . Dazu: Jede Symmetrioperation ist durch das Bild des Paares (der Kante)  $1-2$  festgelegt, da  $1-2$  benachbart bleiben und das restliche  $n$ -Eck starr an der Kante ist.

Worauf kann also die Kante  $1-2$  abgebildet werden?

Die Kante  $1-2$  kann auf jede beliebige andere Ecke abgebildet werden. Die 2 handelt auf einer benachbarten Ecke; beide sind möglich. Eine Seite ist automatisch durch vorherige Drehung, die andere Möglichkeit kann durch Spiegelung an der Achse durch das Bild von 1 und den Ursprung / Schwerpunkt erledigt werden.

$2n$  mögliche Symmetrien gefunden. Da dies alle Möglichkeiten für das Bild von  $1-2$  sind, gilt  $|D_{2n}| = 2n$ .



Bsp.:  $n=4$  4 Drehungen ( $0^\circ, 90^\circ, 180^\circ, 270^\circ$ ) 4 Spiegelungen  
  
 Dies sind alle Symmetrien des Quadrates.

Wir schreiben jetzt  $D_{2n}$  als abstrakte Gruppe. (Dann können wir ohne die unterliegende Geometrie argumentieren).

Sei ein  $n$ -Eck fixiert. Bezeichne mit  $r$  die Drehung/Rotation um  $\frac{2\pi}{n}$ ,  $s$  die Spiegelung an der Achse durch 1 und den Ursprung.

Behauptungen über  $r$  und  $s$ : (1)  $1, r, r^2, \dots, r^{n-1}$  sind alle verschiedenen und  $r^n = 1$   
 (2)  $|s| = 2$  (doppelte Spiegelung macht nichts)  $((|r| = n))$   
 (3)  $s \neq r^i$  (keine Rotation ergibt die Spiegelung) für jedes  $i$   
 (denn  $s$  ändert die Orientierung)

(4)  $s r^i \neq s r^j$  für  $i, j \in \{0, \dots, n-1\}$  ( $i, j$  mal ablesen und dann spiegeln)

Beweis: Wende  $s$  auf (1) an.

Insgesamt haben wir schon  $2n$  Elemente gefunden:  $D_{2n} = \{1, r, \dots, r^{n-1}, s, sr, \dots, sr^{n-1}\}$

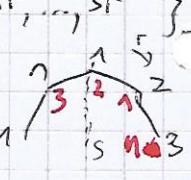
(5)  $r s = s r^{-1}$  Beweis: Betrachte, was beide Seiten mit  $1 \cdot 2$  machen.

(6)  $r^i s = s r^{-i}$  per Induktion

Mit diesen "Regeln" kann jedes Produkt in  $D_{2n}$  sortiert werden.

Konvention: alle  $r$  nach rechts sortieren mittels (5); mit (6)

überflüssige  $r, s$  eliminieren ( $r^2 = 1, r^n = 1$ ).



Bsp. in  $D_{24}$  für  $n=12$ :  $(sr^9)(sr^6) = ssr^{-9}r^6 = r^{-9}r^6 = r^{-3} = r^9$   
assoziativ, (5)

Wir haben nun  $D_{2n}$  beschrieben durch die Angabe von Erzeugern ( $r, s$ ), d.h. Elementen, s.d. sich jedes  $x \in D_{2n}$  als Produkt dieser Elemente ausdrücken lässt.

Dazu haben wir Relationen, die bestimmen, welche Produkte der Erzeuger gleich sind. Damit kann effizient in der Gruppe gerechnet werden.

Für Gruppen, bei denen endlich viele Erzeuger und Relationen genügen, kann damit die Gruppe kommuniziert werden. Man sagt: Erzeuger und Relationen bilden eine Präsentation der Gruppe. (Falls endlich, "endlich präsentiert").

alles kann man mit  $S$  schreiben

Im Allgemeinen falls eine Teilmenge  $S \subseteq G$  einer Gruppe  $G$  diese erzeugt schreiben wir  $G = \langle S \rangle$ . Falls  $R_1, \dots, R_m$  Relationen sind (also Gleichungen in Produkten aus  $S$  und 1) s.d. jede gültige Relation in  $G$  daraus folgt, so schreiben wir  $G = \langle S | R_1, \dots, R_m \rangle$ .

Präsentationen vereinfachen die Arbeit mit Gruppen, aber gewisse Eigenschaften sind aus ihnen nicht leicht abzulesen:

- Bsp.:
- Sind 2 Produkte von Elementen aus  $S$  die gleichen Elemente in  $G$ ?  $\leftarrow$  Witzig, obwohl
  - Was ist die Ordnung der Gruppe?
  - Ist die Gruppe endlich?

in der theoretischen Informatik

Bsp.:  $G = \langle x, y \mid x^2 = y^2 = (xy)^2 = 1 \rangle$ . Was ist  $|G|$ ? Beweisung:  $|G| = 4$ , nämlich  $G = \{1, x, y, xy\}$ .

Z.B.  $yx? \quad xy \cdot y = 1 \Rightarrow xy = y^{-1}x^{-1} = yx$  und auch  $x = x^{-1}, y = y^{-1}$   
 $\Rightarrow G$  ist abelsch  $\Rightarrow$  Sortieralgorithmus (x nach links, y nach rechts) liefert die Beweisung

aber:

$G' = \langle x, y \mid x^3 = y^3 = (xy)^3 = 1 \rangle$  ist unendlich, denn

$xyx, xyxxyx, xyxxyxxyx, \dots, (xyx)^n$  sind alle verschieden  
(da die Relationen nicht aufgeweckt werden können), also  $G$  unendlich

obere Schranke für  $|X_{2n}|$ :

Ein weiteres Problem sind verdeckte Relationen:  $X_{2n} = \langle X, Y \mid x^n = 1, y^n = 1, xy = yx^2 \rangle$   
Die Relation  $xy = yx^2$  erlaubt, Produkte zu sortieren.  
 $x^n = 1$  und  $y^n = 1$  erlauben zu reduzieren, analog zu  $D_{2n}$ . Frage: Ist  $|X_{2n}| = 2n$ ? Nein. Jedes Element kann als  $y^k x^l$  mit  $k \leq 1$  ( $k \leq n-1$ ) geschrieben werden, also  $|X_{2n}| \leq 2n$ . Aber:  $x = xy^2 = xyy = yx^2y = yxy = yxyx^2 = yyx^2 = x^4$ . Es gilt (unabhängig von  $n!$ )  $x^4 = x$ . Also dann  $l \leq 3 \Rightarrow |X_{2n}| \leq 6$ . (?)

Zusammen: Präsentationen sind ein wichtiges Werkzeug der Gruppentheorie, erlauben aber manchmal keine leichten Antworten auf leidliche Fragen.



4  $x^l$  können zu  $x$  vereinfacht werden, also

(höchstens)  $|X_{2n}| = \{1, x, xx, xxx, y, yx, yxx, yxxx\}$

damit Höchstas  $(X_{2n}) \leq 8$  (?) (nicht 6?)

### 1.3 Die symmetrische Gruppe

Sei  $\Omega$  eine Menge.  $S_\Omega$  bezeichnet die Permutationen von  $\Omega$ , d.h. bijektive Abbildungen  $\Omega \rightarrow \Omega$ .  $S_\Omega$  ist eine Gruppe unter Komposition. Sie heißt symmetrische Gruppe auf  $\Omega$ . Sie ist in gewissen Sinn universell für alle Gruppen, z.B. ist jede abzählbare Gruppe eine Untergruppe der  $S_{\mathbb{N}}$ . Falls  $\Omega = \{1, \dots, n\}$ , schreibt man  $S_n = S_{\{1, \dots, n\}}$ . Jede endliche Gruppe ist Untergruppe einer  $S_n$ .

Fakt:  $|S_n| = n! = n \cdot (n-1) \cdot (n-2) \cdots 2 \cdot 1$

Grund: Bijektionen sind injektiv, d.h. dass die Bilder von  $\{1, \dots, n\}$  bestimmt.

Für das Bild der 1 besteht  $n$  Möglichkeiten. Für das Bild der 2 dann wg. Injektivität  $n-1$  Möglichkeiten usw.

Schreibweisen für Elemente der  $S_n$ : Sei  $\sigma \in S_n$ .

1) Abbildungspaare  $(i, \sigma(i))$ , zweidige Notation:  $\begin{pmatrix} 1 & 2 & 3 & \dots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & & \sigma(n) \end{pmatrix}$

einzelige Notation:  $(\sigma(1) \ \sigma(2) \ \dots \ \sigma(n))$

2) Zyklendarstellung:

Def: Ein Zykel ist eine Permutation  $a_1 \xrightarrow{\sigma} a_2, a_2 \xrightarrow{\sigma} a_3, \dots, a_n \xrightarrow{\sigma} a_1$ , d.h.  $\sigma(a_1) = a_2, \dots, \sigma(a_n) = a_1$ , wobei gilt  $\sigma(k) = k$  für alle  $k \in \{1, \dots, n\} \setminus \{a_1, \dots, a_n\}$ .

Bsp: (in  $S_4$ )  $\begin{pmatrix} 1 \mapsto 2 \\ 2 \mapsto 1 \\ 3 \mapsto 4 \\ 4 \mapsto 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$  ist kein Zykel (besteht aus Zykeln).

Ein Zykel wird geschrieben als  $(a_1 \dots a_m)$ . Dies darf nicht mit einziger Notation verwechselt werden. Ein beliebiges  $\sigma \in S_n$  besteht im Allgemeinen aus  $m$  weiteren disjunkten Zykeln. Diese werden in Zyklendarstellung nebeneinander geschrieben:  $\sigma = (a_1 \dots a_m)(a_{m+1} \dots a_{m+2}) \dots (a_{m+1+m} \dots a_{m+2+m})$ , falls  $m \neq n$ , lässt  $\sigma$  einige Elemente fest. Jedes  $x \in \{1, \dots, n\}$  kommt höchstens einmal vor, und auf seinen rechten Nachbarn respektive des entsprechenden Element des Zyklus abgebildet.

Folgender Algorithmus überführt Abbildungsdruck in Zyklendarstellung:

1) Finde das Element  $a$ , welches noch nicht im Ausgabetypel vor kommt, und füge "(a)" zur Angabe hinzu.

2) Finde  $b = \sigma(a)$ . Falls  $b = a$ , schreibe " $a$ " unter  $a$  ansonst schreibe " $a$ " und gehe zu 2) mit  $a = b$ .

Dieser Prozess endet, wenn alle  $x \in \{1, \dots, n\}$  vor kommen.

3) entferne alle Zykel der Länge 1, d.h. Zykel der Form  $(a)$ .

Def. / Konventionen: Die Länge eines Zyklus ist die Anzahl der Elemente im Zykel.

Ein Zykel der Länge  $t$  wird als  $t$ -Zykel bezeichnet. Zwei Zyklen liegen disjunkt, wenn kein  $x \in \{1, \dots, n\}$  in beiden vorkommt. Die Identität wird mit  $1 \in S_n$  bezeichnet.  $(1 \ 2)$  kann als Element jeder  $S_n, n \geq 2$  betrachtet werden.

Bsp.:  $S_3$  hat  $3! = 6$  Elemente:  $S_3 = \{1, (1 \ 2), (2 \ 3), (1 \ 3), (1 \ 2 \ 3), (1 \ 3 \ 2)\}$  (in Zyklendarstellung)

Zum Rechnen mit Zykeln: -Zykel können zyklisch geschrieben werden, d.h.  $(a_1 \dots a_m)$

- Rückwärtslesen gilt die Umkehrabbildung:  $(a_1 \dots a_m)^{-1} = (a_m \dots a_2 \ a_1)$ .
- Falls  $\sigma$ -Produkt disjunkter Zykel geschrieben ist, so ist deren Reihenfolge egal. Merke: Disjunkte Zykel kommutieren:  $\sigma \tau = \tau \sigma$

Zur Rechnung von Produkten erlaubt mir auch Produkte von nicht-disjunkten Zykeln.

Dann ist die Operation in  $S_n$  einfach Kettenfolge von Zykeldarstellungen. Solche Zykeldarstellungen sind absolut nicht eindeutig: z.B.  $(1\ 2)(2\ 3)$  kann als Produkt zweierzykler Zykel geschrieben werden, indem weder der obige Algorithmus verwendet wird. Dann müssen Elemente von rechts verfolgt werden:  $(1\ 2)(2\ 3) = (1\ 2\ 3)$ . Später kann (einfach) gezeigt werden: Jede Permutation ist bis auf Anordnung und zyklische Verbauung ein eindeutiges Produkt zweierzykler Zykel.  $\rightarrow$  Algorithmus findet dieses Produkt. Damit ist es auch leicht, zu prüfen, ob 2 Elemente einer  $S_n$  gleich sind. Die Ordnung eines Elements ist das kleinste gewisse Vielfache der Zykelängen (in der dargestellten Darstellung), denn  $(g \cdot h)^n = g^n \cdot h^n$  und für ein Zykel ist die Ordnung  $m$ :  $(1\ 2\ 3)^3 = 1$ ; außerdem kann man durchgezogene Zykel verbauen.

## 1.4 Homomorphismen (strukturhaltende Abbildungen, lineare Abbildungen realisiert)

In der Mathematik betrachten wir mathematische Objekte oft mit Hilfe von Abbildungen zwischen ihnen. In der Algebra berechnet man als Homomorphismen allgemein die strukturverhaltenden Abbildungen von ~~und~~ algebraischen Strukturen, z.B. lineare Abbildungen zwischen Vektorräumen oder,

Definition: Seien  $(G, \cdot)$  und  $(H, \circ)$  Halbgruppen. Eine Abbildung  $\varphi: G \rightarrow H$  ist ein Halbgruppenhomomorphismus, falls  $\varphi(g_1 \cdot g_2) = \varphi(g_1) \circ \varphi(g_2) \quad \forall g_1, g_2 \in G$ .

Ein Homomorphismus heißt  $\begin{cases} \text{Monomorphismus} & \text{falls } \varphi \text{ injektiv} \\ \text{Epimorphismus} & \text{falls } \varphi \text{ surjektiv} \\ \text{Isomorphismus} & \text{falls } \varphi \text{ bijektiv} \end{cases}$

Homomorphismen mit  $G \rightarrow G$  heißen auch Endomorphismen bzw. Automorphismen.

Der Begriff der Isomorphie, d.h. der Existenz eines Isomorphismus, ist zentral in der Algebra. Isomorphe Objekte werden als gleich angesehen. Alle Konstruktionen, die nur die algebraische Struktur\* verwenden, liefern auf isomorphen Objekten das gleiche Ergebnis. z.B. ist keine abelsche Gruppe isomorph zu einer nicht-abelschen Gruppe. ( $G$  nicht abelsch:  $\exists x, y \in G: xy \neq yx$ ,  $H$  abelsch und  $\varphi: G \rightarrow H$  Isomorphismus.  $\varphi(xy) \neq \varphi(yx)$  da  $\varphi$  injektiv.  $\rightarrow \varphi(x)\varphi(y) \neq \varphi(y)\varphi(x)$ , da  $\varphi$  Homomorphismus - Widerspruch zu  $H$  abelsch.)

Ziele in der Algebra sind oft Klassifizierungen, d.h. Angabe aller Objekte bis auf Isomorphie (wobei isomorphe Objekte ~~als~~ gleich betrachtet werden).

Bsp.: Alle Gruppen der Ordnung 4: Es gibt 2 nicht-isomorphe:  $\mathbb{Z}/4\mathbb{Z}$  dreieckiger Produkt und  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$  (kleinste Viergruppe)

Warum nicht isomorph?  $\mathbb{Z}/4\mathbb{Z}$  enthält ein Element der Ordnung 4,  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$  aber nicht. Isomorphismen erhalten Ordnungen.

Def.: Ein Monoidhomomorphismus ist ein Halbgruppenhomomorphismus zwischen Monoiden  $\varphi: M \rightarrow N$  mit  $\varphi(1_M) = 1_N$ . Ein Gruppenhomomorphismus ist ein Halbgruppenhomomorphismus zwischen Gruppen.

Bew.: Gruppenhomomorphismus  $\Rightarrow$  Monoidhomomorphismus, denn:  
 $\varphi(1) = \varphi(1 \cdot 1) = \varphi(1) \cdot \varphi(1) \xrightarrow{\varphi(1)=1} 1 = \varphi(1)$

Bsp.: -  $H$  Halbgruppe,  $M$  Monoid:  $\varphi: H \rightarrow M$  ist ein Homomorphismus, d.h. es existiert  $\varphi$  ein Homomorphismus  $H \rightarrow M$ .  $h \mapsto 1$  Was ist mit 2 Halbgruppen?

- Für  $a \in U(M)$  ist  $\varphi_a: M \rightarrow M$  ein Automorphismus genannt Konjugation.  
Beweis.  $x \mapsto axa^{-1}$

$\varphi(ax) = axa^{-1} = axa^{-1}aya^{-1} = \varphi_a(x)\varphi_a(y)$ . Bijektiv, da  $\varphi_a$  die Umkehrabbildung ist. Ein Automorphismus dieser Form heißt innerer Automorphismus. Es gibt auch nicht-inne ("äußere") Automorphismen.

## 2. Untergruppen und Satz von Lagrange

### 2.1 Zyklische Untergruppen

Def. Sei  $(G, \circ)$  Gruppe. Dann heißt  $H \subseteq G$  Untergruppe von  $G$  wenn  $H$  mit der Operation  $\circ$  selber eine Gruppe bildet.

Bem. Es reicht zu überprüfen:  $H \neq \emptyset$  und  $x, y \in H \Rightarrow x \cdot y \in H$  und  $x^{-1} \in H$

Bsp.  $(\mathbb{Z}, +) \subseteq (\mathbb{Z}, +)$  ist Untergruppe. Man schreibt auch:  $H \leq G$   
 $(\mathbb{N}_0^*, \cdot) \subseteq (\mathbb{Z}, \cdot)$  ist keine Untergruppe

Def. Sei  $a \in G$ . Dann definiert man die Ordnung von  $a$  als  $\text{o}(a) (= \text{ord}(a)) = |\langle a \rangle|$  mit  $\langle a \rangle := \{ \min \{ k \in \mathbb{N}_0 : a^k = e \} \}$  falls so ein  $k$  existiert, wobei  $e = 1_G$ .  
 sonst

Bsp.  $(123) \in S_3 \Rightarrow (123) \neq e, (123)^3 = e = \text{id} \Rightarrow \text{o}((123)) = 3$

Def.  $a \in G \Rightarrow \langle a \rangle = \{ a^{\pm 1} \mid a \in \mathbb{Z} \} = \{ a, a^2, a^3, \dots, a^0 = e, a^{-1}, a^{-2}, \dots \}$   
 $\langle a \rangle$  ist die zyklische Untergruppe, die von  $a$  erzeugt wird.

Bem.  $\langle a \rangle$  ist kleinste Untergruppe, die  $a$  enthält (alle Gruppen mit  $a$  enthalten auch  $\langle a \rangle$ ).

Def.  $G$  heißt zyklisch wenn  $a \in G$  existiert mit  $\langle a \rangle = G$ .

Bsp. Die Diedergruppe  $D_{2n}$  hat zyklische Untergruppen (z.B. Rotationen), ist aber selber nicht zyklisch.

- $i \in (\mathbb{C}^*, \cdot) \Rightarrow \langle i \rangle = \{ i, -1, -i, 1 \}$  ( $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$ )
- $i \in (\mathbb{C}, +) \Rightarrow \langle i \rangle = \{ -2i, -i, 0, i, 2i, \dots \}$

Proposition  $a \in G$ .

$$\left. \begin{array}{l} \text{Falls: } \\ \text{alle Parameter} \\ \text{verschieden} \end{array} \right\} \begin{array}{l} - \text{o}(a) < \infty \Rightarrow \langle a \rangle = \{ e, a, \dots, a^{\text{o}(a)-1} \} \\ - \text{o}(a) = \infty \Rightarrow \langle a \rangle = \{ e, a^{\pm 1}, a^{\pm 2}, \dots \} \\ \text{Insbes. } |\langle a \rangle| = \infty \end{array} \quad \begin{array}{l} \text{a} \stackrel{\text{def}}{=} a^{\text{o}(a)-1} \stackrel{a^0=e}{\rightarrow} \text{alle paar} \nearrow \\ \text{werte verbinden,} \\ \text{mit anderen Werten } |ka| = \text{o}(a). \end{array} \quad \begin{array}{l} \text{a}^1 \\ \text{a}^2 \\ \vdots \\ \text{a}^{\text{o}(a)} \\ \text{zyklisch} \end{array}$$

Korollar.  $i, j \in \mathbb{Z}$ . Dann  $a^i = a^j \Leftrightarrow \text{o}(a) \mid (i-j)$   
 und  $\text{o}(a) < \infty \Leftrightarrow i \equiv j \pmod{\text{o}(a)}$ .

Insbes.  $a^i = e \Leftrightarrow \text{o}(a) \mid i$ .

Beweis der Proposition: Sei  $\text{o}(a) < \infty$ . Dann existiert  $l \in \mathbb{N}_{>1}$  mit  $\underbrace{e, a, a^2, \dots, a^{l-1}}$ , aber  $a^l \in \{e, a, a^2, \dots, a^{l-1}\}$ , d.h. es existiert  $i \in \{0, \dots, l-1\}$  s.d.  $a^l = a^i$ .

Ang.,  $i \geq 1$  Dann  $a^{l-i} = a^0 = e$ , aber  $l-i < l$ .  $\square$   
 $\Rightarrow i=0 \Rightarrow a^l = e = a^0 = \text{o}(a)$ .

Sei nun  $\text{o}(a) = \infty$ . [Langeweig.]  $\square$

Bedeutung: Zu jeder Ordnung gibt es (bis auf Isomorphie) nur eine zyklische Gruppe (Kettenleit mit Ordnung = Anzahl der Zeiger).

Satz: Sei  $G$  endliche zyklische Gruppe. Sei  $G = \langle g \rangle$ ,  $|G| = n = \text{o}(g) \in \mathbb{N}_{\geq 1}$ .

(a) Jede Untergruppe von  $G$  ist endlich und zyklisch. [Beweis nicht trivial.]

(b) Sei  $d \in \mathbb{N}$  Teiler von  $n \Rightarrow |\langle g^d \rangle| = \text{o}(g^d) = \frac{n}{d}$ ,

denn  $\{g^0, g^{2d}, g^{3d}, \dots, g^{\frac{n}{d} \cdot d} = g^n = e\} = \langle g^d \rangle$ .

(c) Sei  $H \leq G \Rightarrow$  existiert  $m \in \mathbb{N}_{\geq 1} : H = \langle g^m \rangle \Rightarrow H = \langle g^{\text{ggT}(m, n)} \rangle$

$\Rightarrow |H| = \text{o}(g^m) = \text{o}(g^{\text{ggT}(m, n)}) = \frac{n}{\text{ggT}(n, m)}$  insb.  $[\text{o}(g^m) = n / \text{ggT}(m, n)]$ .

Beweis (a) Siehe KM-Lemma S1.

(b)  $\langle g^d \rangle = \langle g^{\text{ggT}(m, n)} \rangle$ . Bsp.:  $2 \mid 10 \Rightarrow \langle g^{10} \rangle \subseteq \langle g^2 \rangle$ . (Warum!)

Insbes.  $\langle g^m \rangle \mid m \Rightarrow \langle g^m \rangle \subseteq \langle g^{\text{ggT}(m, n)} \rangle$

$\exists i, j \in \mathbb{Z} : im + jn = \text{ggT}(m, n)$  (Lemma von Bézout)

$$" \supset " : \dots g^{\text{ggT}(m,n)} = g^m \cdot g^{n-m} = (\underbrace{g^m}_e)^i \cdot (\underbrace{g^n}_e)^j = (g^m)^i \in \langle g^m \rangle. \square$$

Korollar  $\left\{ \begin{array}{l} \text{Teiler von } n \\ \text{Da: } d \mid n \end{array} \right\} \xrightarrow[1:1]{\text{bijektiv}} \left\{ \begin{array}{l} \text{Untergruppen von zyklischen Gruppen der Ordnung } n \\ \text{(bijektiv nach (a), (b), (c))} \end{array} \right\}$   
 Insb. gibt es nur eine Untergruppe von einer Ordnung. (von zyklischen Gruppen)

Bsp.  $(\mathbb{Z}_{10}, +)$  Restklassen modulo 10. ( $\mathbb{Z}_{10} = \langle \bar{1} \rangle$ )  
 $\langle \bar{4} \rangle \subseteq G \Rightarrow \langle \bar{4} \rangle = \{ \bar{4}, \bar{8}, \bar{2}, \bar{6}, \bar{10}=0 \}$  und  $\alpha(\bar{4}) = S$ ,  
 $|\langle \bar{4} \rangle| = \frac{10}{\text{ggT}(\bar{4}, 10)} = \frac{10}{2} = 5$ , passt.  
 $\langle \bar{4} \rangle = \langle \text{ggT}(4, 10) \rangle = \langle \bar{2} \rangle$

Korollar In Situation/Bekannter vom vorigen Satz:  $g^m$  ist Erzeuger von  $\langle g \rangle$   
 $\Leftrightarrow \langle g^m \rangle = \langle g \rangle \Leftrightarrow |\langle g^m \rangle| = |\langle g \rangle| = n$   
 $\Leftrightarrow \frac{n}{\text{ggT}(m, n)} = n \Leftrightarrow \text{ggT}(m, n) = 1$

Bsp:  $\bar{4} = h \xrightarrow{\text{korollar}} \langle m \cdot h \rangle = \langle h \rangle \Leftrightarrow \text{ggT}(m, 5) = 1$   
 $\alpha(h) = S$

Korollar:  $H$  Erzeuger von zyklischer Gruppe der Ordnung  $n$  ist  $\{1 \leq i \leq n-1 : \text{ggT}(i, n) = 1\}$   
 wird mit  $\phi(n)$  bezeichnet und heißt euklidische  $\phi$ -Funktion.

Bsp:  $\phi(5) = 4, \phi(12) = 4$  (nämlich 1, 5, 7, 11)

## 2.2 Nebenklassenzerlegung

Sei  $H \leq G, x \in G$ .

Def.:  $Hx := \{hx \mid h \in H\}$  heißt die Rechtsnebenklasse von  $x$  mod  $H$  (d.h. Rechte Untergruppe)  
 (Analog  $xH$  Linksneneklasse.)

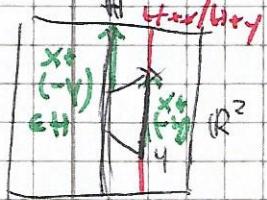
Lemma:  $x, y \in G$ . Dann gilt:  $Hx = Hy \Leftrightarrow Hx = Hy \Leftrightarrow xy^{-1} \in H$ .

Beweis: (ii)  $\Rightarrow$  (i) ✓

$$(i) \Rightarrow (iii) : \exists h, h' \in H: hx = h'y \Rightarrow hxy^{-1} = h' \Rightarrow xy^{-1} = h^{-1}h' \in H$$

$$(iii) \Rightarrow (ii)$$

<u>Lemma.</u> $H \leq G$ , $x, y \in G$ . Äquivalent:	
s.u. (i) $Hx \cap Hy \neq \emptyset$	Beweis: (ii) $\Rightarrow$ (i) $\vee$ (i) $\Rightarrow$ (iii) $\vee$
(ii) $Hx = Hy$	(iii) $\Rightarrow$ (iv): $xy^{-1} \in H \Rightarrow x = hy \in Hy$
s.m. (iii) $x^{-1} \in H$	(iv) $\Rightarrow$ (i): $x = e \cdot x \in Hx \cap Hy$
(iv) $y^{-1} \in H$	$\Rightarrow$ (i) $\Leftrightarrow$ (iii) $\Leftrightarrow$ (iv)
(iv') $x \in Hy$	(i) sym. in $x$ und $y \Rightarrow$ (i) $\Leftrightarrow$ (iii) $\Leftrightarrow$ (iv)
(iv') $y \in Hx$	
(iv): $x \in Hy \Rightarrow x = hy \Rightarrow Hx \subseteq Hy$	{ Damit (i) $\Rightarrow$ (ii). $\square$
(iv): $Hy \subseteq Hx$	

Lemma  $|Hx| = |H|$ Beweis Bijektion  $H \rightarrow Hx$  (Rechtsmultiplikation mit  $x$ )  
 $h \mapsto hx$ ist eine Bijektion, denn die Umkehrabbildung ist die Rechtsmultiplikation mit  $x^{-1}$ .  $\square$ Mit anderen Worten, die Rechtsnebenklassen von  $H$  sind alle gleich groß;  
zwei Rechtsnebenklassen von  $H$  sind entweder gleich oder disjunkt.Bemerkung Die Relation auf  $G$ :  $x \sim_H y \Leftrightarrow Hx = Hy$ ist eine Äquivalenzrelation, (offensichtlich wegen  $\Delta$ )mit Äquivalenzklassen von  $x$ :  $\{y \in G : y \sim_H x\} \stackrel{\text{Lemma}}{=} \{y \in G : y \in Hx\} = Hx$ (d.h. Äquivalenzklassen sind gerade die Rechtsnebenklassen von  $H$ .)Beispiel  $G = (\mathbb{R}^2, +)$  (Vektoraddition)

$$H = \{(0, \beta) : \beta \in \mathbb{R}\} \leq G$$

Die Menge der Nebenklassen entspricht genau den Parallelen

Berechnen zu  $H$ : - es gibt unendlich viele, gleichmächtige, und diese sind alle disjunkt.Nebenklassenzerlegung: AuszeichnungSei  $H \leq G$ , wähle  $\{x_i\}_{i \in I}$  Vertretersystem für alle Rechtsnebenklassen von  $H$ .  
(d.h.  $\{Hx_i\}_{i \in I}$  sind genau die paarweise disjunktten Rechtsnebenklassen).Dann gilt:  $G = \bigcup_{i \in I} Hx_i$ . Die Anzahl der Rechtsnebenklassen von  $H$ heißt Index von  $H$  in  $G$  und wird mit  $|G:H|$  (manchmal  $[G:H]$ ) bezeichnet.

Bem. Es gibt genau viele Rechts- wie Linksnabenklassen.

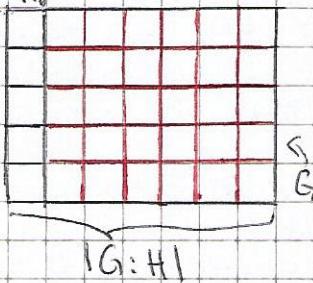
Beweisidee:  $Hx_i \mapsto x_i^{-1}H$  ist eine BijektionSatz von Lagrange $H \leq G$ ,  $G$  endlich.  $\Rightarrow$ 

$$|G| = (H| \cdot |G:H|)$$

Mit anderen Worten:  $|G:H| = \frac{|G|}{|H|}$ Beweis:

$$\text{Beweis: } \sum_{i=1}^{|G:H|} |H| = |G|$$

Beweis durch Schachbrettaufstellung.

also  $|H| \cdot |G:H| = |G|$ .Korollar.  $G$  endlich,  $H \leq G$ (a)  $|H| \mid |G|$  und  $|G:H| \mid |G|$ (b) kleiner Satz von Fermat:

$$x \in G \Rightarrow x^{|G|} = e$$

Mit anderen Worten:  $\alpha(x) \mid |G|$ .

Beweis:  $H := \langle x \rangle \leq G$ ,  $|H| = o(x)$   $\hookrightarrow$  RSA-Algorithmen

$$\Rightarrow |G| = o(x) \cdot |G : H|$$

$$x^{o(x)} = e \Rightarrow x^{|G|} = (x^{o(x)})^{|G : H|} = e$$

(c) Ist  $|G| = p$  prim, dann ist  $G$  zyklisch.

Beweis: Sei  $x \in G$ ,  $x \neq e$ .

$$(c) \Rightarrow o(x) \mid |G| = p \Rightarrow (e \neq x, o(x+1)) \Rightarrow o(x) = p = |G|$$

Aber  $|\langle x \rangle| = |G| \Rightarrow \langle x \rangle = G$ . (mit oben Werten  $\oplus \oplus(p) = p-1$ )

### 3. Normalteiler, Faktorgruppen & Homomorphiesatz

#### 3.1 Normalteiler

Bsp.:  $G = (\mathbb{Z}, +)$ ,  $H = n\mathbb{Z} \leq G \Rightarrow n\mathbb{Z} + k \stackrel{4}{=} \begin{matrix} 4 \\ 0 \\ 0 \\ 8 \end{matrix} \stackrel{3}{=} \begin{matrix} 3 \\ 1 \\ 5 \\ 9 \end{matrix} \stackrel{2}{=} \begin{matrix} 2 \\ 2 \\ 0 \\ 10 \end{matrix} \stackrel{1}{=} \begin{matrix} 1 \\ 3 \\ 7 \\ 11 \end{matrix} \stackrel{0}{=} \begin{matrix} 0 \\ 4 \\ 8 \\ 12 \end{matrix}$

$\Rightarrow |G : H| = 4$

$\rightsquigarrow$  nur können hier mit Nebenklassen rechnen!  
 $\rightsquigarrow$  Können wir das allgemein? Leider nicht.  $\rightsquigarrow$  Nebenklassen = Restklassen

Sei  $G = (G, \cdot)$  Gruppe,  $H \leq G$  Untergruppe.

Def.:  $H$  ist Normalteiler von  $G$  ( $H \trianglelefteq G$ ), wenn  $Hx = xH$  für alle  $x \in G$ .

Bem.:  $R, S, T \subseteq G \Rightarrow R \cdot S := \{r \cdot s \mid r \in R, s \in S\} \leftarrow$  Komplexprodukt  
 $\Rightarrow (R \cdot S) \cdot T = R \cdot (S \cdot T)$

Dann ist  $H \trianglelefteq G \Leftrightarrow x^{-1}Hx = H \quad \forall x \in G$ . (man kann mit Nebenklassen)

(denn  $x^{-1}Hx = (x^{-1}x)H = e(H) \quad \text{assoziativ rechnen}$ )

(i)  $\Leftrightarrow x^{-1}Hx \subseteq H \quad \forall x \in G \quad \text{kein \& unterdrücklich genügend fein!}$

$\Leftrightarrow x^{-1}Hx \subseteq H \quad \forall x \in G, \text{ h.t.}$

Ad (i):  $x^{-1}Hx \subseteq H \quad \forall x \in G$

$\Leftrightarrow H \subseteq x^{-1}Hx^{-1} \forall x \in G$   $\quad \text{offenbar, denn } x^{-1} \text{ invers zu } x^{-1}$

$\Leftrightarrow H \subseteq y^{-1}Hy \quad \forall y \in G \quad \text{denn } y^{-1} \text{ muss zu } y:$

$\Leftrightarrow H \subseteq x^{-1}Hx \quad \forall x \in G \quad \{x^{-1}Hx^{-1} : x \in G\} = \{y^{-1}Hy : y \in G\}$

d.h.  $H = x^{-1}Hx \quad \forall x \in G$

triviale

Bsp.:  $\{-e\}$  und  $G$  sind Normalteiler

- Ist  $G$  abelsch (d.h. kommutativ) so ist jede Untergruppe ein Normalteiler.

- Ist  $|G : H| = 1 \Rightarrow G = H$

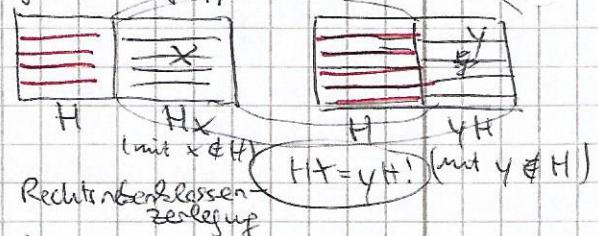
- Ist  $|G : H| = 2$  dann ist  $H \trianglelefteq G$ .

Beweis durch Schiebtafel:

(Es gibt nur 2 Nebenklassen Rechtsnebenklassen, weil eine davon ist)

$H \cdot e \cdot H = H$  selbst, die andere muss

dann  $xH = yH, x, y \in G, x, y \notin H$  sein.)



#### 3.2 Faktorgruppe

Satz: Sei  $H \trianglelefteq G$ . Dann definiert das Komplexprodukt ( $S \cdot T = \{s \cdot t \mid s \in S, t \in T\}$ ) eine Gruppenstruktur auf der Menge der (Rechts = Linken) Nebenklassen von  $H$ . Man bezeichnet diese Gruppe als Faktorgruppe (oder Quotientengruppe)  $G/H$  von  $G$  nach  $H$  modulo  $H$ . (wir können mit Nebenklassen rechnen.)

Beweis:  $x, y \in G$ :  $(Hx) \cdot (Hy) = H(x \cdot y) \stackrel{(\Leftarrow)}{=} H(Hx) \cdot y = (H \cdot H) \cdot (xy) = Hxy$ ,  
 denn  $H \cdot H \subseteq H$  wegen  $h \cdot e \cdot h = h$ , also  $H \subseteq H \cdot H$ .

Also definiert das Komplexprodukt eine assoziative Verknüpfung auf der Menge der Nebenklassen.

Dabei ist  $H$  das Neutralerelement (denn  $Hx \cdot H = Hx \cdot He = Hx = Hx \forall x \in G$ )  
 (entspricht von links).  
 und das Inverse von  $Hx$  ist  $Hx^{-1}$  (denn.  $(Hx)(Hx^{-1}) = Hx \cdot Hx^{-1} = He = H$ ;  
 entsprechend von links).  
 Also ist  $G/H$  mit dem Komplexprodukt eine Gruppe, die Faktorgruppe.  $\square$

Bem.  $- H \leq G \Rightarrow |G/H| = |G : H|$  (Anzahl der Nebeklassen)

- Sei  $H \leq G$ :  $(Hx)(Hy) = Hxy \quad \forall x, y \in G \quad (*)$   
 für  $h \in H$   $Hx \cdot Hy \stackrel{(*)}{=} Hx \cdot h \cdot Hy$

$$Hx = Hx \stackrel{(*)}{=} Hx \cdot e = Hx = H \Rightarrow H = Hx \cdot h \cdot x^{-1}$$

$$\Rightarrow x \cdot h \cdot x^{-1} \in H \quad \forall x \in G \quad \forall h \in H \Rightarrow H \trianglelefteq G$$

(d.h. die Faktorgruppenregel ( $*$ ) über die Multiplikation impliziert, dass  $H$  Normalteiler von  $G$  sein muss,  
 deshalb faktorielle Faktorgruppen nur auf Normalteilern)

## Algebra

24.04.2018

$x$	$y$	$xy$	$(N \trianglelefteq G)$
$x$	$y$	$xy$	
$x'$	$y'$	$x'y'$	

$N_x \quad N_y \quad (N_x)(N_y) = N_{xy}$   
 $= N_{x'} \quad = N_{y'} \quad = (N_x)(N_{y'}) = N_{x'y'}$

dee linke  
Faktorgruppen

Lemma:  $\varphi: G \rightarrow \bar{G}$  Gruppenhomomorphismus

Dann gilt: (1)  $H \leq G \Rightarrow \varphi(H) \leq \bar{G}$

(2)  $K \leq \bar{G} \Rightarrow \varphi^{-1}(K) := \{x \in G : \varphi(x) \in K\} \leq G$

(3)  $K \trianglelefteq \bar{G} \Rightarrow \varphi^{-1}(K) \trianglelefteq G$

Beweis (1), (2) Trivial

(3) sei  $h \in \varphi^{-1}(K)$ ,  $x \in G$ .  $\exists x^{-1}hx \in \varphi^{-1}(K)$

$$\text{Check: } \varphi(x^{-1}hx) \stackrel{\text{Defn.}}{=} (\varphi(x))^{-1} \underbrace{\varphi(h)}_{\substack{\text{konjugieren} \\ \oplus}} \varphi(x) \in K$$

$\uparrow$   
 $K \trianglelefteq \bar{G}$

Bem.  $H \trianglelefteq G \Rightarrow \varphi(H) \trianglelefteq \bar{G}$

Bsp.: sei  $H \trianglelefteq G$ ,  $H \leq G$ ,  $\varphi: H \rightarrow \bar{G}$  Homom. Es gilt:  $H \trianglelefteq H$

$$\text{aber: } H \trianglelefteq G$$

$\equiv$   
 $\varphi(H)$

Bem. "Normalität" ist keine intrinsische Eigenschaft einer Untergruppe, sondern hängt von der Obergruppe ab.

Gleichzeitig ist es normal, nicht unter der Brille zu stehen.  
 Es ist nicht normal, nicht auf den Umplatz runterzufallen.

Bsp.:  $G := S_3$   $H := \langle (12) \rangle = \{ \text{id}, (12) \}$

$$(123)(12) \stackrel{G/H}{=} (1)(32) = (32) \notin H, \text{ also } H \neq G.$$

### 3.3 Homomorphiesatz

Bem.  $N \trianglelefteq G \Rightarrow \Psi: G \rightarrow G/N$  mit der <sup>Menge der</sup> <sup>(Kerngruppe)</sup> <sup>natürliche Epimorphismus</sup>  
<sup>X \mapsto Nx</sup> <sup>(Surjektiver</sup> <sup>Homomorphismus)</sup>  
von  $G$  nach  $G/N$  mit Kern  $\text{Ker}(\Psi) = N$ .

Check: Sei  $x, y \in G \Rightarrow \Psi(x, y) = Nx = (Nx)(Ny) = \Psi(x) \circ \Psi(y)$

$$(\text{Ker}(\Psi)) = \{x \in G : \Psi(x) = 1\} = \{x \in G : Nx = N\} = N.$$

(freies Element bzgl.  $G/N$ )

Mit anderen Worten: Normalteiler sind genau die Kerne von Homomorphismen.

Bem:  $\Psi: G \rightarrow \overline{G}$  Homom.  $\Rightarrow \text{Ker}(\Psi) = \Psi^{-1}(\{e\}) \trianglelefteq G$  <sup>Lemma (3.1)</sup>  
 <sup>$\{e\} \trianglelefteq G$</sup>

### Satz (Noetherscher Homomorphiesatz)

Jeder Homomorphismus  $\Psi: G \rightarrow \overline{G}$  von Gruppen induziert einen Isomorphismus  $\overline{\Psi}: G/\text{Ker}(\Psi) \rightarrow \text{Im}(\Psi)$  mit  $\overline{\Psi}(x) = \Psi(x) \circ \Psi^{-1}(\text{Ker}(\Psi))$ .  $\overline{\Psi}$  ist wohldefiniert und injektiv.

Bem.  $\text{Ker}(\Psi) \trianglelefteq G \rightsquigarrow G/\text{Ker}(\Psi)$  exist. Sinn.  $N := \text{Ker}(\Psi)$  für Unterräume.

Seien  $x, y \in G$ .  $\Psi(x) = \Psi(y) \Leftrightarrow \Psi(x)\Psi(y)^{-1} = e$   
 $\Leftrightarrow \Psi(xy^{-1}) = e \Leftrightarrow xy^{-1} \in \text{Ker}(\Psi) = N \Leftrightarrow Nx = Ny$

$\rightsquigarrow \Psi$  ist wohldefiniert und injektiv.

$\rightsquigarrow \Psi$  ist surjektiv nach Definition.

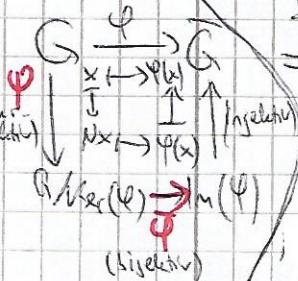
Folgt noch zu zeigen:  $\Psi$  ist Homomorphismus.

$$\begin{aligned} \text{Seien } x, y \in G &\Rightarrow \Psi((Nx)(Ny)) \stackrel{\text{Def.}}{=} \Psi(Nxy) \stackrel{\text{Def.}}{=} \Psi(Nx) \circ \Psi(Ny). \quad \square \end{aligned}$$

Bem. Bezug zu kanonischer Factorisierung von  $\Psi$ :

Seien  $x, y \in G$ . Dann definiere Äquivalenzrelation  $\sim_\Psi$ :  $x \sim_\Psi y \Leftrightarrow \Psi(x) = \Psi(y)$   
 $\Rightarrow$  Äquivalenzklassen von  $\sim_\Psi$  sind genau Nebenklassen von  $\text{Ker}(\Psi)$ :  
 $[x]_\Psi := \{y \in G : y \sim_\Psi x\} = Nx$

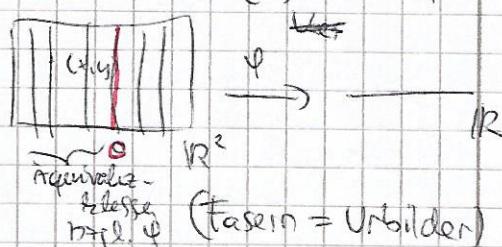
$\rightsquigarrow x$  und  $y$  liegen in gleicher Nebenklasse vom Kern



Bsp.:  $G = (\mathbb{R}^2, +)$   $\overline{G} = (\mathbb{R}, +)$   $\Psi: G \rightarrow \overline{G}$  (Projektion auf  $x$ -Achse)

$$\begin{array}{ccc} \mathbb{R}^2 & \xrightarrow{\Psi} & \mathbb{R} \\ \downarrow \Psi & \nearrow \text{proj.} & \uparrow \text{proj.} \\ \text{Ker}(\Psi) & \xrightarrow{\cong} & \text{Im}(\Psi) = \mathbb{R} \end{array}$$

$$\begin{aligned} \text{Ker}(\Psi) &= \{x \in G : \Psi(x) = 0_{\mathbb{R}}\} \\ &= \{(0, y) : y \in \mathbb{R}\} \end{aligned}$$



$\rightsquigarrow$  die Fasern von  $\mathbb{R}^2$  sind isomorphe zu  $\mathbb{R}$  (unfa.).

Bsp.:  $G := S_n$ . Jeder Permutation  $\sigma \in S_n$  kann man ein Vorzeichen (Signum)  $+1$  oder  $-1$  zuordnen:  $\text{sgn}(\sigma) = 1 \Leftrightarrow \sigma$  ist Produkt von gerade Anzahl von Transpositionen;  $-1$  sonst. oder jede Permutation ist Produkt von Transpositionen

Satz (ohne Beweis): Das ist wohldefiniert. (nicht trivial)

$$\Rightarrow \text{sgn}: (S_n, \circ) \xrightarrow{\quad \text{surjektiv} \quad} (\{+1, -1\}, \cdot) \quad \text{ist Homomorphismus.}$$

$$\sigma \mapsto \text{sgn}(\sigma) \quad \text{(einfach nachrechnen)}$$

mit  $\text{Ker}(\text{sgn}) = \{\sigma \in S_n : \text{sgn}(\sigma) = 1\} = A_n$  gerade Permutationen.  
 $A_n$  heißt alternierende Gruppe.

Hom. Satz:  $\Rightarrow S_n / A_n \cong (\{+1, -1\}, \cdot)$  bzw.

+1	-1
A <sub>n</sub>	

gerade ungerade

(Bsp. für Normatteiler von Index 2)

Bem.  $G$  zyklische Gruppe  $\Rightarrow \varphi: \mathbb{Z} \rightarrow G$

$$(G, \circ) = \langle g \rangle$$

$$k \mapsto g^k$$

$\varphi$  ist surjektiv, ein Homomorphismus ( $\varphi(k+l) = g^{k+l} = g^k \cdot g^l = \varphi(k) \cdot \varphi(l)$ ), mit  $\text{Ker}(\varphi) = \{k \in \mathbb{Z} : g^k = e\}$ .

Sei  $|G| = o(g) = n$ .

1. Fall:  $n = \infty$ . Dann ist  $\text{Ker}(\varphi) = \{0\}$ .  $\xrightarrow[\text{Hem.}]{\text{Ker}} \mathbb{Z}/\{0\} \cong G$

Also  $\mathbb{Z} \cong G$ , es gibt nur eine endliche zyklische

Gruppe der ganzen Zahlen.

2. Fall:  $n \in \mathbb{N}$ . Dann  $\text{Ker}(\varphi) = \{n \cdot z : z \in \mathbb{Z}\} = n\mathbb{Z}$ .

$$\xrightarrow[\text{Hom. Satz}]{\quad} \mathbb{Z}/n\mathbb{Z} \cong G$$

Bem.  $\varphi: G \rightarrow \bar{G}$  Homomorphismus.  $\varphi$  injektiv  $\Leftrightarrow$  alle Fasern von  $\varphi$

$$\text{ker}(\varphi)$$

bestehen aus einem Element

$\hookrightarrow$  Untergruppen von  $G$  bestehen aus 1 Element  $\Leftrightarrow |\text{Ker } \varphi| = 1 \Leftrightarrow \text{Ker } \varphi = \{e\}$ .

Satz Sei  $p > 2$  Primzahl.  $|G| = 2 \cdot p \Rightarrow G \cong \mathbb{Z}_{2p} (= \mathbb{Z}/2p\mathbb{Z})$  oder  $G \cong D_p$

zyklische Gruppe

### 3.4 Isomorphiesätze

Blasius-Diagramm  $\rightarrow$

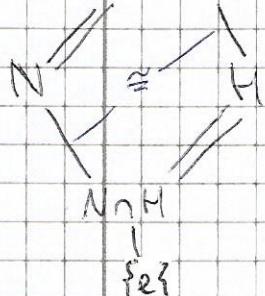
$G$

1. Satz Sei  $N \trianglelefteq G$ ,  $H \trianglelefteq G$ . Dann gilt:  $NH = HN \trianglelefteq G$ ,

$$\frac{N \cap H \trianglelefteq H \text{ und}}{NH \cong H/H \cap N}$$

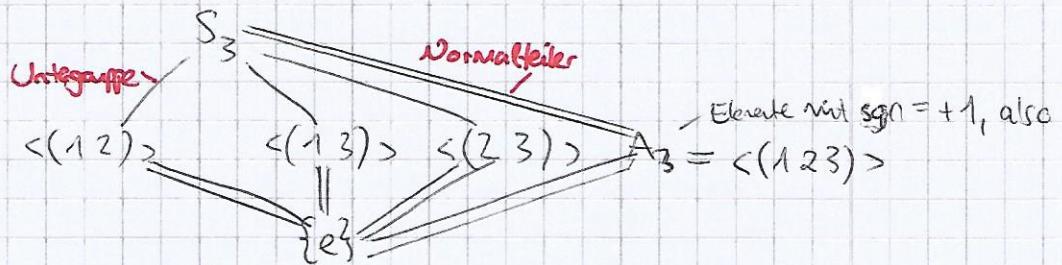
$$HN = NH$$

$$\text{Bsp. } \langle (12)^2, (13)^2 \rangle = \langle (12), (13) \rangle \trianglelefteq S_3. \quad \text{denn 4 Elemente sind kein Teiler von } |S_3| = 6.$$



Bem./Rsp.  $S_3$ ,  $|S_3| = 6$ , alle Unterguppen haben Ordnung 6, 3, 2, 1.  
Untergruppen der Ordnung 2 bestehen aus  $\{e\}$  und einem  
Selbstinversen:  $\langle(12)\rangle \quad \langle(13)\rangle \quad \langle(23)\rangle$

Hasse-Diagramm:  
(des Unterguppenverbandes von  $S_3$ )



### 3.4. Isomorphiesätze

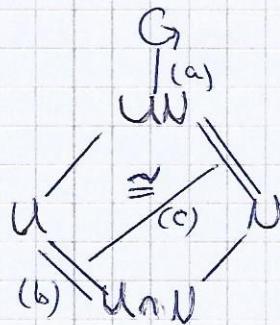
#### 1. Isomorphiesatz

Sei  $G$  eine Gruppe,  $U \leq G$ ,  $N \trianglelefteq G$ . Dann gilt:

$$(a) U \cdot N \leq G$$

$$(b) UN \trianglelefteq U$$

$$(c) UN/N \cong U/(U \cap N) \quad \begin{array}{l} \text{"UN verhält sich zu/N wie U zu U \cap N"} \\ \text{isomorph} \end{array}$$



Beweis:

$$(a) UN \subseteq G, \forall u \in U, n \in N$$

- seien  $u_1, u_2 \in U$ ;  $n_1, n_2 \in N$ .  $\exists u_1 n_1 (u_2 n_2) \in UN$

$$(u_1 n_1)(u_2 n_2) = u_1 n_1 u_2 n_2 = \dots$$

$$\begin{aligned} (\text{Da } N \text{ Normalteiler ist, gilt } u_2 N = N u_2 \Rightarrow \exists n'_1 \in N: u_2 n'_1 = n_1 u_2) \\ \dots = \underbrace{u_1 u_2 n'_1 n_2}_{\in UN} \in UN \end{aligned}$$

-  $\exists n_1^{-1} u_1^{-1} \in U \cdot N^*$ , wie oben, da  $N$  Normalteiler

$$\Rightarrow \exists (n_1^{-1})' \in N: (u_1^{-1})'(n_1^{-1}) = \underbrace{n_1^{-1} u_1^{-1}}_{\in UN}.$$

(b) und (c): Def. Homomorphismus:  $\pi: U \rightarrow G/N$  (eingeschränkter kanonischer Epimorphismus)

Dann ist  $\pi(U) = \{uN | u \in U\} = \{u \cap N | u \in U, n \in N\} = U \cdot N / N$   
und  $\text{Ker}(\pi) = U \cap N$ .

$$\text{Homomorphiesatz: } \text{Im}(\pi) = U \cdot N / N \cong U / U \cap N = U / \text{Ker}(\pi) \quad \square$$

Bsp:  $\exists$   $A_4$  hat keine Untergruppe  $N$  mit  $|N|=6$

$A_4$  hat Index 2 in  $S_4$ , d.h.  $|A_4| = |S_4|/2 = 4!/2 = 12$ , d.h.

$A_4$  hat Index 2 und alle  $U \leq G$  mit Index 2 sind Normalteiler, also

$N \trianglelefteq A_4$ . Ang. es gäbe so ein  $N$ .

Sei  $z \in A_4$  ein 3er-Zykel (hat positives Signum und ist in  $A_4$ ) mit  $z \notin N$  (es gibt 8 3er-Zykeln in  $A_4$  und  $|N|=6$ , also gibt es  $z \notin N$ )

$$\begin{array}{c} (Kern=3) \quad \text{3er-Zykel}; (abc) = (bac) = (cab) \\ \text{Betrachte } \langle z \rangle \text{ und } N \cdot N \cap \langle z \rangle = \{e\} \text{ und } \langle z \rangle \cdot N \cong \langle z \rangle / \{e\} = \langle z \rangle \end{array}$$

$$\Rightarrow |\langle z \rangle \cdot N / N| = 3 \Rightarrow |\langle z \rangle \cdot N| = |\langle z \rangle / N| = 18 \quad \text{g zu } \langle z \rangle \cdot N \leq A_4 \quad \square$$

(Wir nutzen aus, dass wenn  $|U \cap N|$  gleich ist, dann ist mit dem 1. Isomorphiesatz  $|UN|$  groß - was zum Widerspruch führt.)

### Lemma

- (a) Für jeden Gruppenhomomorphismus  $\varphi: G \rightarrow H$  gilt:  $V \trianglelefteq H \Rightarrow \varphi^{-1}(V) \trianglelefteq G$   
 b) Für jeden surjektiven Gruppenhomomorphismus  $\varphi: G \rightarrow H$  gilt:  $N \trianglelefteq G \Rightarrow \varphi(N) \trianglelefteq H$

Beweis: (a) siehe vorige Vorlesung

(b) Sei  $N \trianglelefteq G$ ,  $h \in H$  und wähle  $g \in \varphi^{-1}(h)$  (gilt, weil  $\varphi$  surjektiv).  
 Dann gilt für jedes  $n \in N$ :  $h \cdot \varphi(n) \cdot h^{-1} = \varphi(gng^{-1}) \in \varphi(N)$ ,  
 da  $N$  Normalteiler  $\Rightarrow \varphi(N) \trianglelefteq H$ .  $\square$

### Korrespondenzsatz

Sei  $G$  eine Gruppe,  $N \trianglelefteq G$  und  $\varphi: G \rightarrow G/N$  kanonischer Epimorphismus.

Dann liefert die Abbildung  $U \mapsto U/N = \varphi(U)$  eine Bijektion

$\{ \text{Untergruppen von } G \text{ mit } N \subseteq U \} \leftrightarrow \{ \text{Untergruppen von } G/N \}$   
 mit Unterabbildung  $V \mapsto \varphi^{-1}(V)$ . Dabei gilt  $U \trianglelefteq G \Leftrightarrow U/N \trianglelefteq G/N$ .

Beweis:

$V \mapsto \varphi^{-1}(V)$  wohldefiniert:

$$\varphi^{-1}(V) \subseteq G \quad \wedge \quad \varphi^{-1}(\{e\}) = N \Rightarrow \varphi^{-1}(V) \triangleright N$$

$$U = \varphi^{-1}(U/N)$$

$U \subseteq \varphi^{-1}(U/N)$  nach Def. von Urbild.

Sei  $g \in \varphi^{-1}(U/N)$ , d.h.  $\varphi(g) \in U/N$  d.h.  $gN \in U/N$ .

Dann gibt es  $w \in U$  sodass  $gw = wN$  und somit  $gw^{-1} \in N$ , da  $N$  Normalteiler.

Da  $N \subseteq U$  gilt  $gw^{-1} \in U \Rightarrow g \in U$  (da auch  $(gw^{-1})w \in U$ ).

Lemma oben anwenden für  $\varphi$  kanonischer Epimorphismus.  $\square$

Ereisbrücke: Bruchrechnen

### 2. Isomorphiesatz

Sei  $G$  eine Gruppe,  $N, U \trianglelefteq G$  mit  $N \subseteq U$ . Dann gilt:  $G/U \cong G/N / (U/N)$

Beweis: Nach Korrespondenzsatz ist  $(U/N) \trianglelefteq (G/N)$ , d.h. der Quotient  $(G/N)/(U/N)$  ist wohldefiniert. Definiere  $\varphi: G \xrightarrow{(G/N)/(U/N)} G/U$ .

$\varphi$  ist surjektiver Homomorphismus da Verknüpfung kanonischer Epimorphismen.

$$\text{Ker } \varphi = \{ g \in G : (gN)(U/N)^{-1} = U/N \}$$

$$= \{ g \in G : gN \in U/N \}$$

$$= \{ g \in G : \exists u \in U : gu^{-1} \in N \}$$

$$(\text{da } N \subseteq U) = \{ g \in G : g \in U \}$$

$$= U.$$

Beweisung folgt nun mit dem Homomorphiesatz.  $\square$

BP: Seien  $m, n \in \mathbb{Z}$  mit  $m \mid n$ . (z.B.  $m=3, n=6$ )

$$\mathbb{Z}$$

$$\parallel$$

$$m\mathbb{Z}$$

$$\parallel$$

$$n\mathbb{Z}$$

$$\parallel$$

$$\{0\}$$

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

Wichtige Bemerkungen zu Blatt 2

- 1)  $\mathbb{Z}_3 = \mathbb{Z}/3\mathbb{Z}$ , also Faktorgruppe von  $\mathbb{Z}$ ; keine Untergruppe von  $\mathbb{Z}$ !  
 (in einer Untergruppe bleibt nur die Operation bei, aber  $\mathbb{Z}_3$  hat eine andere Operation (röhrt mit Modulo))  
 In  $\mathbb{Z}_3$  hat jedes Element insb. endliche Ordnung, in  $\mathbb{Z}$  hat nur 0 endliche Ordnung.
- 2)  $(\mathbb{Z}_{24}, +)$  Gruppe. ( $\mathbb{Z}_{24}, \cdot$ ) ist keine Gruppe.  
 Bestellt betrachten wir "by default" die additive Gruppe von  $\mathbb{Z}_n$ .  
 , denn  $[6]^{-1}$  existiert nicht:  $[6][n] = [1] \leftarrow n \cdot [6] = [1] \rightarrow$  kann nicht sein  $(6, 12, 18, 24, 6 \dots)$
- 3)  $2 \cdot [3]_6 = 2 \cdot [0]_6$   
 $\Leftrightarrow [3]_6 = [0]_6$ , da 2 nicht invertierbar ist in der multiplikativen Gruppe.
- 4) zyklische Gruppen gleicher Ordnung sind eindeutig bis auf Isomorphie, aber A. nicht gleich!  
"alle isomorphe"

3.5 Einfache Gruppen

$(G, \circ)$  Gruppe.  $G \neq \{e\}$  und

Def.:  $G$  heißt einfach, wenn  $\{e\}$  und  $G$  die einzigen Normalteiler von  $G$  sind.

Bem.: Einfache Gruppen sind die Bausteine der Gruppentheorie (wie Primzahlen in der Zahlentheorie).

Satz:  $G$  endlich. Dann ist  $G$  einfach und abelsch gew.  $|G|$  prim ist.

Beweis: " $\Leftarrow$ "  $|G|$  prim. Mit Lagrange folgt  $G$  zyklisch (also  $G \cong \mathbb{Z}_p$ ) damit abelsch.

$G$  hat nur  $\{e\}$  und  $G$  als Untergruppe, da die Ordnung jeder Untergruppe  $p$  teilt. (Damit auch Normalteile nur  $\{e\}$  und  $G$ .)

" $\Rightarrow$ "  $G$  einfache & abelsch. Sei  $x \in G$ ,  $x \neq e$ .  $\langle x \rangle \leq G$  gesucht  $\langle x \rangle \trianglelefteq G$

$\Leftrightarrow \text{ergibt } x \neq e \Rightarrow \langle x \rangle = G$ . Also ist  $G$  zyklisch. Sei  $p$  Primzahl mit  $p \mid |G| \neq 1$ .

$\Rightarrow o(x^{(G)/p}) = p \Rightarrow |\langle x^{(G)/p} \rangle| = p$  und  $\langle x^{(G)/p} \rangle \trianglelefteq G$

ergibt  $\langle x^{(G)/p} \rangle = G$ ,  $|G| = p$ .  $\square$

Rsp.:  $\mathbb{Z}_p$  ( $p$  prim);  $A_n$  ( $n \geq 5$ ); ... Gruppen vom Lie-Typ ...

18  $\Rightarrow$   $\infty$ -Familien

KLASSEFAKTION ENDLICHER EINFACHER GRUPPEN

(Beweis umfasst 1500 Seiten, 1920 - 1980 - 2000,  $\geq 100$  Mathematiker)

und 26 sporadische Gruppen:

kleinste hat Ordnung 7920 (Mathieu-Gruppe)

größte hat Ordnung  $2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 53 \cdot 71$   
 (Monstrigruppe) (taucht bei schwarzen Löchern auf)

4. Wirkungen4.1 Die Grundlagen

Sei  $(G, \cdot)$  Gruppe,  $\Omega \neq \emptyset$  Menge.

Def.: Für  $a \in \Omega$  und  $\sigma, \tau \in \text{Sym}(\Omega) \subset$  Permutationen von  $\Omega$

$$\alpha^\sigma := \sigma(a) \in \Omega$$

$$\Rightarrow (\alpha^\sigma)^\tau = \tau(\sigma(a)) = (\tau \circ \sigma)(a) = a^{\tau \circ \sigma} \Rightarrow (\alpha^\sigma)^\tau = \alpha^{\sigma \circ \tau}.$$

Def.:  $\alpha \circ \beta := \beta \circ \alpha$   $\quad (G, \cdot)$   $\quad (\text{Sym}(\Omega), \circ)$ ,  $\circ$  links definiert

Ein Homomorphismus  $\varphi: G \rightarrow \text{Sym}(\Omega)$  heißt eine Permutationsdarstellung  
 von  $G$  auf  $\Omega$ .  $\varphi$  heißt treu, wenn  $\ker(\varphi) = \{e\}$  ( $\varphi$  injektiv ist).  
 (Monomorphismus)

Geg.  $\Phi$  wie in vorheriger Definition.

Def. Sei  $x \in G$ ,  $\alpha \in \Omega$ .  $\alpha^x := \alpha^{\Phi(x)} \in \Omega$  ( $= (\Phi(x))(\alpha)$ )  
 Es gilt für  $x, y \in G$  und  $\alpha \in \Omega$ :  
 $(w_1) \alpha^x = \alpha$  denn:  $\alpha^1 \stackrel{\text{def.}}{=} \alpha \stackrel{\Phi(1) \text{ hom.}}{=} \alpha^{\Omega} \stackrel{\text{def.}}{=} \alpha$   
 $(w_2) \alpha^{xy} = (\alpha^x)^y$ , denn:  $\alpha^{xy} = \alpha^{\Phi(xy)} \stackrel{\text{hom.}}{=} \alpha^{\Phi(x)\Phi(y)} = (\alpha^{\Phi(x)})^{\Phi(y)} = (\alpha^x)^y$ .

Gegeben  $(G, \cdot)$  Gruppe,  $\Omega \neq \emptyset$  Menge.

Def. Die Gruppe  $G$  wirkt auf  $\Omega$ , falls Verknüpfung  $\Omega \times G \rightarrow \Omega$  existiert  
 die Regeln  
 so dass  $(w_1)$  und  $(w_2)$  gelten. Die Verknüpfung heißt Wirkung.  
 Man sagt auch:  $\Omega$  ist ein  $G$ -Raum.

Bem. Also: Eine Permutationsdarstellung von  $G$  auf  $\Omega$   
 definiert eine Wirkung von  $G$  auf  $\Omega$ .

## 4.2 Hauptsatz über Wirkungen

Satz: Sei  $\Omega$  ein  $G$ -Raum.

(a) Für jedes  $x \in G$  ist  $\hat{x}: \Omega \rightarrow \Omega$   
 $\alpha \mapsto \alpha^x$

eine Bijektion, also  $\hat{x} \in \text{Sym}(\Omega)$ .

Die Abbildung  $G \rightarrow \text{Sym}(\Omega)$  ist eine Permutationsdarstellung von  $G$  auf  $\Omega$ .  
 $x \mapsto \hat{x}$

(b) Für jedes  $\alpha \in \Omega$  ist der Stabilisator  $G_\alpha := \{x \in G : \alpha^x = \alpha\}$   
 eine Untergruppe von  $G$ ;  
 und für die  $G$ -Bahn von  $\alpha$   $\alpha^G = \{\alpha^x \mid x \in G\}$   
 gilt die BahngröÙigkeit:  $|G_\alpha| = |G : G_\alpha|$

(c)  $\Omega$  ist disjunkte Vereinigung von  $G$ -Bahnen (Bahnzerlegung).

Beweis (a)  $\hat{x}$  ist injektiv:  $\alpha, \beta \in \Omega$ ,  $x \in G$ :

$$\text{Ang. } \alpha = \beta^x : \quad \alpha \stackrel{(w_1)}{=} \alpha^1 = \alpha^{x \cdot x^{-1}} \stackrel{(w_2)}{=} (\alpha^x)^{x^{-1}} \\ = (\beta^x)^{x^{-1}} \stackrel{(w_2)}{=} \beta^{x \cdot x^{-1}} = \beta^1 \stackrel{(w_1)}{=} \beta$$

$\hat{x}$  ist surjektiv: Sei  $\alpha \in \Omega$ . Wähle  $\beta := \alpha^{x^{-1}} \in \Omega$ .  
 $\Rightarrow \beta^x = (\alpha^{x^{-1}})^x \stackrel{(w_2)}{=} \alpha^{x^{-1}x} = \alpha^1 \stackrel{(w_1)}{=} \alpha$ .

Zeige Homomorphie: Seien  $x, y \in G$ .

$(\hat{x} \cdot \hat{y})(\alpha) \in \text{Sym}(\Omega)$  soll gleich  $\hat{x} \cdot \hat{y} \in \text{Sym}(\Omega)$  sein:

Sei  $\alpha \in \Omega$ .

$$\Rightarrow (\hat{x} \cdot \hat{y})(\alpha) = \alpha^{x \cdot y} \stackrel{(w_2)}{=} (\hat{x})(\alpha)^y$$

$$(\hat{x} \cdot \hat{y})(\alpha) = (\hat{y} \circ \hat{x})(\alpha) = \hat{y}(\hat{x}(\alpha)) = \hat{y}(\alpha^x) = (\alpha^x)^y \stackrel{?}{=}$$

(b)  $-1 \in G_\alpha$ :  $\alpha^1 \stackrel{(w_1)}{=} \alpha \checkmark$

$-x+y \in G_\alpha$ :  $\alpha^{x+y} \stackrel{(w_2)}{=} (\alpha^x)^y = \alpha^y = \alpha \Rightarrow x-y \in G_\alpha \checkmark$

$-x \in G_\alpha$ :  $\alpha \stackrel{(w_1)}{=} \alpha^1 = \alpha^{x+x^{-1}} \stackrel{(w_2)}{=} (\alpha^x)^{x^{-1}} = \alpha^{x^{-1}} \Rightarrow x^{-1} \in G_{\alpha^{-1}}$

(c) Seien  $x, y \in G$ ;  $\alpha \in \Omega$ .

$$\alpha^x = \alpha^y \Leftrightarrow (\alpha^x)^{y^{-1}} = \alpha \Leftrightarrow \alpha^{x \cdot y^{-1}} = \alpha \Leftrightarrow xy^{-1} \in G_\alpha$$

$$\Leftrightarrow G_\alpha x = G_\alpha y$$

...



(Rotierungen auf einer Schleife)

Beweis: ... b)  $x, y \in G: \alpha^x = \alpha^y \Leftrightarrow (\alpha^x)^{y^{-1}} = (\alpha^y)^{x^{-1}} = \alpha^x = \alpha$   
 Das heißt  $\begin{array}{c} \alpha^x \\ \alpha^y \end{array} \xrightarrow{\text{1:1}} \{G_x : x \in G\}$  (Wirkungsklassen über den Normalteiler)  
 $\alpha^x \mapsto G_x$   
 Hier: wohldefiniert wg. " $\Rightarrow$ ", injektiv wg. " $\Leftarrow$ ", surjektiv per Definition  
 Also  $|G_x| = |G : G_x|$ .  
 (zwei Elemente aus der gleichen Klasse liegen sie in der gleichen Wirkungsklasse des Normalteilers liegen.)

c)  $\alpha \sim_G \beta : \Leftrightarrow \exists x \in G: \beta = \alpha^x$   
 (mit  $x, \beta \in \Omega$ ). Dies ist eine Äquivalenzrelation auf  $\Omega$ . (Nachrechnen)  
 mit Äquivalenzklassen  $[a] = a^G \Rightarrow$  führt direkt zur Bahnerzeugung. □

Bem./Def. - Die Wirkung von  $G$  auf  $\Omega$  heißt treu, wenn die Permutationsdarstellung injektiv ist. D.h.  $\ker \left( \begin{array}{c} \Omega \rightarrow \text{Sym}(\Omega) \\ x \mapsto \alpha^x \end{array} \right) = \{e_G\}$

= "alle Elemente von  $G$ , die identisch/trivial wirken auf  $\Omega = \bigcap_{x \in \Omega} G_x$ "  
 (Es gibt keine Elemente außer  $\text{id}$ , die alle Elemente unverändert lassen/stabilisieren  
 $\Rightarrow$  Wirkung ist treu).

- Die Wirkung von  $G$  auf  $\Omega$  heißt transitiv, falls  $\exists \alpha \in \Omega: \Omega = \alpha^G$ , d.h. es gibt nur eine Bahn,  
 d.h.  $\Omega = \alpha^G \forall \alpha \in \Omega$ .

### 4.3 Beispiele

1) Diedergruppe   $D_n$  mit  $n > 2$ .  $D_n$  wirkt auf der Teilmenge  $S_2$  eines regelmäßigen  $n$ -Ecks;  $S_2 = \{1, \dots, n\}:$

- transitiv (es gibt nur eine Bahn)

- treu (nur Identität lässt alle Ecken fest)

$\Rightarrow D_n \rightarrow \text{Sym}(\Omega) = S_n$  injektiv, also  $D_n \cong$  Unterguppe von  $S_n$   
 (vgl. Homomorphiesatz)

D.h.  $|G : G_\alpha| = |\alpha^G|$  für  $\alpha = 1 \in \Omega = |D_n : (D_n)_1| = |1^{D_n}| = |\Omega| = n$   
 $(D_n)_1 = \{ \text{id}, \text{Spiegelung durch Seite 1} \}$   
 (Spiegelung durch Seite 1)  
 (lasse Seite 1 fest)

es gibt nur eine Bahn, transitiv

$$\Rightarrow |D_n| = |(D_n : (D_n)_1| \cdot |(D_n)_1| = n \cdot 2 = 2n$$

2) Reguläre Darstellung  $\Omega = G; \alpha \in G, x \in G, \alpha^x := \alpha x \Rightarrow$  Wirkung (nachrechnen)

heißt reguläre Wirkung. Sei  $\alpha \in G \Rightarrow G_\alpha = \{x \in G : \alpha^x = \alpha\}$

Sie ist transitiv und treu und

stetig transitiv ( $G_\alpha = \{e\}$ ).

$= \{x \in G : \alpha x = \alpha\}$

$= \{e\}$  (jeder Stabilisator ist trivial).

$\Rightarrow G$  injektiv  $\text{Sym}(G) \cong S(|G|)$

(Satz von Cayley:  $G$  ist isomorph zu Unterguppe der  $\text{Sym}(G)$ .

(Wenn man alle Permutationsgruppen und deren Unterguppen verstehen würde,

würde man die Gruppentheorie (endlicher Gruppen) verstehen.)  $\rightarrow$  aber:  $|S_k| = k!$

3) Konjugation  $\Omega = G; \alpha \in G, x \in G: \alpha^x := x^{-1} \alpha x$

Wirkung: (1)  $\alpha^x = \alpha^x x = \alpha \checkmark$  (2)  $(\alpha^x)^y = (x^{-1} \alpha x)^y = y^{-1} x^{-1} \alpha x + y = (xy)^{-1} \alpha (xy) = \alpha^{xy} \checkmark$   
 i.e. nicht total oder transitiv, dafür  $\hat{x}$  ist ein Automorphismus (bijektiv sowie ein Homomorphismus).

Denn:  $\hat{x}(\alpha \cdot \beta) = (\alpha \beta)^x = x^{-1} \alpha \beta x = (x^{-1} \alpha x)(x^{-1} \beta x) = \alpha^x \beta^x = \hat{x}(\alpha) \cdot \hat{x}(\beta)$

$\Rightarrow Q \rightarrow \text{Aut}(G)$  (die Automorphismen auf  $G$ )

$x \mapsto \hat{x} \Rightarrow$  Permutationsdarstellung

$\alpha \in G: \alpha^G = \{x^{-1} \alpha x : x \in G\}$  Konjugierter Klasse von  $\alpha$ .

$G_\alpha = \{x \in G : x^{-1} \alpha x = \alpha\}$

$= \{x \in G : \alpha x = x \alpha\} = C_G(\alpha)$  Zentralisator von  $\alpha$  in  $G$ .

Der Kern der Darstellung heißt Zentrum von  $G$ :  $Z(G) := \bigcap_{\alpha \in G} C_G(\alpha) = \{x \in G : \alpha x = x \alpha \forall x \in G\}$   
 (alle Elemente, die mit allen Elementen vertauschen)  
 $\hookrightarrow$  z.B. Rotation um  $180^\circ$  ist in  $Z(D_n)$ .  
 $G$  abelsch  $\Leftrightarrow Z(G) = G$  (je größer das Zentrum, umso besser ist die Gruppe zu verstehen.)  
 $\hookrightarrow$  einfache Gruppen haben nur triviale Elemente und ein sehr schlechtes Zentrum, kleine Sadie.

4) Konjugierte Untergruppen Sei  $H \leq G$ .  $\Sigma := H^G := \{H^x := x^{-1}Hx : x \in G\}$   
 Hier ist  $H^x \leq G$ , denn Konjugation mit  $x$  ist Homomorphismus ( $\hat{x} : G \rightarrow G$  Homomorphismus)  
 und Bilder von Untergruppen sind Untergruppen.  
 $\alpha \mapsto x^{-1}\alpha x$   
 Damit ist  $\Sigma = H^G$  ein  $G$ -Raum:  $h \cdot e = e^{-1}h e = H$ , Rest nachrechnen.  
 (Jedes Element in  $\Sigma$  ist eine Untergruppe)  
 $\Rightarrow$  transitiv per Definition, alle konjugiert zu  $H$ .  
 Stabilisator von  $H \in \Sigma$  heißt Normalisator von  $H$  in  $G$ :  
 $N_G(H) := \{x \in G : H^x = H\} = \{x \in G : x^{-1}Hx = H\}$ , def.  
 $H \trianglelefteq G \Leftrightarrow N_G(H) = G$  (normal  $\Leftrightarrow$  Normalteiler)  
 Es gilt (nachrechnen):  $N_G(H)$  ist die größte Untergruppe von  $G$ , die  
 $H$  enthält, in der  $H$  normal ist. (fazt mit  $N_G(H) \supseteq H$ ,  $H \trianglelefteq N_G(H)$ )  
 Ferner  $|H^G| = |G : N_G(H)|$ ,  $|HG| = 1 \Leftrightarrow HG = \{H\} \Leftrightarrow G = N_G(H) \Leftrightarrow H \trianglelefteq G$ .  
 (Wenn  $H$  total unnormal ist, hat  $H$  total viele konjugierte Untergruppen.)

## 5. P-Gruppen, abelsche Gruppen, Sätze von Sylow

### 5.1 P-Gruppen

Def.  $G$  heißt P-Gruppe, wenn  $p$  prim und  $|G| = p^k$  mit  $k \in \mathbb{N}$ ; z.B.  $|G| = 2, 3, 4, 5, \cancel{6}, 7, 8, 9, \cancel{10}, \dots$

Lemma  $G$  P-Gruppe.  $\Sigma$  endlicher  $G$ -Raum.

Sei  $\text{Fix}_G(\Sigma) := \{\alpha \in \Sigma : \alpha^x = \alpha \forall x \in G\}$  Menge der Fixpunkte. (z.B.  $\text{Fix}_{D_3}(t)$  zentriert =  $\emptyset$ )

Dann gilt:  $|\Sigma| \equiv |\text{Fix}_G(\Sigma)| \pmod{p}$

Bew.  $\text{Fix}_G(\Sigma)$  ist Vereinigung der Bahnen der Länge 1.

Beweis: Aus Behauptung folgt:  $\text{Fix}_G(\Sigma) \cup \bigcup_{i \in I} \Sigma_i = \Sigma$ , wobei  
 $\{\Sigma_i\}_{i \in I}$  Bahnen der Länge  $> 1$  sind.  
 Sei  $\alpha \in \Sigma_i$ . Dann gilt nach Bahnformel:  $1 < |\Sigma_i| = |\alpha^G| = |G : G_\alpha| = \frac{|G|}{|G_\alpha|}$   
 ist Teiler von  $p^k = |\Sigma| = p^{n_i} > 1$  mit  $n_i \in \mathbb{N}_{\geq 1}$ .  
 $\Rightarrow |\Sigma| = |\text{Fix}_G(\Sigma)| + \sum_{i \in I} p^{n_i} \equiv |\text{Fix}_G(\Sigma)| \pmod{p}$   $\square$

Bem. Falle  $p \nmid |\Sigma|$ , dann  $|\text{Fix}_G(\Sigma)| \not\equiv 0 \pmod{p}$ , insb.  $\text{Fix}_G(\Sigma) \neq \emptyset$ .  
 (Dann gibt es mindestens einen Fixpunkt)

Satz  $G \neq \{e\}$  eine  $p$ -Gruppe, so ist  $Z(G) \neq \{e\}$ . ( $p$ -Gruppen sind nicht so sauber wie einfache)  
 ( $p$ -Gruppe der Ordnung 25 hat mindestens 5 Elemente, die sich mit allen vertauschen.)

Beweis  $G$  nicht auf  $\Sigma = G$  durch Konjugation.  $\Rightarrow \text{Fix}_G(\Sigma) = \{\alpha \in G : x^{-1}\alpha x = \alpha \forall x \in G\}$   
 $= \{\alpha \in G : \alpha x = x \alpha \forall x \in G\} = Z(G)$ .  
 Lemma  $|G| = |\Sigma| \equiv |\text{Fix}_G(\Sigma)| = |Z(G)| \pmod{p}$ .  
 Aber:  $|G| \equiv 0 \pmod{p} \Rightarrow |Z(G)| \equiv 0 \pmod{p}$ , also  $p \mid |Z(G)|$   
 $\Rightarrow Z(G) \neq \{e\}$ .  $\square$

Anwendung:  $|G| = p^2 \Rightarrow G$  abelsch ( $p$  prim)

Beweis: Wir wissen:  $|Z(G)| \neq \{e\}$ . Ist  $|Z(G)| = p^2$ , so ist  $G$  abelsch.

Ist  $|Z(G)| = p$ , so gilt  $|G/Z(G)| = p^2/p = p$ , also ist  $G/Z(G)$  zyklisch.  
Umgekehrt  $G$  abelsch ( $G = Z(G)$ ).

## 5.2 Direkte Produkte

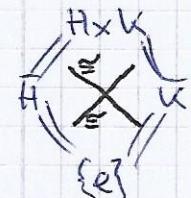
### - Außenes direktes Produkt:

Seien  $H$  und  $K$  Gruppen (multiplikativ).  $\Rightarrow H \times K = \{(h, k) : h \in H, k \in K\}$

ist Gruppe mit komponentenweiser Multiplikation, also  $(h_1, k_1) \cdot (h_2, k_2) = (h_1 \cdot h_2, k_1 \cdot k_2)$   
mit  $e_{H \times K} = (e_H, e_K)$ .

$$\text{Def. } \bar{H} := H \times \{e_K\}, \quad \bar{K} := \{e_H\} \times K, \quad H \cong \bar{H}, \\ \leq H \times K \quad \leq H \times K \quad K \cong \bar{K}.$$

$$\text{Dam. } \bar{H} \leq H \times K, \bar{K} \leq H \times K, \quad H \times K = \bar{H} \cdot \bar{K}, \quad \bar{H} \cap \bar{K} = \{e_{H \times K}\}$$



## Algebra

22.05.2018

### Bemerkungen zu Blatt 3

Achtung:  $H \trianglelefteq D, D \trianglelefteq G \not\Rightarrow H \trianglelefteq G$

$$? \begin{array}{c} G \\ || \\ D \\ \cup \\ H \end{array} \quad D \trianglelefteq G \\ H \trianglelefteq D$$

$$3.1 \varphi: Q \rightarrow G \text{ Hom. } U \trianglelefteq G \\ \Rightarrow D = \varphi^{-1}(U) \trianglelefteq G$$

$$\text{Bew. } Q \xrightarrow{\varphi} \bar{G} \xrightarrow{\psi} \bar{G}/U \Rightarrow \ker(\psi \circ \varphi) = \varphi^{-1}(U) = D \trianglelefteq G$$

Oft:  $\varphi(D) = U$  ist i.d. falsch!

## 5.2 Direkte Produkte

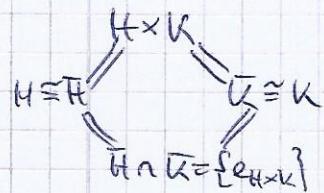
### - Außenes direktes Produkt:

$H, K$  Gruppen  $\Rightarrow H \times K$  Gruppen

$$\text{Def. } \bar{H} = H \times \{e_K\} \trianglelefteq H \times K \text{ dem } (h, k)^{-1}(x_1, x_2)(h, k)$$

$$\bar{K} = \{e_H\} \times K \trianglelefteq H \times K = (k^{-1}x_1h, k^{-1}x_2k)$$

$$\text{Es gitt: } \bar{H} \trianglelefteq H, \bar{K} \trianglelefteq K, \quad \bar{H} \cap \bar{K} = \{(e_H, e_K)\}, \quad \bar{H} \cdot \bar{K} \leq H \times K, \text{ da Normalteiler} \\ = H \times K$$



### - Inneres direktes Produkt:

Def./Satz: Seien  $H, K \leq G$  mit  $G = H \cdot K$  und  $H \cap K = \{e_G\}$ .

Wir sagen,  $G$  ist inneres direktes Produkt von  $H$  und  $K$ .

Dann ist  $H \times K \rightarrow G$  ein Isomorphismus.

$$(h, k) \rightarrow h \cdot k$$

$$G = HK \\ \begin{array}{c} // \\ H \\ \cup \\ K \\ \backslash \\ // \end{array} \\ HK = \{e_G\}$$

Lemma (Kommutatortrick): Ist  $G$  inneres direktes Produkt von  $H$  und  $K$ , so

kommutieren Elemente in  $H$  mit Elementen in  $K$ :  $h \cdot k = k \cdot h \quad \forall h \in H, k \in K$ .

Bew. Seien  $h \in H, k \in K \Rightarrow [h, k] := h^{-1}k^{-1}h \cdot k$  Kommutator mit  $h^{-1}k^{-1}h \cdot k \in H \cap K = \{e_G\}$   
 $\Rightarrow h^{-1}k^{-1}h \cdot k = e \Rightarrow h \cdot k = k \cdot h$ .

$$\begin{array}{c} \nearrow \text{CH w.g. } H \trianglelefteq G, h^{-1} \cdot CH \\ \searrow \text{CK w.g. } K \trianglelefteq G, -k \in CK \end{array} \Rightarrow$$

Bew. von Satz  $\varphi$  Homom.  $\varphi((h, k) \cdot (h', k'))$

$$= \varphi((hh', k'k)) = hh'k'k' \stackrel{\text{Lemma}}{=} hkh'k' = \varphi((h, k)) \cdot \varphi((h', k'))$$

-  $\varphi$  surjektiv wegen  $G = H \cdot K$

-  $\varphi$  injektiv:  $h, h' \in H, k, k' \in K$  mit  $\varphi((h, k)) = \varphi((h', k')) \Rightarrow h \cdot k = h' \cdot k'$

$$\Rightarrow \underbrace{h^{-1}h}_{\in H} = \underbrace{k'k^{-1}}_{\in K} \in H \cap K = \{e_G\} \Rightarrow h^{-1}h = e_G, k'k^{-1} = e_G$$

$$\Rightarrow h = h', k = k' \Rightarrow (h, k) = (h', k') \quad \square$$

### 5.3 Endliche abelsche p-Gruppen

Lemma:  $H, K \leq G$  Gruppen,  $h \in H, k \in K \Rightarrow |\langle o(h, k) \rangle| = \text{kgV}(\langle o(h), o(k) \rangle)$

Beweis:  $\langle o(h, k) \rangle \mid l \Leftrightarrow (h, k)^l = (e_H, e_K) \Leftrightarrow h^l = e_H, k^l = e_K \Leftrightarrow o(h) \mid l, o(k) \mid l \Leftrightarrow \text{kgV}(\langle o(h), o(k) \rangle) \mid l \quad \square$

Prop.:  $H, K$  endliche zyklische Gruppen. Dann gilt

$$H \times K \text{ zyklisch} \Leftrightarrow \text{ggT}(|H|, |K|) = 1$$

Beweis:  $H \times K$  zyklisch  $\Leftrightarrow$   $\exists$   $h \in H, k \in K: o((h, k)) = |H \times K| = |H| \cdot |K|$

$$\Leftrightarrow \exists h \in H, k \in K: \text{kgV}(o(h), o(k)) = |H| \cdot |K| = \dots$$

Lemma:  $n, m \in \mathbb{N} \Rightarrow \text{kgV}(n, m) \cdot \text{ggT}(n, m) = n \cdot m$

Beweis:  $\dots$  Lemma:  $\frac{o(h) \cdot o(k)}{\text{ggT}(o(h), o(k))} / \frac{o(h) \mid |H|}{o(k) \mid |K|} \Leftrightarrow \exists h \in H, k \in K: o(h) = |H|, o(k) = |K|, \text{ggT}(o(H), o(K)) = 1$

$$\Leftrightarrow \text{ggT}(|H|, |K|) = 1 \quad \square$$

Bsp.:  $\mathbb{Z}_2 \times \mathbb{Z}_3$  muss dann als zyklisch sein wg.  $\text{ggT}(2, 3) = 1$  und

$$\text{wegen } 2 \cdot 3 = 6 \text{ gilt } \mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_6.$$

Also auch  $\mathbb{Z}_2 \times \mathbb{Z}_2 \neq \mathbb{Z}_4$ , da  $\mathbb{Z}_2 \times \mathbb{Z}_2$  nicht zyklisch.

### Satz (Frobenius-Stickelberger)

Sei  $G$  abelsche p-Gruppe. Ist  $H \leq G$  eine zyklische Untergruppe maximaler Ordnung, so existiert eine Untergruppe  $K \leq G$  mit  $G = H \cdot K$  und  $H \cap K = \{e\}$ . Man sagt:  $K$  ist Komplement zu  $H$ , insbesondere:  $G \cong H \times K$ .

Folgerung: Jede abelsche p-Gruppe ist direktes

Produkt von zyklischen p-Gruppen.

Bem./Def.: Ist  $G \cong \mathbb{Z}_{p^{a_1}} \times \dots \times \mathbb{Z}_{p^{a_r}}$ , so heißt  $(p^{a_1}, \dots, p^{a_r})$  Typ von  $G$ . (Notiz:  $\overset{G \text{ multiplikativ}}{a_i}$  additiv)

Bsp.:  $\mathbb{Z}_2 \times \mathbb{Z}_2$  hat Typ  $(2, 2)$ ;  $\mathbb{Z}_4$  hat Typ  $(4)$ .

$(a_1; 2, 1)$

Prop.: Ist  $G$  vom Typ  $(p^{a_1}, \dots, p^{a_r})$  mit  $a_1 \geq a_2 \geq \dots \geq a_r$ , so ist  $(a_1, \dots, a_r)$  eindeutig.

Bew.:  $G \cong \mathbb{Z}_{p^{a_1}} \times \dots \times \mathbb{Z}_{p^{a_r}}$ ,  $b_1 \geq b_2 \geq \dots \geq b_r$

Idee:  $\Psi: G \rightarrow G, (\Psi(xy) = (xy)^p = x^p y^p = \Psi(x)\Psi(y))$  Homomorphismus,  $\Psi(G) = G^p \leq G$

$$x \mapsto x^p \quad \text{abelsch}$$

(Bsp.:  $\mathbb{Z}_8 = \langle [1] \rangle \rightarrow 2\mathbb{Z}_8 = \langle [2] \rangle$  d.h.  $|2\mathbb{Z}_8| = 8, |2\mathbb{Z}_8| = 4, 2\mathbb{Z}_8 \cong \mathbb{Z}_4$ )

$$\text{und } G^p \cong (\mathbb{Z}_{p^{a_1}})^p \times \dots \times (\mathbb{Z}_{p^{a_r}})^p \cong (\mathbb{Z}_{p^{b_1}})^{a_1} \times (\mathbb{Z}_{p^{b_r}})^{a_r}$$

$\cong \mathbb{Z}_{p^{b_1}} \times \dots \times \mathbb{Z}_{p^{b_r}}$ . Jetzt Induktion.  $\square$

Bsp.: Alle abelschen Gruppen der Ordnung 16, bis auf Isomorphie:

$$\mathbb{Z}_{16}, \mathbb{Z}_4 \times \mathbb{Z}_4, \mathbb{Z}_2 \times \mathbb{Z}_8, \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2, \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_4$$

### 5.4 Sätze von Sylow

Sei  $G = (G, \cdot)$  endliche Gruppe,  $p$  Primzahl,  $|G| = p^a \cdot r$ , mit  $a, r \in \mathbb{N}, p \nmid r$ .

(z.B.  $12 = 2^2 \cdot 3$ ;  $p = 2, a = 2, r = 3$ ;  $p = 3, a = 1, r = 4$ )

Def.: Eine Untergruppe  $P \leq G$  heißt eine p-Sylowgruppe von G,  $P \in \text{Syl}_p(G)$

falls gilt: (i)  $P$  ist p-Gruppe (ii)  $P \nmid (G:P)$ . D.h.  $|P| = p^a$

( $p$ -Sylow-Gruppe ist eine p-Gruppe maximaler Ordnung.)

### Hauptatz (Sylow)

(a) Es gibt p-Sylowgruppen ( $\text{Syl}_p(G) \neq \emptyset$ ) und je zwei sind konjugiert in  $G$ .

(b)  $|\text{Syl}_p(G)| \equiv 1 \pmod{p}$

(c) Jede p-Untergruppe von  $G$  liegt in einer geeigneten p-Sylowgruppe von  $G$ .

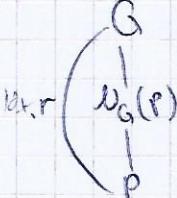
Bem.:  $G$  nicht auf  $\text{Syl}_p(G)$  durch Konjugation, denn Konjugation ist Automorphismus, erhält alle die Untergruppenrechtsförm und die Anzahl an Elementen

$$P \in \text{Syl}_p(G) \Leftrightarrow P^g := g^{-1} P g \leq G, |P^g| = |P| = p^a \Rightarrow P^g \in \text{Syl}_p(G).$$

Ist  $P \in \text{Syl}_p(G)$  dann  $|P^G| \overset{\text{Beh.}}{=} [G : N_G(P)] = |G| / |N_G(P)|$

Stabilisator

erreichender Schritt



Sylow-Gruppen

Bem. Die Umkehrung vom Satz von Lagrange ist falsch:

Sei  $G$  endliche Gruppe und  $d \mid |G|$ . Dann muss es nicht sein, dass  $H \leq G$  s.d.  $|H|=d$ .

Bsp.:  $G = A_4 \leq S_4$  alternierende Gruppe,  $|G|=12$ .  $A_4$  hat aber keine Untergruppe mit Ordnung 6:

Untergruppen von  $A_4$ :

$$\begin{array}{c}
 A_4 \\
 \{e, (12)(34), (14)(32)\} \quad \{e, (24), (234)\} \quad \{e, (134), (143)\} \\
 \{e, (12)(34)\} \quad \{e, (13)(24)\} \quad \{e, (14)(23)\} \quad \{e, (142), (1247)\} = H_2 \\
 \{e\} \quad \{e, (123), (132)\} = H_1
 \end{array}$$

ABER: Falls  $d=p^k$  wobei  $p$  prim, dann  $\exists H \leq G$  mit  $|H|=p^k$ .

Falls  $k$  die größte Potenz von  $p$  s.d.  $p^k \mid |G|$  und falls

$$|H_1| = |H_2| = p^k, \text{ dann } \exists g \in G \text{ s.d. } gH_1g^{-1} = H_2.$$

Def. Sei  $G$  endliche Gruppe,  $p$  eine Primzahl. Eine Untergruppe von  $G$  mit Ordnung  $p^k$  heißt eine  $p$ -Sylow-Untergruppe von  $G$ , falls  $k$  ist die größte Potenz von  $p$ , d.h.  $p^{k+1} \nmid |G|$ .  $Syl_p(G)$  ist die Menge der  $p$ -Sylow-Untergruppen.

- Bsp.:
- $|A_4|=12=2^2 \cdot 3$  Sei  $H \in Syl_2(A_4)$ ,  $|H|=4$   
 $H_1, H_2 \in Syl_3(A_4)$ ,  $gH_1g^{-1}=H_2$  wobei  $g=(12)(34) \in A_4$ .
  - $|G|=100=5^2 \cdot 2^2$ .  $H \in Syl_5(G) \rightarrow |H|=25$   
 $h \in Syl_2(G) \rightarrow |H|=2^2$
  - $\mathbb{Z}_{12}$ . Wir wissen, dass für  $d \mid 12$   $\exists H \leq \mathbb{Z}_{12}$  mit  $|H|=d$ .  
 $\Rightarrow$  Die einzige 2-Sylow-Untergruppe ist  $\{0, 3, 6, 9\}$ .  
Die einzige 3-Sylow-Untergruppe ist  $\{0, 4, 8\}$ .

Sätze von Sylow (1872)Satz 5.4.1 (Sylow I)

Eine endliche Gruppe  $G$  hat eine  $p$ -Sylow-Untergruppe für jede Primzahl  $p$ , und jede  $p$ -Untergruppe liegt in einer  $p$ -Sylow-Untergruppe.

Bsp.:  $\{e, (12)(34)\} \leq \{e, (12)(34), (13)(24), (14)(23)\}$   
unter einer 2-Gruppe  $\quad \quad \quad$  2-Sylow-Untergruppe

Satz 5.4.2 (Sylow II)

Für jede Primzahl  $p$  sind die  $p$ -Sylow-Untergruppen von  $G$  konjug. et. ( $Q=gPg^{-1}$ )

Beweis: Seien  $P, Q$  zwei  $p$ -Sylow-Untergruppen. Betrachte die Wirkung von  $Q$  auf  $pG$  als die Multiplikation von links. Da  $Q$  endlich und eine  $p$ -Gruppe ist  $|Q:P| \equiv |pG| = |\text{Fix}_Q(pG)| \pmod{p}$ . Dann  $|G:P| = |G|/|P| \not\equiv 0 \pmod{p}$ , da  $P$  eine  $p$ -Sylow-Untergruppe ist.  $\Rightarrow |\text{Fix}_Q(pG)| \not\equiv 0 \pmod{p}$   
 $\Rightarrow \exists gP \in pG$  s.d.  $gPg^{-1} = P$   $\forall q \in Q \Rightarrow gq \in gP \quad \forall q \in Q$   
 $\Rightarrow Q \subseteq gPg^{-1} \Rightarrow$  Da  $|Q| = |gPg^{-1}| \Rightarrow Q = gPg^{-1}$ .  $\square$   
Wiederholung

### Satz 5.4.3 (Sylow III)

Für jede Primzahl  $p$  sei  $n_p$  die Anzahl von  $p$ -Sylow-Untergruppen von  $G$ .

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

Dann  $n_p \equiv 1 \pmod{p}$  und  $n_p \mid m$ .

Bem. (Sylow III')

$$\text{Ist } P \in \text{Syl}_p(G). \Rightarrow n_p = |\text{Syl}_p(G)| = |pG| \stackrel{(+)}{=} |G : \text{Stab}_{G(p)}|$$

(\*) Behr.-Stabilisator-Satz:

$$|pG| = |\{g \in G : gPg^{-1} = P\}| = N_G(P) \quad \text{(*)}$$

Außerdem  $P \trianglelefteq G \Leftrightarrow G = N_G(P) \Leftrightarrow \text{Syl}_p(G) = \{P\}$ .

( $P$  ist Normalteiler wenn es die einzige Sylowgruppe ist.)

Widerr.: nach Sylow II

Widerr.:

$$G \not\simeq \text{Syl}_p(G)$$

$$pG = \{p = x^{-1}px \mid x \in G\}$$

$$\text{Bsp.: } G = A_4, |A_4| = 2^2 \cdot 3 = 12 \quad (p=2, 3=n) \quad (|G| = p^k m)$$

$$n_2 \equiv 1 \pmod{2}, n_2 \mid 3 \Rightarrow n_2 = 1$$

$$n_3 \equiv 1 \pmod{3}, n_3 \mid 4 \Rightarrow n_3 = 1 \text{ oder } 4$$

- Sei  $|G| = 24 = 2^3 \cdot 3$

$$n_2 \equiv 1 \pmod{2}, n_2 \mid 3 \Rightarrow n_2 = 1 \text{ oder } 3$$

$$n_3 \equiv 1 \pmod{3}, n_3 \mid 8 \Rightarrow n_3 = 1 \text{ oder } 4$$

Anwendungen von Sylow:

(1) Zeige, dass es keine einfache Gruppe mit Ordnung 30 gibt.

Sei  $Q$  einfach und  $|G| = 30 = 2 \cdot 3 \cdot 5$ . (Sylow III  $\Rightarrow n_3 \mid 10$  und  $n_3 \equiv 1 \pmod{3}$ )

$\Rightarrow n_3 = 1$  oder 10. Falls  $n_3 = 1$ , dann ist 3-Sylow-Untergruppe ein Normalteiler (Sylow III'). Widerspruch zu  $G$  einfach.

Dann  $n_3 = 10$ . Der  $P \in \text{Syl}_3(G)$ ,  $P = \{p_1, p_2\}$ ,  $p_1^3 = p_2^3 = e$ .

$\Rightarrow$  Es gibt 20 Elemente von  $G$  mit Ordnung 3.

$n_5 \mid 6$  und  $n_5 \equiv 1 \pmod{5} \Rightarrow n_5 = 1$  oder 6;  $n_5 \neq 1$  (s.d.).

Dann  $n_5 = 6$ .  $P \in \text{Syl}_5(G)$ ,  $P$  hat 4 Elemente mit Ordnung 5.

$\Rightarrow$  Es gibt 24 Elemente von  $G$  mit Ordnung 5.

$$\Rightarrow 20 + 24 > 30. \quad \text{Widerspruch!}$$

(2) Es gibt nur eine Gruppe mit Ordnung 15. <sup>W.W.</sup>

Sei  $|G| = 15 = 3 \cdot 5$ . Jede 3-Sylow-Untergruppe hat die Ordnung  $3 \cong \mathbb{Z}_3$ .

Jede 5-Sylow-Untergruppe hat die Ordnung  $5 \cong \mathbb{Z}_5$ .

Nach Sylow III:  $n_3 \equiv 1 \pmod{5}, n_3 \mid 5 \Rightarrow n_3 = 1$

$n_5 \equiv 1 \pmod{3}, n_5 \mid 3 \Rightarrow n_5 = 1$

Nach Sylow III':  $P \trianglelefteq G$  &  $Q \trianglelefteq G$ .

Da  $P$  el. Ordnung 3,  $Q$  el. Ordnung 5 hat, mit  $P \cap Q = \{e\}$

$$\Rightarrow |P \cdot Q| = |\{p \cdot q \mid p \in P, q \in Q\}| = 15.$$

$$\Rightarrow P \cdot Q = G = P \times Q \quad \text{direkter Produkt}$$

$$\Rightarrow Q = \mathbb{Z}_3 \times \mathbb{Z}_5 \cong \mathbb{Z}_{15}. \quad \text{Restsatz}$$

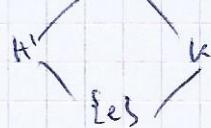
### 5.5 Normalformen abelscher Gruppen (Verallgemeinerung von (2))

Def. Seien  $H$  und  $K$  multiplikative Gruppen. Dann ist  $\bar{G} = H \times K = \{(h, k) \mid h \in H, k \in K\}$  eine Gruppe bzgl. komponentenweiser Multiplikation.  $((h_1, k_1) \cdot (h_2, k_2)) = (h_1 \cdot h_2, k_1 \cdot k_2)$

$\bar{G} = H \times K$  heißt direktes Produkt von  $H$  und  $K$ .  $|G| = |H| \cdot |K| = |H| \cdot |K|$

Seien  $H' = \{(h, 1) \mid h \in H\}$  und  $K' = \{(1, k) \mid k \in K\}$ .  $H'$  und  $K'$  sind Untergruppen von  $\bar{G} = H \times K$ .  $H' \cap K' = \{e\}$ . Jedes Element von  $g \in \bar{G}$ ,  $g = h'k'$ , mit  $h' \in H'$ ,  $k' \in K'$ .  $h'k' = h'k'$ , also  $H' \trianglelefteq \bar{G}$ ,  $K' \trianglelefteq \bar{G}$ .

Nach (\*)  $\bar{G} = H \times K = H'K' = \{(h'k') \mid h' \in H', k' \in K'\}$



Dieses Produkt nennt man  
inneres direktes Produkt.

Prop. 5.5.1 Seien  $H, K$  Normalteiler von  $G$  mit  $H \cap K = \{e\}$ . Dann  $G \cong H \cdot K \cong H \times K$ .

Bew. Sei  $x \in G$  und  $x = hkh^{-1}k^{-1}$ ,  $h \in H$ ,  $k \in K$   
 $= hkh^{-1}k^{-1}$   
 $\underset{H \in K}{\Rightarrow} x \in K$

ähnlich:  $x = h \underset{K \in H}{(k k^{-1} k^{-1})} \underset{K \in H}{\Rightarrow} x \in H$

Ri.A. muss  $H \cdot K$  keine Gruppe sein)

$$\Rightarrow x \in H \cap K \Rightarrow x = e \Rightarrow hk = kh \quad \forall h \in H, k \in K$$

$$\Rightarrow HK \text{ ist eine Gruppe, } h_1k_1h_2k_2 = \underset{H}{h_1h_2} \underset{K}{k_1k_2} \in HK$$

Betrachte den Homomorphismus  $H \times K \rightarrow HK$ . Dieser ist ein Isomorphismus:  
 $(h, k) \mapsto hk$

Sei  $hk = h'k'$  mit  $h, h' \in H$ ,  $k, k' \in K$ . Dann  $(h')^{-1}h = k'^{-1}k \in H \cap K = \{e\}$   
 $\Rightarrow h = h'$  und  $k = k'$   $\Rightarrow HK \cong H \times K$ .  $\square$

Sei  $G$  endliche Gruppe,  $|G| = \prod_{i=1}^k p_i^{a_i}$  Primfaktorzerlegung und sei  
 $Syl_p(G) = \{P_i\}$   $\underset{\text{alle } p}{\text{mit }} P_i \trianglelefteq G$  für jedes  $i$ .

Dann nach Prop. 5.5.1  $G = P_1 \dots P_k$   
 $\underset{\text{inneres direktes}}{\text{Produkt}}$

Beweis kann man rekursiv machen:  
 $(P_1 \dots P_{k-1}) P_k$   
 $\underset{\text{Normalteiler Normalteiler}}{\text{Produkt}}$

Folgerung 5.5.2 Jede endliche abelsche Gruppe  $G$  ist ein inneres direktes Produkt ihrer Sylowgruppen (da diese alle Normalteiler sind).

Bem.  $|G| = \prod_{i=1}^k p_i^{a_i} = |P_1| \dots |P_k| = p_1^{a_1} \dots p_k^{a_k}$ .

Wiederholung: Eine endliche abelsche  $p$ -Gruppe ist ein <sup>inneres direktes</sup> Produkt von zyklischen Gruppen.

1. Normalform  $G = P_{p_1} \dots P_{p_k}$ . Dann existieren für jede  $p$ -Sylow-Untergruppe  $P_p$  mit  $|P_p| = p^m$ ,  $k \in \mathbb{N}$  und  $m_i \in \mathbb{N}$ ,  $1 \leq i \leq k$  mit  $n_1 > m_2 > \dots > m_r$  und  $n_1 + \dots + m_k = m$  so dass  $P_p \cong \mathbb{Z}_{p^{n_1}} \times \dots \times \mathbb{Z}_{p^{n_r}}$ .

Bsp.:  $|G| = 100 = 2^2 5^2 \Rightarrow \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{25} \cong \mathbb{Z}_4 \times \mathbb{Z}_5 \times \mathbb{Z}_5 \dots$   
 $\dots \cong \mathbb{Z}_4 \times \mathbb{Z}_{25} \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_5 \overset{P_2}{\cong} \mathbb{Z}_5 \cong G$ .

2. Normalform:  $G \cong \mathbb{Z}_{a_1} \times \dots \times \mathbb{Z}_{a_r}$  mit  $a_1 | a_2 | \dots | a_r$

Bsp.:  $|G| = 100 \rightarrow G \cong \mathbb{Z}_2 \times \mathbb{Z}_{50} \cong \mathbb{Z}_5 \times \mathbb{Z}_{20} \cong \mathbb{Z}_{100} \cong \mathbb{Z}_{10} \times \mathbb{Z}_{10}$

II. Ringe und KörperG. Grundlagen über RingeG.1 Ringe

Def.  $(R, +, \cdot)$  Ring, wenn  $+, \cdot$  binäre Operationen auf  $R$  sind mit

- (1)  $(R, +)$  abelsche Gruppe
- (2)  $(R, \cdot)$  assoziativ
- (3)  $a \cdot (b+c) = a \cdot b + a \cdot c \quad \forall a, b, c \in R$   
 $(a+b) \cdot c = a \cdot c + b \cdot c$   
d.h. Distributivgesetze gelten.

Bem.  $R$  heißt kommutativer Ring, wenn  $(R, \cdot)$  kommutativ ist.

-  $R$  heißt Ring mit 1 (oder unitär), wenn  $(R, \cdot)$  ein (oder 1-Ring) Neutralelement hat, bezeichnet mit  $1 = 1_R$ .

Bsp.:  $\mathbb{R}[x]$  Polynomring,  $\mathbb{Z}$  Restklassenring,  $\text{Mat}_{n \times n}(R)$  Matrizenring  
und natürlich  $\mathbb{Z}$ ,  $\mathbb{Q}$ ,  $\mathbb{R}$ ,  $\mathbb{C}$ ,  $2\mathbb{Z} \leftarrow$  ring ohne 1 nicht kommutativ

Bem.: Additives Neutralelement heißt  $0 = 0_R$ . Erwartete Eigenschaften gelten.

- $0 \cdot a = 0 \quad \forall a \in R$   
(Bew.  $0 \cdot a = (0+0)a = 0 \cdot a + 0 \cdot a \Leftrightarrow 0 = 0 \cdot a$  wg. Gruppe)
- $-a = (-1) \cdot a \quad \forall a \in R$
- $(-a)(-b) = a \cdot b \quad \forall a, b \in R$  uvm.
- $1 = 0 \Leftrightarrow R = \{0\}$  (trivialer Ring)  
( $\Rightarrow a \in R \Rightarrow a = 1 \cdot a = 0 \cdot a = 0$ )

G.2 Teilringe

Def. Sei  $S$  Ring, dann heißt  $R \subseteq S$  Teilring von  $S$  wenn Addition und Multiplikation in  $R$  gleich wie in  $S$  ist. (Abgeschlossenheit wie bei Gruppen)  
(Untergruppe additiv und abgeschlossen multiplikativ)

Bsp.:  $R := \{\bar{0}, \bar{2}, \bar{4}\} \subset \mathbb{Z}_6 =: S$ ,  $R$  Teilring von  $S$  mit  $1_R = \bar{4} \neq \bar{1} = 1_S$   
(Teilring kann bei uns ein anderes Neutralelement bzgl. Multiplikation haben als der Oberring!)

-  $\mathbb{Q} \subset \mathbb{R}$  mit  $1_{\mathbb{Q}} = 1_R$

Bem. Für Ring mit 1 wird oft gefordert, dass Teilringe gleiche 1 haben (wie jedoch nicht).

G.3 Einheiten und Nullteiler

Sei  $R$  kommutativer Ring mit 1.

Def.:  $R^\times := \{a \in R : \exists b \in R \text{ mit } a \cdot b = 1\}$  heißen Einheiten von  $R$ .

Bem.  $(R^\times, \cdot)$  ist abelsche Gruppe, genannt Einheitengruppe von  $R$ .

Bem.  $0 \in R^\times \Rightarrow \exists b \in R : 0 = 0 \cdot b = 1 \Rightarrow R = \{0\}$

Also  $R \neq \{0\} \Rightarrow R^\times \subseteq R \setminus \{0\}$ .

Obzg.:  $R_1, \dots, R_e$  kommutative 1-Ringe.

$\Rightarrow R_1 \times \dots \times R_e$  kommutativer 1-Ring mit  
 $(R_1 \times \dots \times R_e)^\times = R_1^\times \times \dots \times R_e^\times$ .

# Algebra

31.05.2018

Def.  $a \in R$  heißt Nullteiler wenn  $\exists b \in R \setminus \{0\}: a \cdot b = 0$ .

Bem.  $R \neq \{0\} \Rightarrow 0$  Nullteiler.

Bem. Sei  $R \neq \{0\}$ . Dann  $\{\text{Einheiten}\} \subseteq \{\text{Nichtnullteiler}\} \subseteq R \setminus \{0\}$

die besten "auch noch okay"

Bsp. In  $\mathbb{Z}_4$ :  $[2]$  Nullteiler.

Def.:  $R$  heißt Körper (field), wenn  $0 \neq 1$ ,  $R$  kommutativer 1-Ring ist und  $R \setminus \{0\} = R^\times$

$R$  heißt Integritätsbereich (integral domain), wenn  $0 \neq 1$ , und  $R \setminus \{0\} = \{\text{Nichtnullteiler}\}$ , d.h.  $a \cdot b = 0 \Rightarrow a = 0 \vee b = 0$ . (\*)

Bem. In Integritätsbereichen gilt die Kürzungseigenschaft:  $\frac{a \cdot x = b \cdot x}{x \neq 0} \Rightarrow a = b$ .

Bem.  $a \cdot x = b \cdot x \Leftrightarrow a \cdot x - b \cdot x = 0 \Leftrightarrow (a - b) \cdot x = 0 \stackrel{(*)}{\Leftrightarrow} a - b = 0 \Rightarrow a = b$ .

Hierarchie:  $\{\text{Körper (und deren Teile)}\}_{(R)} \subset \{\text{Integritätsbereiche}\}_{(\mathbb{Z})} \subset \{\text{kommutative 1-Ringe}\}_{(\mathbb{Z}_4)}$

Satz:  $R$  ist endlicher Integritätsbereich. Dann ist  $R$  Körper.

Bew. Sei  $a \in R \setminus \{0\}$ . Definiere  $\varphi: R \rightarrow R \quad \varphi: (R, +) \rightarrow (R, \cdot)$  ist

$$b \mapsto a \cdot b$$

Gruppenhomomorphismus, d.h.  $\varphi(b_1 + b_2) = a \cdot b_1 + a \cdot b_2 = a(b_1 + b_2) = \varphi(b_1 + b_2)$ .

$R$  Integritätsbereich  $\Leftrightarrow \text{Kern } (\varphi) = \{0\}$ , Hergestellt.  $\varphi$  injektiv

Mit  $R$  endlich und injektiver Selbstabbildung folgt  $\varphi$  bijektiv

$\Rightarrow \varphi$  surjektiv: ex.  $b \in R$  s.d.  $a \cdot b = \varphi(0) = 1$ .  $\square$

Bsp.:  $\mathbb{Z}_p, p \text{ prim}$  ist endlicher Integritätsbereich, also auch Körper.

## 6.4 Ringhomomorphismen

Seien  $R, S$  Ringe.

Def.  $\varphi: R \rightarrow S$  heißt Ringhomomorphismus, wenn  $\varphi(a+b) = \varphi(a) + \varphi(b)$   $\forall a, b \in R$ . Ist  $\varphi$  bijektiv, heißt  $\varphi$  Ringisomorphismus.  $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$

Bem. Es gilt nicht automatisch für 1-Ringe, dass  $\varphi(1_R) = 1_S$ .

Dies wird aber oft in Def. gefordert (die jedoch nicht).

Bem (Übung):  $\varphi$  Ringisomorphismus  $\Leftrightarrow \text{Kern } (\varphi) := \{a \in R : \varphi(a) = 0\} = \{0\}$  und  $\varphi(R) = S$

$\Rightarrow \varphi^{-1}$  ebenfalls Ringisomorphismus.

'def':  $\overset{R}{\underset{\text{Ringm. räumen}}{\xrightarrow{\varphi}}} \overset{S}{\underset{\text{Ringm. räumen}}{\xrightarrow{\varphi^{-1}}}} \Rightarrow \overset{\varphi \circ \varphi^{-1}}{\text{Ringm. räumen}}$ .

Bsp:  $- R \rightarrow \text{Mat}_{2 \times 2}(R) \quad - \quad \mathbb{Z}_{12} \rightarrow \mathbb{Z}_{30}$  (wohldefiniert, da  $30 | 5 \cdot 12 = 60$ )

$$r \mapsto \begin{pmatrix} r & 0 \\ 0 & r \end{pmatrix}$$

Ringhomomorphismus

$$\Rightarrow \varphi: (\mathbb{Z}_{12}, +) \rightarrow (\mathbb{Z}_{30}, +)$$

Gruppenhomomorphismus

$$\text{Aber: } \varphi(1 \cdot 1) = \varphi(1) = S \cdot (1)_{30} = [S]_{30} \neq$$

$$[1]_{30} = \varphi(1) \cdot \varphi(1) = [S]_{30} \cdot [S]_{30} = [2S]_{30}$$

$\Rightarrow \varphi$  kein Ringhomomorphismus.

Bem (Übung):  $\varphi: R \rightarrow S$  Ringhomomorphismus  $\Rightarrow \varphi(R) \subseteq S$  Teilring

Bedeutung:  $(R / \text{Ker } (\varphi), +) \xrightarrow{\cong} (\varphi(R), +)$

Wir wollen: Ring und Ringisomorphismus, Indiz:  $(\mathbb{Z}/n\mathbb{Z}, +, \cdot) \cong (\mathbb{Z}_n, +, \cdot)$

## 6.5 Ideale und Faktorringe

Idee:  $\begin{array}{c} \text{Teilring} \\ \text{Ideale} \end{array} \begin{matrix} \cong \\ \cong \end{matrix} \begin{array}{c} \text{Untergruppen} \\ \text{Normalteile} \end{array}$

Def.  $I \subseteq R$  heißt Ideal, wenn  $\begin{array}{l} (1) a, b \in I \Rightarrow a - b \in I \\ (2) a \in I, r \in R \Rightarrow a \cdot r \in I \wedge r \cdot a \in I \end{array}$

"man ist gefangen im Ideal und kommt nicht mehr raus"

Bem. Dann ist  $I$  Teilring.

Def. Hier: Ideal = beidseitiges Ideal. Ist nur (1) erfüllt  $\Rightarrow$  Rechtideal  
bzw. (2) erfüllt  $\Rightarrow$  Linkideal.

Notation:  $\leq$  für Teilringe,  $\trianglelefteq$  für Ideale.

Bsp.:  $n\mathbb{Z} \trianglelefteq \mathbb{Z}$ .

Satz/Def.  $I \trianglelefteq R \Rightarrow R/I$  ist Ring, genannt Faktoring, durch  $(x+I) \cdot (y+I) := xy + I$ .

Beweis Einige nicht klar ist Verallgemeinerung.

Seien  $x^i, y^i, y^j \in R$  mit  $x+I = x^i+I, y+I = y^i+I$ .

$\Rightarrow$  ex.  $a \in I : x^i = x+a \Rightarrow x^i y^j = (x+a)(y+b) = xy + x^i y^j + ab \in I$

ex.  $b \in I : y^i = y+b$

$\Rightarrow x^i y^j + I = x^i y + I$ .  $\square$

Korollar.  $I \trianglelefteq R \Rightarrow \Psi: R \rightarrow R/I$  ist surjektiver Ringhomomorphismus  
 $r \mapsto r+I$  mit  $\text{Ker } (\Psi) = I$ .

Bew.  $\Psi(x) \cdot \Psi(y) = (x+I) \cdot (y+I) = xy + I = \Psi(xy) \quad \forall x, y \in R$ .  $\square$

Algebra

05.06.2010

$R$  kommutative Ring mit Eins,  $I \trianglelefteq R$ .

Korrespondenzsatz

$$\begin{array}{ccc} R & & R/I \\ | & & | \\ \{I \trianglelefteq R\} & \leftrightarrow & \left\{ \begin{array}{c} | \\ \overline{J} \trianglelefteq R/I \\ | \\ \{0+I\} \end{array} \right\} \end{array}$$

Noethersches Homomorphiesatz für Ringe

$\varphi: R \rightarrow S$  Ringhomomorphismus  $\Rightarrow \text{Ker } \varphi \trianglelefteq R$  und

$$\begin{array}{ccc} R & \xrightarrow{\varphi} & S \\ \text{surj.} \downarrow & \curvearrowright & \uparrow \text{inj.} \\ R/\text{Ker } \varphi & \xrightarrow{\cong} & \varphi(R) \end{array}$$

weiter alle Abbildungen Ringhomomorphismen sind.

Beweis. Sei  $a \in \text{Ker } \varphi, r \in R$ .

$\Rightarrow \varphi(a \cdot r) = \varphi(a) \cdot \varphi(r) = 0$

$\Rightarrow a \cdot r \in \text{Ker } \varphi$ . Damit  $\text{Ker } \varphi \trianglelefteq R$ .

Nun noch checken, dass  $\varphi$  Ringhomomorphismus ist:

$$x, y \in R \Rightarrow \varphi(x \cdot y + I) = \varphi((x+I)(y+I)) \stackrel{\text{Def}}{=} \varphi(x \cdot y) = \varphi(x) \varphi(y)$$

$$\stackrel{\text{Def}}{=} \varphi(x+I) \varphi(y+I). \quad \square$$

Bem.  $J \trianglelefteq S \Rightarrow \varphi^{-1}(J) \trianglelefteq R$ , aber  $I \trianglelefteq R \neq \varphi(I) \trianglelefteq S$

Bsp.:  $\varphi: \mathbb{Z} \hookrightarrow \mathbb{R}$ ,  $\mathbb{Z} \trianglelefteq \mathbb{Z}$ ,  $\varphi(\mathbb{Z}) = \mathbb{Z} \neq \mathbb{R}$ .

### Chinesischer Restsatz

Sei  $\text{ggT}(n, m) = 1 \Rightarrow \mathbb{Z}/n.m\mathbb{Z} \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$  (als Ringe)

Beweis.  $\varphi: \mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$   
 $z \mapsto ([z]_n, [z]_m)$

ist Ringhomomorphismus, mit  
 $\text{Ker } \varphi = \{ z \in \mathbb{Z} : [z]_n = [0]_n \wedge [z]_m = [0]_m \}$   
 $= \{ z \in \mathbb{Z} : n/z \text{ und } m/z \}$   
 $\text{ggT}(n, m) = \{ z \in \mathbb{Z} : n \cdot m | z \} = n \cdot m \cdot \mathbb{Z}$

(Isomorphieatz)

$\Rightarrow \mathbb{Z}/n\mathbb{Z} \cong \varphi(\mathbb{Z})$  als Ringe.  $|\varphi(\mathbb{Z})| = n \cdot m = |\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}|$ , damit  
 surj- und bijektiv.

### G.6 Hauptideale

R kommutativer Ring mit 1.

Bem./Def.  $A \subset R \Rightarrow \langle A \rangle := \left\{ \sum_{i \in I} r_i a_i : r_i \in R, a_i \in A, |I| < \infty \right\}$   
 heißt Erzeugnis von A.

$\langle A \rangle$  ist das kleinste Ideal, das A enthält (reduzieren).

Def.  $a \in R$ . Dann heißt  $\langle a \rangle = R \cdot a = \{r \cdot a \mid r \in R\}$  Hauptideal (principal ideal), das von  $a$  erzeugt wird.

Bem. -  $\langle 1 \rangle = R$ .

-  $\varphi: R \rightarrow S$  ist surjektiver Ringhomomorphismus, dann  $\varphi(\langle a \rangle) = \langle \varphi(a) \rangle$ .

Bsp.  $\langle 1 \rangle = \mathbb{Z} \hookrightarrow \mathbb{R}$ , aber  $\mathbb{Z} \neq \langle 1 \rangle = \mathbb{R}$ .

Def. R Hauptidealbereich (principal ideal domain), wenn R Integritätsbereich und jedes Ideal ist ein Hauptideal (kann man durch ein Element erzeugen).

Prop. R Körper  $\Leftrightarrow R$  hat nur  $\{0\}$  und R als Ideale

Beweis " $\Rightarrow$ "  $I \neq \{0\}, I \neq R \Rightarrow \exists x \in I, x \neq 0 \Rightarrow 1 = x^{-1} \cdot x \in I$

$\Rightarrow R = \langle 1 \rangle \subseteq I \Rightarrow R = I$ .

" $\Leftarrow$ " Sei  $x \in R, x \neq 0 \Rightarrow \langle x \rangle = R \Rightarrow 1 \in \langle x \rangle = R \cdot x$   
 $\Rightarrow \exists r \in R : 1 = r \cdot x$ .

Bsp.: Jeder Körper ist Hauptidealbereich;  $\mathbb{Z}$ ;  $\mathbb{K}[x]$

aber:  $\mathbb{Z}[x]$ ,  $\mathbb{K}[x,y]$  keine Hauptidealbereiche

### G.7 Charakteristik eines Rings

R kommutativer Ring mit 1.

$\frac{\text{Kern}}{\text{Ker } \varphi = \{1\}}$

Def.  $\text{char}(R) := \min \{ k \in \mathbb{Z}_{>0} : k \cdot 1 = 0 \} = 0(1)$  (Ordnung von 1 in  $(R, +)$ )  
(Charakteristik) oder 0, wenn kein solches  $k$  existiert (dieselbe so sinnvoller wäre)

Bsp.: -  $\text{char}(\mathbb{Q}) = 0$  (also kann es z.B. keine Isomorphismen dazu geben, da  $\varphi(1) = 1$  !)

für prim -  $\text{char}(\mathbb{Z}_n) = n$  (Charakteristik ist mehr als die unterscheidung zwischen verschiedenen Gruppen!)

-  $\text{char}(\mathbb{Z}_n[x]) = n$ , aber  $\mathbb{Z}_n[x]$  verschieden

Prop:  $R$  Integritätsbereich,  $\text{char}(R) > 0 \Rightarrow \text{char}(R)$  prim

Beweis:  $n := \text{char}(R)$  seienkt prim.  $\Rightarrow n = a \cdot b$  mit  $a, b \in \mathbb{Z}_{\geq 1}$  ( $1 < a, b < n$ )  
 $\Rightarrow 0 = n \cdot 1 = (a \cdot b) \cdot 1 = (a \cdot 1) \cdot (b \cdot 1) \Rightarrow a \cdot 1 = 0 \vee b \cdot 1 = 0 \quad \square$

## 7. Primideale und Maximalideale

Bem.  $a, b \in R$ . Dann gilt  $\langle a \rangle \subseteq \langle b \rangle \Leftrightarrow b | a$ . ( $R$  kommutativer 1-Ring.)  
 $= R \cdot a \qquad = R \cdot b$   
 $\uparrow$   
 $\exists r \in R : a = r \cdot b$

$\rightarrow$  Ideale verallgemeinern Teilbarkeitsbedingungen, Ideale hinter Idealen!

Def.  $I \subseteq R$  Primideal wenn  $I \neq R$  und  $(a \cdot b \in I \Rightarrow a \in I \vee b \in I) \forall a, b \in R$ .

Bsp:  $p \in \mathbb{Z}$  prim. Behauptung:  $\langle p \rangle$  Primideal.

Bew.  $p \neq \pm 1 \Rightarrow \langle p \rangle \neq \mathbb{Z}$ .

$a, b \in \mathbb{Z}$  mit  $a \cdot b \in \langle p \rangle \Rightarrow p | (a \cdot b) \Rightarrow p | a \vee p | b$   
 $\Rightarrow a \in \langle p \rangle$  oder  $b \in \langle p \rangle$ .  $\square$

Def.  $I \subseteq R$  maximales Ideal wenn  $I \neq R$  und  $I \subset J \subseteq R \Rightarrow J = R$ .

Bem.  $\{0\} \subseteq R$  ist maximal  $\Leftrightarrow R \neq \{0\}$  und  $\{0\}$  und  $R$  sind einzige Ideale  
 $\Leftrightarrow R$  Körper

Satz  $I \subseteq R$ .

(1)  $I$  prim  $\Leftrightarrow R/I$  Integritätsbereich

(2)  $I$  maximal  $\Leftrightarrow R/I$  Körper

Kor.  $I$  maximal  $\Rightarrow I$  prim

Bem.  $\{0\}$  Primideal  $\Leftrightarrow R$  Integritätsbereich

Beweis  $\pi: R \rightarrow R/I =: \bar{R}$  kanonischer Epimorphismus.

$r \mapsto r + I =: \bar{r}$   
 $-I \neq R \Leftrightarrow R/I \neq \{\bar{0}\} \Leftrightarrow \bar{0} \neq \bar{1}$

(1)  $a, b \in R : a \cdot b \in I \Leftrightarrow \bar{a} \cdot \bar{b} = \bar{0} = \bar{a} \cdot \bar{b}$   
 $a \in I \vee b \in I \Leftrightarrow \bar{a} = \bar{0} \vee \bar{b} = \bar{0}$

(2)  $\bar{R}$  Körper  $\Leftrightarrow$  nur  $\{\bar{0}\}$  und  $\bar{R}$  sind Ideale von  $\bar{R}$

sei  $R \neq I$ .  $\begin{matrix} \text{nur } I \text{ und } R \text{ sind Ideale von } R, \\ \text{die enthalten } \\ \text{diesesatz} \end{matrix} \Leftrightarrow I$  maximales Ideal von  $R$ .  $\square$

Bsp:  $\{0\} \subseteq \mathbb{Z}$  ist prim aber nicht maximal.

$\langle p \rangle \subseteq \mathbb{Z}$  Primideale, sogar maximale Ideale

Satz:  $R$  Hauptidealbereich,  $I \subseteq R$ ,  $I \neq \{0\}$ . Dann  $I$  prim  $\Leftrightarrow I$  maximal

Bew.  $I$  prim.,  $I \subset J \subseteq R$  als Annahme.  $\xrightarrow{R \text{ HIB}} I = \langle a \rangle, J = \langle b \rangle$  für  $a, b \in R$ .

$\Rightarrow b | a \Rightarrow$  ex.  $r \in R : a = b \cdot r$   $\xrightarrow{I \text{ prim}} r \in I$

$\Rightarrow \exists s \in R : r = s \cdot a \Rightarrow a = b \cdot s \xrightarrow{\text{Korrektur}} 1 = b \cdot s \Rightarrow 1 \in \langle b \rangle \Rightarrow$   $\text{Integritätsbereich} \Rightarrow R = J \quad \square$

Obige:  $K$  Körper. Dann

$K[x, y] / \langle y \rangle \cong K[x]$ ,  $\subseteq$  Integritätsbereich

Kor.  $K[x, y]$  kein Hauptidealbereich.

Bew.  $\{0\} \subset \langle y \rangle \subset \langle x, y \rangle \not\subseteq K[x]$ .

$\uparrow$  prim (Ding), aber nicht maximal und  $\neq \{0\}$ ,  $y$  zu Sezzen  $\square$

Integritätsbereich: (kommutativer, nullteilerfreier Ring mit 1  
 $(a \cdot b = 0 \Rightarrow a=0 \vee b=0)$ )

## 8. Quotientenkörper

Analog zu  $\mathbb{Z}$ . ( $\mathbb{Z}$  kann durch die Bildung  $\mathbb{Z}_n$  mit  $n \in \mathbb{N}$  von Brüchen zum Körper  $\mathbb{Q}$  erweitert werden).

Jeder Integritätsbereich  $R$  kann zu einem (Quotienten-)Körper erweitert werden.

Konstruktion: Sei  $R$  Integritätsbereich. Setze  $S := R \setminus \{0\}$ ,  $D := R \times S$  (kartesisches Produkt). Auf  $D = R \times S$  führen wir eine Relation  $\sim$  ein:

$(a, s) \sim (a', s') : \Leftrightarrow as' = a's$ . Die Relation  $\sim$  ist eine Äquivalenzrelation:

- reflexiv:  $(a, s) \sim (a, s) \Leftrightarrow as = as$

- symmetrisch:  $(a, s) \sim (a', s') \Leftrightarrow (a', s') \sim (a, s)$

- transitiv:  $(a, s) \sim (a', s')$  und  $(a', s') \sim (a'', s'')$

$\Rightarrow as' = a's$  und  $a's'' = s'a''$

$\Rightarrow as's'' = a'sa'' = sa's'' = ss'a''$

$\stackrel{R \text{ Integ.}}{\Rightarrow} s'(as'' - sa'') = 0$

$\stackrel{\text{stetlich}}{\Rightarrow} as'' - sa'' = 0 \quad (s'' \in R \setminus \{0\}) \Rightarrow as'' = a''s \Rightarrow (a, s) \sim (a'', s'')$

Def. 8.1 Wir bezeichnen die Äquivalenzklasse von  $(a, s)$  mit  $\frac{a}{s}$  und die Quotientenmenge  $\left\{ \frac{a}{s} \mid a \in R, s \in S \right\}$  mit  $\mathbb{Q}(R)$ .

$$\frac{a}{s} = \frac{a'}{s'} \Leftrightarrow (a, s) \sim (a', s') \Leftrightarrow as' = a's$$

Auf der Quotientenmenge  $\mathbb{Q}(R)$  definieren wir eine Addition und Multiplikation:

$$\frac{a}{s} + \frac{a'}{s'} := \frac{as' + a's}{ss'} \text{ und } \frac{a}{s} \cdot \frac{a'}{s'} := \frac{aa'}{ss'}.$$

Wohldefiniert? Angenommen  $\frac{a}{s} = \frac{b}{t}$  und  $\frac{a'}{s'} = \frac{b'}{t'}$ .

$$\text{Addition: } \frac{a}{s} + \frac{a'}{s'} \stackrel{?}{=} \frac{b}{t} + \frac{b'}{t'} \quad at = bs \text{ und } a't' = b's'$$

$$\Rightarrow ss'(bt' + b't) = ats' + a't's = tt'(as' + a's)$$

Multiplication: Übungsaufgabe

→ Die Quotientenmenge  $\mathbb{Q}(R)$  ist ein kommutativer Ring  $(\mathbb{Q}(R), +, \cdot)$  mit Einselement  $\frac{s}{s}$  und Nullelement  $\frac{0}{s}$ ,  $s \in S$ .

Beispiel:  $\mathbb{Z}$  ist ein  $(\mathbb{Q}(\mathbb{Z}), +, \cdot)$  Ring.

Satz 8.2 Für jeden Integritätsbereich  $R$  ist  $\mathbb{Q}(R)$  ein Körper – der Quotientenkörper von  $R$ .

$$\frac{s}{s} = 1 \in \mathbb{Q}(R), \quad \frac{0}{s} \neq \frac{s}{s} \in \mathbb{Q}(R), \quad \frac{a}{s} \cdot \frac{a'}{s'} = \frac{a}{s} \cdot \frac{a'}{s'} \text{ kommutativ}$$

$$\text{Für jedes } \frac{a}{s} \in \mathbb{Q}(R), a \neq 0 \quad \exists \frac{b}{t}: \frac{a}{s} \cdot \frac{b}{t} = \frac{0}{s} \cdot \frac{a}{s} = 1 \Rightarrow ab = st \Rightarrow \frac{b}{t} = \frac{s}{a}$$

Satz 8.3 "R ist ein Teilring des  $\mathbb{Q}(R)$ ". Seien  $\varphi, \psi$  wie oben.

$\varphi: R \rightarrow \mathbb{Q}(R)$  ist eine Einbettung von  $R$  in  $\mathbb{Q}(R)$  und es gilt:

$$a \mapsto \frac{a}{1}$$

$$\mathbb{Q}(R) = \left\{ \varphi(a) \varphi(s)^{-1} = \frac{a}{s} \mid a \in R, s \in S \right\}$$

$\varepsilon$  ist ein Homomorphismus:  $\varepsilon(a+b) = \frac{a+b}{1} = \frac{a}{1} + \frac{b}{1} = \varepsilon(a) + \varepsilon(b)$

$$\varepsilon(a \cdot b) = \frac{a \cdot b}{1} = \frac{a}{1} \cdot \frac{b}{1} = \varepsilon(a) \cdot \varepsilon(b)$$

$\varepsilon$  ist injektiv:  $\varepsilon(a) = \frac{a}{1} = \frac{a}{1} \Rightarrow a=0$ .

Bsp.: -  $\mathbb{Q} = \mathbb{Q}(Z)$

-  $R = F[x]$ ,  $F$  Körper,  $\mathbb{Q}(R) = \left\{ \frac{f(x)}{g(x)} \mid g(x) \neq 0 \right\}$  rationale Funktionenkörper

-  $R$  Körper:  $R \cong \mathbb{Q}(R)$ ,  
dem  $\varepsilon: R \rightarrow \mathbb{Q}(R)$ ,  $ab^{-1} \mapsto \frac{a}{b}$

Bem. -  $R \cong R' \Rightarrow \mathbb{Q}(R) \cong \mathbb{Q}(R')$   $R \hookrightarrow \mathbb{Q}(R)$

$$R \cong R' \Leftrightarrow \mathbb{Q}(R) \cong \mathbb{Q}(R') \\ \mathbb{Z} \cong \mathbb{Q} \Leftrightarrow \mathbb{Q}(Z) \cong \mathbb{Q}(Q)$$

-  $R$  SF Körper  
 $\Rightarrow \mathbb{Q}(R) \cong \{ab^{-1} \mid a \in R, b \in S\} \subseteq F$  (nach der universellen Eigenschaft)

### Die universelle Eigenschaft

Betrachten wir einen Homomorphismus  $\varphi: \mathbb{Q}(R) \rightarrow K$ ,  $K$  beliebiger Körper.

Dann  $\varphi\left(\frac{a}{s}\right) = \varphi\left(\frac{a}{s} \cdot \frac{1}{s}\right) = \varphi(\varepsilon(a)\varepsilon(s)^{-1}) = \varphi(\varepsilon(a)) \cdot \varphi(\varepsilon(s))^{-1}$ .

Alle Bilder  $\varphi\left(\frac{a}{s}\right)$  sind durch die Bilder  $\varphi(\varepsilon(a))$  und  $\varphi(\varepsilon(s))$  von Werten aus  $\varepsilon(R) \cong R$  bestimmt.

Universelle Eigenschaft:

$$\begin{array}{ccc} \mathbb{Q}(R) & \xrightarrow{\varphi} & K \\ \varepsilon \uparrow & \nearrow \varphi & \\ R & & \end{array} \quad \left. \begin{array}{l} \text{kommutiert.} \end{array} \right\}$$

Satz 8.4 Sei  $\varepsilon: R \rightarrow \mathbb{Q}(R)$  die Einbettung von  $R$  in  $\mathbb{Q}(R)$ .

Dann gibt es zu jedem Monomorphismus  $\varphi: R \rightarrow K$  genau einen Monomorphismus  $\tilde{\varphi}: \mathbb{Q}(R) \rightarrow K$ , der  $(1) \tilde{\varphi} \circ \varepsilon = \varphi$  erfüllt, nämlich

$$(2) \tilde{\varphi}: \frac{a}{s} \mapsto \varphi(a)\varphi(s)^{-1}, a \in R, s \in S.$$

Bew. (1)  $\tilde{\varphi}(\varepsilon(a)) = \varphi(a)$ ,  $\forall a \in R$ :  $\varepsilon(R) \cong R$ . Wenn  $a$  mit  $\varepsilon(a)$  identifiziert wird,

sehen wir, dass  $\tilde{\varphi}$  eine Fortsetzung von  $\varphi$  ist:  $\tilde{\varphi}|_R = \varphi$  (\*).

$$(2) \tilde{\varphi}\left(\frac{a}{s}\right) = \tilde{\varphi}\left(\varepsilon(a)\varepsilon(s)^{-1}\right) = \varphi(\varepsilon(a))\varphi(\varepsilon(s))^{-1} \stackrel{(1)}{=} \varphi(a)\varphi(s)^{-1}.$$

$\tilde{\varphi}$  Homomorphismus: Für alle  $\frac{a}{s}, \frac{a'}{s'}, \in \mathbb{Q}(R)$  gilt  $\tilde{\varphi}\left(\frac{a}{s} + \frac{a'}{s'}\right) = \tilde{\varphi}\left(\frac{as' + a's}{ss'}\right)$   
 $= \varphi(as' + a's)\varphi(ss')^{-1} = (\varphi(a)\varphi(s')) + (\varphi(a')\varphi(s'))\varphi(s)^{-1}\varphi(s')^{-1}$   
 $= \varphi(a)\varphi(s)^{-1} + \varphi(a')\varphi(s')^{-1} = \tilde{\varphi}\left(\frac{a}{s}\right) + \tilde{\varphi}\left(\frac{a'}{s'}\right)$   
Ähnlich für Multiplikation (Übung).

$\tilde{\varphi}$  injektiv:  $\tilde{\varphi}\left(\frac{a}{s}\right) = 0 \Rightarrow \varphi(a)\varphi(s)^{-1} = 0 \stackrel{s \neq 0}{\Rightarrow} \varphi(a) = 0 \stackrel{\varphi \text{ injektiv}}{\Rightarrow} a = 0 \Rightarrow \frac{a}{s} = 0$ .

### 9. Euklidische Bereiche

Def. 9.1 Ein Integritätsbereich  $R$  heißt ein euklidischer Ring, wenn es eine Abbildung  $\varphi: R \setminus \{0\} \rightarrow \mathbb{N} \setminus \{0\}$  mit den folgenden Eigenschaften gibt:

Zu beliebigen  $a, b \in R$  mit  $b \neq 0$  existieren  $q, r \in R$  mit  $a = q \cdot b + r$  und  $r = 0$  oder  $\varphi(r) < \varphi(b)$ . Eine solche Abbildung  $\varphi$  bezeichnet man als euklidische Norm.

Bsp.: -  $\mathbb{Z}$  ist ein euklidischer Ring mit gewöhnlicher Norm (Betrag).

- Polynomring  $K[x]$  für jeden Körper  $K$ , euklidische Norm

$$\varphi = \deg \text{ (Grad)}: |\varphi(f(x))| = \deg(f(x)).$$

- Der Ring  $\mathbb{Z}[i] = \{a+bi \mid a, b \in \mathbb{Z}\}$  mit Norm  $N: \mathbb{Z}[i] \setminus \{0\} \rightarrow \mathbb{N} \setminus \{0\}$   
ist ein euklidischer Ring. Bew.: ...

$$z \mapsto z\bar{z}$$

Bsp.: Für  $\alpha, \beta \in \mathbb{Z}[i]$  mit  $\beta \neq 0$  gilt:  $x = (\alpha\beta^{-1})\beta$  mit  $\alpha\beta^{-1} = x+iy \in \mathbb{C}$ ,  $x, y \in \mathbb{R}$ .

Es existieren  $u, v \in \mathbb{Z}$  mit  $|x-u| \leq \frac{1}{2}$  und  $|y-v| \leq \frac{1}{2}$

Für  $\tau := u+iv \in \mathbb{Z}[i]$  und  $\rho := \alpha - \tau\beta = ((x-u)+i(y-v))\beta \in \mathbb{Z}[i]$ .

$\sim \alpha = \tau\beta + \rho$ . Nach (\*) folgt:

$$\rho = 0 \text{ oder } \nu(\rho) = ((x-u)^2 + (y-v)^2) N(\beta) \stackrel{(*)}{=} \frac{x+iy - (u+iv)}{\alpha\beta^{-1} - \tau} \leq \frac{1}{2} N(\beta) < N(\beta).$$

- Sei  $F$  ein Körper,  $x, y \in F \Rightarrow x = qy$ , wobei  $q = xy^{-1}$ . (Körper sind euklidische Ringe)

Satz 9.2 Jeder euklidische Ring ist ein Hauptidealbereich.

Beweis:  $A \neq \langle 0 \rangle$  Ideal des euklidischen Rings  $(R, \varphi)$ . Es sei  $b \in A \setminus \{0\}$  mit kleinster Norm  $\varphi(b)$  gewählt. Natürlich  $\langle b \rangle \subseteq A$ .

$A \subseteq \langle b \rangle$ : Zu jedem  $a \in A$  existieren  $q, r \in R$  mit  $a = qb + r$  und  $r=0$  oder  $\varphi(r) < \varphi(b)$ . Wegen  $r = a - qb \in A$  und der Minimal-eigenschaft von  $b$ ,  $\varphi(r) < \varphi(b)$  ist nicht möglich für  $r \neq 0 \Rightarrow r=0$  und  $a = qb \in \langle b \rangle$ .  $\square$

"Einheiten sind Einheitenelemente der Norm."

Behauptung: Angenommen  $\varphi(ab) \geq \varphi(b) \quad \forall a, b \in R \setminus \{0\}$ . Dann  $x \in R^\times \Leftrightarrow \varphi(x) = \varphi(1)$

Beweis: " $\Rightarrow$ "  $x \cdot y = 1 \Rightarrow \varphi(1) = \varphi(x \cdot y) \geq \varphi(x) \geq \varphi(1) \Rightarrow \varphi(1) = \varphi(x)$ . (minimale Norm)  
 " $\Leftarrow$ "  $1 = qx+r$ . Falls  $r \neq 0 \Rightarrow \varphi(r) < \varphi(1) = \varphi(1)$   $\notin$  dem  $\varphi(1)$  ist minimal  
 $\Rightarrow r=0 \Rightarrow qx=1 \Rightarrow x \in R^\times$ .  $\square$

Bsp.:  $\mathbb{Z}[i]$  mit der Norm  $N: \mathbb{Z} \mapsto \mathbb{Z}$ . Wir können die Einheitselemente von  $\mathbb{Z}[i]$  finden:  $a+bi \in \mathbb{Z}[i]$  Einheit  $\Leftrightarrow (a+bi)(a-bi) = a^2+b^2=1$ .  
 $\sim$  Die Einheitselemente sind  $-i, -1, i, 1$ .

## 10. Primelemente und irreduzible Elemente

### 10.1 Assoziierte Elemente

Sei  $R$  Integritätsbereich.

Def.:  $a, b \in R$  sind assoziiert ( $a \sim b$ ), wenn  $a = ub$  mit  $u \in R^\times$   
 ( $a$  und  $b$  unterscheiden sich um eine Einheit).

Bsp.:  $7 \sim -7$  in  $\mathbb{Z}$        $x-1 \sim \frac{7}{5}(x-1)$  in  $\mathbb{Q}[x]$

Bem.:  $\sim$  ist Äquivalenzrelation.

Lemma:  $a \sim b \Leftrightarrow a | b$  und  $b | a$       ( $a | b \Leftrightarrow \exists q \in R: bq = a$ )  
Beweis: " $\Rightarrow$ "  $a = ub, u \in R^\times \Rightarrow b | a$   
 $b = u^{-1}a \Rightarrow a | b$   
 " $\Leftarrow$ "  $b = ua$  mit  $u \in R \Rightarrow b = uvb \Rightarrow 1, b = 0 \Rightarrow a = 0 \Rightarrow a \sim b$   
 $a = vb$  mit  $v \in R$   
 $2, b \neq 0 \Rightarrow$  (Körperz. reg. in Integritätsbereich)  
 $\Rightarrow 1 = uv \Rightarrow v \in R^\times = a \sim b$ .  $\square$

Kor.:  $a \sim b \Leftrightarrow \langle b \rangle \subseteq \langle a \rangle \wedge \langle a \rangle \subseteq \langle b \rangle$

$\Leftrightarrow \langle b \rangle \subseteq \langle a \rangle$  und  $\langle a \rangle \subseteq \langle b \rangle$

$\Leftrightarrow \langle a \rangle = \langle b \rangle$  (  $a \sim b$ , wenn beide das gleiche Ideal erzeugen )

### 10.2 Definitionen

Def.: -  $a \in R$  prim, wenn  $0 \neq a \notin R^\times$  und  $a | x \cdot y \Rightarrow a | x$  oder  $a | y$ .

$a \in R$  irreduzibel, wenn  $0 \neq a \notin R^\times$  und  $a = x \cdot y \Rightarrow x \in R^\times \vee y \in R^\times$   
 (Äquivalent:  $a = xy \Rightarrow a \sim x$  oder  $a \sim y$ ).

Bem.: In Körpern gibt es keine Prim- oder irreduzible Elemente (nach Def.).

Prop: prim  $\Rightarrow$  irreduzibel

Beweis:  $a$  prim. sei  $a = xy \Rightarrow a | xy \stackrel{\text{prim}}{\Rightarrow} a | x$  oder  $a | y$ . Ohne Einschränkung  $a | x$ .  
 Aber  $x \mid a$ , d.h.  $a \sim x$  und  $a$  irreduzibel.  $\square$

### 10.3 Prim- und irreduzible Elemente in Hauptidealbereichen

Prop. Sei  $R$  Hauptidealbereich. Dann sind irreduzible Elemente prim.

(also prim  $\Leftrightarrow$  irreduzibel)

Def. Seien  $a_1, \dots, a_n \in R$ : Element  $d \in R$  heißt größter gemeinsamer Teiler (ggT) von  $a_1, \dots, a_n$ , wenn

- (1)  $d | a_i$  für  $i = 1, \dots, n$
- (2)  $d' | a_i$  für  $i = 1, \dots, n \Rightarrow d' | d$

Lemma: Sei  $R$  Hauptidealbereich. Seien  $a, b \in R$ . Dann gilt:  $\langle a, b \rangle = \langle d \rangle \Leftrightarrow d \in \text{ggT}(a, b)$ .

(Insbesondere existieren größte gemeinsame Teiler.)

korrekte Schreibweise,  
nicht =

Bew. Alle ggT's sind assoziiert zueinander (in Integritätsbereichen).

Bew. Lemma  $\Rightarrow$  (1)  $a \in \langle d \rangle \Rightarrow d | a$ ,  $b \in \langle d \rangle \Rightarrow d | b$

$$(2) d' | a \wedge d' | b \Rightarrow a = d' \cdot x \wedge b = d' \cdot y$$

$$\text{Gilt: } d = f \cdot a + g \cdot b \Rightarrow d = (fx + gy) \cdot d' \Rightarrow d' | d.$$

$$\Leftarrow \text{R Hauptidealbereich} \Rightarrow \exists d' \in R \text{ mit } \langle a, b \rangle = d' \Rightarrow d' \in \text{ggT}(a, b)$$

$$\Rightarrow d \sim d' \Rightarrow \langle d \rangle = \langle d' \rangle = \langle a, b \rangle. \quad \square$$

(Kann mehrere  
ggT's geben!)

im Prinzip: Lemma von Bezout

Bew. von Prop. Sei  $R$  Hauptidealbereich,  $a$  irreduzibel,  $a \in R$ .

Sei  $a | x$  für  $x \in R$ . OBdA  $a \nmid x$ .  $\exists a \nmid y$ :  $a | y$ ,  $y \in \text{ggT}(a, x)$ .

Angenommen,  $d \notin R^\times$ :  $d | a \Rightarrow a = u \cdot d$  für  $u \in R$

$$a | x \Rightarrow x = v \cdot d \text{ für } v \in R.$$

$$\begin{aligned} & a \text{ irreduzibel} \quad \stackrel{d \notin R^\times}{\Leftrightarrow} u \in R^\times \Rightarrow d = u^{-1}a \Rightarrow x = vu^{-1}a \Rightarrow a | x \quad \text{↯} \\ & \Rightarrow d \in R^\times \quad \text{Lemma} \quad \langle a, x \rangle = \langle d \rangle = R = \langle 1 \rangle \Rightarrow 1 = r \cdot a + s \cdot x \text{ für } r, s \in R \\ & \Rightarrow y = r \cdot a \cdot y + s \cdot x \cdot y \stackrel{a | xy}{\Rightarrow} a | y. \quad \square \end{aligned}$$

### 10.4 Wichtiges Beispiel

Sei  $R = \mathbb{Z}[\sqrt{-3}] = \{a + b\sqrt{-3} \mid a, b \in \mathbb{Z}\} \subset \mathbb{C} \quad (\Leftrightarrow R \text{ ist Integritätsbereich})$ .

Beh.  $1 + \sqrt{-3}$  ist irreduzibel, aber nicht prim (in  $R$ ).

Bew. Definiere  $N: \mathbb{Z}[\sqrt{-3}] \rightarrow \mathbb{Z}_{\geq 0}$  (Normabbildung)

$$z = a + b\sqrt{-3} \mapsto a^2 + 3b^2 = (a+b\sqrt{-3})(a-b\sqrt{-3}) = z \cdot \bar{z} = |z|^2$$

$$= N(x \cdot y) = N(x) \cdot N(y) \quad \forall x, y \in R.$$

$$1 + \sqrt{-3} = xy \text{ für } x, y \in R \Rightarrow 4 = N(1 + \sqrt{-3}) = N(x) \cdot N(y)$$

- 1.) Ohne Einschränkung  $N(x) = 1 \Rightarrow x \in R^\times \quad \in \mathbb{Z}_{\geq 0}$
- 2.)  $N(x) = N(y) = 2 \Rightarrow$  für  $x = a + b\sqrt{-3}$  gilt  $2 = a^2 + 3b^2$  mit  $a, b \in \mathbb{Z}$  ↯

$\Rightarrow 1 + \sqrt{-3}$  irreduzibel.

$$N(1 + \sqrt{-3}) = 4 = (1 + \sqrt{-3})(1 - \sqrt{-3}) = 2 \cdot 2.$$

Ang.  $1 + \sqrt{-3}$  prim, dann  $(1 + \sqrt{-3}) \mid z \cdot \bar{z} \Rightarrow 1 + \sqrt{-3} \mid z$ .

$$\Rightarrow z = (1 + \sqrt{-3})(a + b\sqrt{-3}) \text{ mit } a, b \in \mathbb{Z}$$

$$= \underbrace{(a - 3b)}_{= \bar{a}} + \underbrace{(a + b)\sqrt{-3}}_{= 0} = \Rightarrow 2 = a - 3b, 0 = a + b$$

$$\Rightarrow 2 = a - 3(-a) = 4a$$

$$\Rightarrow a = \frac{1}{2} \notin \mathbb{Z} \quad \text{↯}$$

Bsp.  $\mathbb{Z}[\sqrt{-3}]$ ; Bew.  $1 + \sqrt{-3}$  irreduzibel, nicht prim

Korollar  $\mathbb{Z}[\sqrt{-3}]$  ist kein Hauptidealbereich. (Sost wäre  $1 + \sqrt{-3}$  prim)

Bem.  $\text{ggT}(4, 2(1 + \sqrt{-3})) = 0$ : ggT existiert nicht. "keine kleinen Eigenheiten"

Beweisidee: Ang. die  $\text{ggT}(4, 2(\lambda + \sqrt{-3})) = d \mid d$  und  $(1 + \sqrt{-3}) \mid d$   
Rechnung gibt Widerspruch (oben).  $\square$

Bem.  $\text{ggT}(2, x) = \{1\}$  in  $\mathbb{Z}[x]$ , aber  $\langle 2, x \rangle \neq \mathbb{Z}$  "super-misser Ring"  
 $\Rightarrow \langle 2, x \rangle \neq \langle \text{ggT}(2, x) \rangle \Rightarrow \mathbb{Z}[x]$  kein Hauptidealbereich

## 11. Faktorielle Ringe

### 11.1 Polynomringe

Falls  $R$  kommutativer Ring ist, ist  $R[x]$  (Polynome über  $R$ ) ebenfalls kommutativer Ring.

Bsp.  $\mathbb{Z}_4[x], (\mathbb{Z}[\sqrt{-3}])[x]$

Universelle Eigenschaft von Polynomringen:

$\varphi: R \rightarrow S$  Ringhomomorphismus,  $\alpha \in S \Rightarrow$  existiert  $\bar{\varphi}: R[x] \rightarrow S$  Ringhomomorphismus,  
(einheitiger)  
mit  $x \mapsto \alpha$ .  
so dass  $\begin{array}{ccc} R & \xrightarrow{\varphi} & S \\ \downarrow & \nearrow \bar{\varphi} & \\ R[x] & & \end{array}$  kommutiert. Dem:  $\bar{\varphi}\left(\sum_{i=0}^n \lambda_i x^i\right) = \sum_{i=0}^n \varphi(\lambda_i) \alpha^i$ .  
Bew.: Check, dass Ringhomomorphismus.

Bem. Sei  $K$  Körper.

(1) Wenn  $f(x) \in K[x]$  eine Nullstelle  $\alpha \in K$  hat und  $\deg(f(x)) \geq 0$ ,  
dann  $f(x) = g(x)(x - \alpha)$ .

(Bew.)  $K[x]$  ist euklidischer Ring  $\Rightarrow \exists q(x), r(x) \in K[x]$  mit  $\deg r(x) < \deg(x - \alpha) = 1$   
oder  $r(x) = 0$  s.d.  $q(x) = g(x)(x - \alpha) + r(x)$   
 $\Rightarrow 0 = f(x) = g(x) \cdot 0 + r(x) = r(x)$   
 $\Rightarrow r(x)$  ist Konstante, also  $0 = r$  und  $f(x) = g(x)(x - \alpha)$ .  $\square$

(2) Folgerung: Ist  $\deg f(x) > 0$ , so hat  $f(x)$  höchstens  $\deg f(x)$  Nullstellen.  
Ist  $\deg f(x) \in \{2, 3\}$ , so ist  $f(x)$  irreduzibel über  $K$  (Körper!).  
geh.  $f(x)$  zweie Nullstelle hat.

(Bew.) Wenn falls irreduzibel, hat ein Faktor Grad 1.)

Aufgabe:  $(x^2 + 1)^2$  hat keine Nullstelle über  $\mathbb{R}$ , ist aber reduzibel (Grad 4!).

Über  $\mathbb{C}$ : Alle Polynome faktorisieren in Linearfaktoren,

Über  $\mathbb{R}$ : nur in Linearfaktoren, aber in Polynome vom Grad  $\leq 2$ .

Beweisidee: Ist  $\alpha \in \mathbb{C}$  Nullstelle von  $f(x) \in \mathbb{R}[x]$ , dann  $\bar{\alpha}$  (Konjugiert)

auch Nullstelle von  $f(x)$ . ( $\star$ )

$\Rightarrow (x - \alpha)(x - \bar{\alpha}) \leftarrow$  Linearfaktore fassen in Paaren auf  
 $= x^2 - (\alpha + \bar{\alpha})x + \alpha\bar{\alpha} \in \mathbb{R}[x]$ .

$\sum_{i=0}^n a_i x^i \in \mathbb{R} \quad \overline{a_i x^i} \in \mathbb{R}$

ad ( $\star$ ): Die Verenzuation  $-: \mathbb{C} \rightarrow \mathbb{C}$  ist Ringautomorphismus.

$\left( \begin{array}{l} \text{I)} \quad \mathbb{C}[x] \rightarrow \mathbb{C}[x] \text{ ist Ringhomomorphismus.} \\ \text{II)} \quad \sum a_i x^i \mapsto \sum \bar{a}_i x^i \end{array} \right)$

Sei  $f(x) = \sum_{i=0}^n a_i x^i \Rightarrow f(\bar{x}) = \sum_{i=0}^n a_i \bar{x}^i = \overline{\sum_{i=0}^n a_i x^i} = \overline{f(x)} = \bar{0} = 0$ .

Bsp.  $\forall z \in (\mathbb{Z}_8^\times): \alpha(z) \geq 2 \quad (\mathbb{Z}_8^\times = \{1, 3, 5, 7\}) \Rightarrow z^2 - 1 = 0 \quad \forall z \in \mathbb{Z}_8^\times$

$\Rightarrow x^2 - 1 \in \mathbb{Z}_8[x]$  hat 4 Nullstellen, aber Grad 2.

$(x^2 - 1) = (x + 1)(x - 1) = (x - 3)(x - 5) \rightsquigarrow$  Faktoriellring nicht einheitlich.

## 11.2 Hauptidealbereiche sind faktorielle Ringe

Def.  $R$  ist faktorieller Ring (UFD, unique factorization domain), wenn  $R$  Integritätsbereich und

Existenz (i)  $0 \neq x \notin R^\times \Rightarrow$  existiert  $p_1, \dots, p_n \in R$  irreduzibel mit  $x = p_1 \cdots p_n$   
 Eindeutigkeit (ii) In (i), falls ex.  $q_1, \dots, q_m \in R$  irreduzibel mit  $x = q_1 \cdots q_m$ ,  
 dann  $m = n$  und ex.  $\sigma \in \text{Sym}(\{1, \dots, n\})$ :  $p_i \sim q_{\sigma(i)}$  assoziiert  
Bsp.  $6 = 2 \cdot 3 = 3 \cdot 2 = (-2)(-3) = (-3)(-2)$

Satz: Hauptidealbereiche sind faktorielle Ringe. ( $\forall x \in R^\times$  kann alles in Primbereich zerlegen)

Beweis: Sei  $0 \neq x \notin R^\times$ . Ang.  $x$  ist reduzibel.

Für (i):  $\Rightarrow$  ex.  $x_1, y_1 \in R$ :  $x = x_1 \cdot y_1$  und  $x_1, y_1 \notin R^\times$ ,  $x_1 \neq x$ .  
 $\Rightarrow \langle x \rangle \subsetneq \langle x_1 \rangle \subseteq R$ .

Wdh.  $\rightsquigarrow \langle x \rangle \subsetneq \langle x_1 \rangle \subsetneq \langle x_2 \rangle \subsetneq \dots \subsetneq R$ ,  
 angenommen, Kette bricht nicht ab.

Def.  $I := \bigcup_{i=1}^{\infty} \langle x_i \rangle$ , Beweis  $I \subseteq R$ .

Bew.  $a, b \in I \Rightarrow \exists i, j: a \in \langle x_i \rangle, b \in \langle x_j \rangle$

ohne Einschränkung  $i \neq j \Rightarrow \langle x_i \rangle \subset \langle x_j \rangle \Rightarrow a + b \in \langle x_j \rangle \subset I$ .

( $\Rightarrow$  Hauptidealbereich)  $\Rightarrow$  ex.  $w \in R$ :  $I = \langle w \rangle$

$\Rightarrow$  ex.  $i: w \in \langle x_i \rangle \Rightarrow \langle w \rangle \subseteq \langle x_i \rangle$

$\Rightarrow I = \langle x_i \rangle$   $\wedge$  zu Annahme: Kette bricht nicht ab

$\Rightarrow x = x_1 y_1 = x_2 y_2 y_1 = \dots = x_i y_i \cdots$

ex.  $p_1 \in R$  irreduzibel mit  $x = p_1 q_1$  und  $q_1 \in R$

Falls  $q_1$  reduzibel:  $q_1 = p_2 \cdot q_2 \cdots q_1 \in \langle q_2 \rangle \subsetneq \langle q_2 \rangle \subsetneq \dots \subsetneq R$  wieder

$\Rightarrow x = p_1 \cdot p_2 \cdots p_i \cdot q_i$ , alle irreduzibel  $\Rightarrow$  (i).

Für (ii):  $x = p_1 \cdots p_n = q_1 \cdots q_n$ , alle irreduzibel

$p_1 \mid x \Rightarrow$  (irr. = prim, da  $R$  Hauptidealbereich)

ex.  $\alpha(1): p_1 \mid q_{\alpha(1)} \Rightarrow p_1 \sim q_{\alpha(1)}$   
 ... (Rest analog).  $\square$

(formal Induktionsbeweis).  $\square$

## 11.3 Alternative Charakterisierung von faktoriellen Ringen

Satz: Sei  $R$  Integritätsbereich. Äquivalent:

(1)  $R$  ist faktorieller Ring

(2) (i) gilt und prim = irreduzibel

(3)  $0 \neq x \notin R^\times \Rightarrow$  ex.  $p_1 \cdots p_n$  prim =  $x = p_1 \cdots p_n$

Beweis: Obige mit folgendem Lemma:

Lemma:  $R$  ist faktorieller Ring, dann ist prim = irreduzibel.

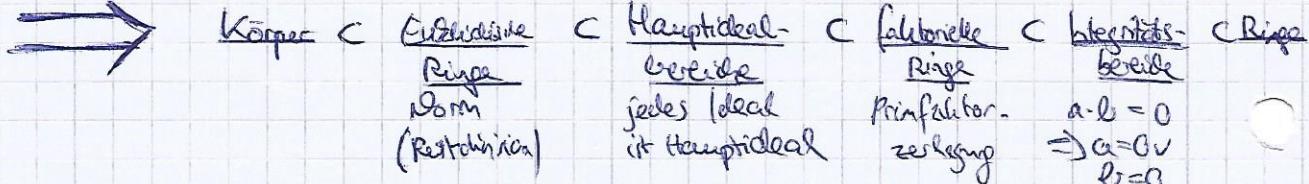
Bew. Sei  $p \in R$  irreduzibel. Seien  $a, b \in R$ :  $p \mid (a \cdot b) \Leftrightarrow (p \mid a) \vee (p \mid b)$  (primärer Zerlegung in irreduzible Elemente, die nicht assoziiert sind)

$\Leftrightarrow p \mid a$  oder  $p \mid b$  (p teilt in

$\{p_1, \dots, p_n\}$  oder  $\{q_1, \dots, q_m\}$  auf)

$\rightarrow p \mid a$  oder  $p \mid b \Rightarrow p$  prim.

Kor.  $\mathbb{Z}[\sqrt{-3}]$  ist kein faktorieller Ring.



11.4 Lemma von Gauß

Satz von Gauß:  $R$  faktorieller Ring  $\Rightarrow R[x]$  faktorieller Ring (z.B.  $\mathbb{Z}[x]$ )

Sei  $R$  faktorieller Ring. Jedes  $\text{ggT}$ 's existiert wegen Primfaktorzerlegung.

Def.  $r_1, \dots, r_k$  heißen teilerfremd, wenn  $\text{ggT}(r_1, \dots, r_k) \subseteq R^\times$   
 $\Leftrightarrow$  kein irreduzibles Element teilt  $r_1, \dots, r_k$ .

Def.  $p(x) \in R[x]$  heißt **primiv**, wenn  $\deg p(x) > 0$  und die Koeffizienten sind teilerfremd.

Bsp:  $4x+2 \in \mathbb{Z}[x]$  ist nicht primiv,  $4x+3$  schon,  
aber  $4x+2 \in \mathbb{Q}[x]$  ist primiv (in  $K[x]$ ,  $K$  Körper, sind alle nicht-konstanten Polynome primiv!). ( $\rightsquigarrow$  Wenn  $\text{ggT} \rightarrow$  teilerfremd  $\Rightarrow K^\times = K$ )  
 $(\text{ggT}(\dots, \dots) \subseteq K^\times = K)$

Bem.  $\forall p(x) \in R[x]$  mit  $\deg p(x) > 0$

$\exists c \in R$  Inhalt (Content) von  $p(x)$  weil  $p^*(x) \in R[x]$  primiv  
s.d.  $p(x) = c \cdot p^*(x)$

Bsp:  $4x+2 = 2(2x+1) = (-2)(-2x-1)$

Bem.) Inhalt und primitiver Teil sind eindeutig nur bis auf assoziierte.

Frage:  $(c \cdot \underbrace{p^*(x)}_{\text{primiv}}) \cdot (d \cdot \underbrace{q^*(x)}_{\text{primiv}}) = c \cdot d \cdot (\underbrace{p^*(x) \cdot q^*(x)}_{\text{primiv } (3)})$

Lemma von Gauß: "primiv  $\cdot$  primiv = primiv"

Beweis  $h(x) = f(x) \cdot g(x)$  mit  $f(x), g(x) \in R[x]$  primiv.

Auf, nicht primiv  $\Rightarrow$  ex.  $p$  Primideal in  $R$  mit  $p \mid h(x)$ .  
Betrachte Reduktionsringhomomorphismus:

$$R[x] \longrightarrow (R/\langle p \rangle)[x]$$

$$\sum_i x^i \longmapsto \sum_i (r_i + \underbrace{\langle p \rangle}_{=: I}) \cdot x^i.$$

$p$  prim  $\Leftrightarrow \langle p \rangle$  Primideal  $\Rightarrow \overline{R} = R/\langle p \rangle$  Integritätsbereich.

$\Rightarrow \overline{h(x)} = \overline{f(x) \cdot g(x)} \not\in p \quad p \nmid \overline{f(x)}, p \nmid \overline{g(x)}$ , da primiv.

$\not\in \overline{I} \quad \Rightarrow \overline{0} = \overline{h(x)} = \overline{f(x) \cdot g(x)} \not\in \overline{I} \quad \text{I zu } \overline{R} \text{ Integritätsbereich.} \quad \square$

Algebra

21.06.2018

Bem. Sei  $R$  Integritätsbereich. Sei  $p \in R$ . Dann gilt:  
 $\{0\} \neq \langle p \rangle$  Primideal  $\Leftrightarrow p$  prim

Sei  $R$  faktorieller Ring.

Bem.  $p(x) \in R[x]$  irreduzibel  $\Leftrightarrow \begin{cases} p(x) \in R \text{ irreduzibel, wenn } \deg p(x) = 0 \\ p(x) = c \cdot p^*(x), c \in R, p^*(x) \text{ irreduzibel, sonst primiv, sonst primiv, sonst primiv} \end{cases}$

11.5 Satz von Gauß - Beweisideen

Sei  $R$  faktorieller Ring.

Sei  $Q := Q(R)$  Quotientenkörper von  $R$ . Wir wissen:  $Q[x]$  ist Hauptidealbereich, also auch faktorieller Ring mit wie früher faktoriell.

$$\text{Bsp. } 3x + \frac{15}{2} = \frac{1}{2}(6x+15) = \underbrace{\frac{3}{2}}_{\in \mathbb{Q}^\times} \underbrace{(2x+5)}_{\in \mathbb{Z}[x] \text{ primiv}}$$

(Existenz) Lemma (ohne Beweis):  $f(x) \in \mathbb{Q}[x] \Rightarrow f(x) = \frac{a}{b} f^*(x)$  für  $a \in \mathbb{R}, b \in \mathbb{R} \setminus \{0\}$ ,

(Endeitheit) Sei  $f(x) = \frac{c}{d} g^*(x)$  für  $c \in \mathbb{R}$ ,  $d \in \mathbb{R} \setminus \{0\}$ ,  $\text{ggT}(c, d) = 1$ ,  $g^*(x) \in \mathbb{R}[x]$  primiv  
 $\Rightarrow c \sim a$  in  $\mathbb{R}$ ,  $d \sim b$  in  $\mathbb{R}$ ,  $f^*(x) \sim g^*(x)$  in  $\mathbb{R}[x]$ .

Prop.  $f(x) \in \mathbb{R}[x]$  primiv,  $\deg f(x) > 0$ .

Dann gilt:  $f(x)$  irreduzibel in  $\mathbb{R}[x] \Leftrightarrow f(x)$  irreduzibel in  $\mathbb{Q}[x]$

Bew. " $\Rightarrow$ " Ang.  $f(x)$  irreduzibel über  $\mathbb{R}$  und reduzibel über  $\mathbb{Q}$ .

Lemma  $f(x) = \left(\frac{a}{c} g^*(x)\right) \left(\frac{c}{d} h^*(x)\right)$  mit Eigenschaften wie im Lemma.

$$\text{von Gauß} = \frac{a \cdot c}{b \cdot d} \underbrace{\left(g^*(x) + h^*(x)\right)}_{\substack{\deg > 0 \\ \text{primiv in } \mathbb{R}[x]}}$$

Lemma  $f(x) \sim g^*(x) h^*(x)$  in  $\mathbb{R}[x]$   $\square$

Einführung  $f(x)$  irreduzibel über  $\mathbb{Q}$ . Sei  $f(x) = g(x)h(x)$  mit  $g(x), h(x) \in \mathbb{R}[x]$ .  
 $\text{durch Einführung } \deg g(x) = 0 \Rightarrow g(x) \in \mathbb{R}$ .  
 $f(x)$  primiv  $\Rightarrow g(x) \in \mathbb{R}^\times$ .  $\square$

Satz von Grusß benutzt Lemma und Proposition.

Idee: Faktorisierung über  $\mathbb{Q}$  ergibt Faktorisierung über  $\mathbb{R}$ .

## 11.6 (Irreduzibilitätskriterium von Eisenstein)

Satz: Sei  $R$  Integritätsbereich mit Quotientenkörper  $\mathbb{Q}$ .

Sei  $p(x) = \sum_{i=0}^n a_i x^i \in R[x]$ ,  $\deg p(x) > 0$ .

Falls ein Primideal  $p \subset R$  existiert mit

$p \mid a_0, p \mid a_1, \dots, p \mid a_{n-1}, p \nmid a_n, p^2 \nmid a_0$ ,  
dann ist  $p(x)$  nicht zerlegbar in Polynome in  $R[x]$  vom Grad  $> 0$ , siehe unten.  $\circledast$

Beweis: Definiere  $-: R \rightarrow \bar{R} := R/\langle p \rangle$  kanonischer Epimorphismus.

$$r \mapsto \bar{r} := r + \langle p \rangle$$

$$\begin{array}{ccc} R & \xrightarrow{\quad r \mapsto \bar{r} \quad} & \bar{R}[x] \\ \downarrow r \mapsto \bar{r} & \nearrow \bar{x} & \downarrow \bar{x} \\ R[x] & \xrightarrow{\quad x \mapsto \bar{x} \quad} & \end{array}$$

universelle  
Eigenschaft existiert Ringhomomorphismus:  
 $\Rightarrow -: R[x] \rightarrow \bar{R}[x]$   
 $\sum_{i=0}^n a_i x^i \mapsto \sum_{i=0}^n \bar{a}_i \bar{x}^i$

Ang.  $p(x) = s(x) \cdot t(x)$  mit  $s(x), t(x) \in \bar{R}[x]$ ,  $\deg s(x) > 0, \deg t(x) > 0$ .

$$\Rightarrow \bar{p}(\bar{x}) = \bar{s}(\bar{x}) \cdot \bar{t}(\bar{x}) \in \bar{R}[\bar{x}], \bar{p}(\bar{x}) = \bar{a}_n \bar{x}^n.$$

Hier:  $\bar{R}$  ist ein Integritätsbereich.  $\text{Obwohl } \bar{s}(\bar{x}) = \bar{a}_s \bar{x}^s, \bar{t}(\bar{x}) = \bar{a}_t \bar{x}^t \text{ mit } 0, s, t \in \mathbb{Z}$ ,  
und  $\bar{s} \cdot \bar{t} = \bar{a}_n \neq \bar{0}$ ,  $s+t=n, s \neq n \neq t, s, t > 0$ .  $\text{Leitkoeffizient}$

(Ang.)  $t=n \Rightarrow s=0 \Rightarrow \deg \bar{s}(\bar{x}) \geq 0, \deg s(x) > 0 \Rightarrow p \mid LC(s(x))$ ,

$$\Rightarrow \underline{LC(p(x))} = LC(s(x)) \cdot LC(t(x)) \quad \square$$

$\Rightarrow p \mid \underline{\text{const}(s(x))}$ ;  $p \mid \text{const}(t(x)) \Rightarrow p^2 \mid \text{const}(p(x)) = a_0$ .  $\square$   $\square$

konstante Koeffizient

$\circledast$  Dann ist  $p(x)$  nicht zerlegbar in Polynome in  $R[x]$  vom Grad  $> 0$ .

Let  $R$  faktorieller Ring, dann ist  $p(x)$  irreduzibel in  $\mathbb{Q}[x]$ . (!)

in  $\mathbb{Q}[x]$

Bsp.:  $x^5 + 4x^3 + 2x + 2 \in \mathbb{Z}[x]$  ist irreduzibel über  $\mathbb{Q}$  (nimm  $p=2$ ).

Bsp.:  $x^n - 2 \in \mathbb{Z}[x]$  ist irreduzibel über  $\mathbb{Q}$   $\forall n \in \mathbb{N}_{>1}$ .

## 12. Körpererweiterungen

### 12.1 Kroneckers Satz

Bsp.: Betrachte  $x^2 + 1 \in \mathbb{R}[x]$ .

$$\mathbb{R} \xrightarrow{\quad} \mathbb{C} \quad \text{Universelle Eigenschaft ex. } \varphi: \mathbb{R}[x] \rightarrow \mathbb{C}$$

$\downarrow \quad \downarrow$   
 $\mathbb{R}[x] \xrightarrow{\quad}$   $\mathbb{C}$  Eigenschaft ex.  $\varphi: \mathbb{R}[x] \rightarrow \mathbb{C}$   
 $p(x) \mapsto p(i)$

so dass  $\varphi$  Ringhomomorphismus ist.  $\varphi$  ist der Ausweitungshomomorphismus.

-  $\varphi$  ist surjektiv. Denn  $\varphi(a+bx) = a+b\cdot i$  ( $a, b \in \mathbb{R}$ )

-  $\ker \varphi = \{ p(x) \in \mathbb{R}[x] : p(i) = 0 \} = \langle m(x) \rangle$  mit  $m(x) \in \mathbb{R}[x]$ ,  $m(x)$  Polynom im  $\ker \varphi$  von minimalem Grad.

$$\Rightarrow \frac{\mathbb{R}[x]}{\ker \varphi} = \frac{\mathbb{R}[x]}{\langle m(x) \rangle} \cong \mathbb{C} \text{ Körper.}$$

$\Rightarrow \langle m(x) \rangle$  ist maximales Ideal,  $\langle m(x) \rangle \neq \{0\}$   
(HIB Prinzipalideal)

$\Rightarrow m(x)$  ist prim  $\Leftrightarrow$  irreduzibel

$$x^2 + 1 \in \ker \varphi \Rightarrow m(x) \mid x^2 + 1 \quad \begin{matrix} \text{irreduzibel} \\ \text{irreduzibel} \end{matrix} \Rightarrow m(x) \sim x^2 + 1$$

$$\Rightarrow \ker \varphi = \langle m(x) \rangle = \langle x^2 + 1 \rangle$$

$$\Rightarrow \boxed{\frac{\mathbb{R}[x]}{\langle x^2 + 1 \rangle} \cong \mathbb{C}}$$

HIB = Hauptideal - Bereich

FR = faktorieller Ring

Def.  $K, L$  Körper mit  $K \subseteq L$  Teilring (oder  $K \rightarrow L$  injektiver Ringhomomorphismus). Dann heißt  $L$  Körpererweiterung von  $K$ . mit  $1_K = 1_L$

Satz (Kronecker):  $f(x) \in K[x]$ ,  $\deg f(x) > 0$ .

Dann existiert eine Körpererweiterung  $L$ , in der  $f(x)$  eine Nullstelle hat.

Beweis: Sei  $p(x) \in K[x]$  irreduzibel ( $\deg p(x) > 0$ ) mit  $p(x) \mid f(x)$

(denn  $K[x]$  ist faktorieller Ring weil man kann  $f(x)$  faktorisieren).

$$\Rightarrow I := \langle p(x) \rangle \text{ maximales Ideal}$$

(denn:  $p(x)$  irreduzibel  $\Leftrightarrow$  prim  $\rightarrow \langle p(x) \rangle \neq \{0\}$  Prinzipalideal  $\stackrel{\text{HIB}}{\Rightarrow}$  maximales Ideal)

$$\Rightarrow L := \frac{K[x]}{I} \text{ Körper.}$$

(Körper haben nur zwei Ideale.)

$\Rightarrow \Psi: K \rightarrow L$  Ringhomomorphismus ist injektiv. (Denn: Sont wäre)

$$c \mapsto c + I \quad \ker \Psi \neq \{0\} \quad \text{Ker } \Psi = K \Rightarrow 1 + I = I$$

$$\Rightarrow 1 \in I \Rightarrow I = K[x] \quad \text{I} \neq K[x], \text{ da max. Ideal}$$

$\Rightarrow K \subset L$  Körpererweiterung (Identifiziere  $K$  mit  $\Psi(K)$ .)

$$\Rightarrow K[x] \subset L[x]$$

Sei  $u := x + I \in L$ , (das soll die Nullstelle sein).

$$\text{Sei } p(x) = \sum_{i=0}^n c_i x^i \text{ mit } c_i \in K =$$

$$= \sum_{i=0}^n (c_i + I) x^i \text{ in } L[x]$$

Rechengesetze für Ideale

$$\begin{aligned} \exists p(u) &= 0_L \\ p(u) &= \sum_{i=0}^n (c_i + I) \cdot u^i = \sum_{i=0}^n (c_i + I)(x + I)^i = (\sum_{i=0}^n c_i x^i) + I \\ &= p(x) + I = I = 0_L. \quad \square \end{aligned}$$

### 12.2 Algebraische und transzendentale Elemente

Def. Sei  $L \supseteq K$  Körpererweiterung. Dann heißt  $u \in L$  algebraisch über  $K$ , wenn  $\exists p(x) \neq 0$ ,  $p(x) \in K[x]$  mit  $p(u) = 0_L$ . Andernfalls heißt  $u$  transzendent über  $K$ .

Bsp. -  $i$  ist algebraisch über  $\mathbb{Q} = x^2 + 1 \in \mathbb{Q}[x]$

-  $\sqrt{2}$  ist algebraisch über  $\mathbb{Q} = x^2 - 2 \in \mathbb{Q}[x]$

-  $e, \pi$  ist transzendent über  $\mathbb{Q}$ ,  $e + \pi$  ist unbekannt. (!)

Def.  $L \supseteq K$ ,  $u \in L$  algebraisch über  $K$  wenn ex.  $p(x) \neq 0$ ,  $p(x) \in K[x]$ :  $p(u) = 0$ .  
sonst  $u$  transzendent.

Def.  $u_1, \dots, u_n \in L$ :  $K(u_1, \dots, u_n)$  kleinster Teilkörper von  $L$ , der  $K$  und  $u_1, \dots, u_n$  enthält.

Z.B.  $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\} \subseteq \mathbb{R}$

$$(m_a, \sqrt{2})(x) = x^2 - 2 \quad K = \mathbb{R}, \zeta = \mathbb{C}, u = i, m_{i,u}(x) = x^2 + 1, \deg \zeta(x) = 2$$

Prop. (Def.) Sei  $u \in L$  algebraisch über  $K$ . Dann ex. ein eindeutiges normiertes  
(koeffizienten 1) irreducibles Polynom in  $K[x]$  mit Nullstelle  $u$ ,

genannt Minimalpolynom  $m_{K,u}(x)$  über  $K$ .

Der Grad  $d := \deg m_{K,u}(x)$  heißt Grad von  $u$  über  $K$ .

Weiterhin: (1)  $f(x) \in K[x]$  mit  $f(u) = 0 \Rightarrow m_{K,u}(x) \mid f(x)$ .

$$\begin{aligned} (2) \quad K[u] &:= \{p(u) : p(x) \in K[x]\} = \left\{ \sum_{i=0}^{d-1} a_i u^i : a_i \in K \right\} \\ &= K(u), \text{ da } K(u) \text{ ist kleinster Teilkörper, der } K \text{ und } u \text{ enthält} \end{aligned}$$

$$(3) \quad K[x]/\langle m_{K,u}(x) \rangle \cong K(u) \rightarrow \text{als Ringe und } K\text{-Vektorräume}$$

$$(\text{vgl. } \mathbb{R}[x]/\langle x^2 + 1 \rangle \cong \mathbb{C}[x])$$

$$(4) \quad K(u) \text{ ist } K\text{-Vektorraum der Dimension } d \text{ mit Basis } 1, u, \dots, u^{d-1}.$$

Beweis: (1)  $K[x] \rightarrow L$

$p(x) \mapsto p(u)$  Ausweitungskomorphismus mit  $\ker \Phi = \langle m_{K,u}(x) \rangle$ , wobei  $m_{K,u}(x)$  minimalen Grad in  $\ker \Phi$  hat und normiert gewählt worden ist.

$$\Rightarrow K[x]/\langle m_{K,u}(x) \rangle \cong \Phi(K) \subseteq L \Rightarrow \langle m_{K,u}(x) \rangle \text{ Primideal in } K[x]$$

$\Rightarrow \langle m_{K,u}(x) \rangle$  ist minimales Ideal

Hauptidealbeh.  $\Rightarrow K[x]/\langle m_{K,u}(x) \rangle$  Körper

Primideal  $\neq \{0\} \Rightarrow m_{K,u}(x)$  prim  $\Rightarrow$  irreducibel

$$(1) \checkmark \quad (2) \quad \Phi(K) = K(u) = K(u) \quad \text{einfacher Ring / Polynomring}$$

(3) Sei  $p(x) \in K[x]$ .  $\Rightarrow$  Divisionsalgorithmus  $\Rightarrow p(x) = q(x) \cdot m_{K,u}(x) + r(x)$  für  $q(x), r(x) \in K[x]$ ,  $r(x) = 0$  oder  $\deg r(x) < d$ ;  $= q(x) \cdot m_{K,u}(x) + \sum_{i=0}^{d-1} \lambda_i x^i$   
 $\Rightarrow p(x) + I = \sum_{i=0}^{d-1} \lambda_i x^i + I$ .

(4) Nur zu zeigen nach (3):  $1, u, \dots, u^{d-1}$  linear unabhängig.  $K[x]/\langle m_{K,u}(x) \rangle$

Resultat:  $1+I, x+I, \dots, (x+I)^{d-1}$  linear unabhängig in  $K[x]/\langle m_{K,u}(x) \rangle$ .

$$\text{Ang. } \left( \sum_{i=0}^{d-1} \lambda_i x^i + I \right) = 0 \Leftrightarrow m_{K,u}(x) \mid \sum_{i=0}^{d-1} \lambda_i x^i$$

Gilt nur für  $\lambda_0 = \dots = \lambda_{d-1} = 0$ .  $\square$

## Algebra

28.06.2018

Wollen  $K \subseteq L$ ,  $u \in L$  alg. über  $K$ .

$$\Rightarrow K[x]/\langle m_{K,u}(x) \rangle \cong K[u] = K(u) \subseteq L$$

mit  $K$ -Basis  $1, u, u^2, \dots, u^{d-1}$  für  $d := \dim_K K(u) < \infty$

Bem. sei  $u \in L$  transzendent über  $K$ . Dann ist  $K[x] \rightarrow L$  ein injektiver Ringhomomorphismus.  $p(x) \mapsto p(u)$  (Ausweitungskomorphismus)  
(da es nur für das Nullpolynom 0 wird).

$$\Rightarrow K[x] \cong \left\{ \sum_{i=0}^n \lambda_i u^i : n \text{ beliebig} \right\} =: K(u) \text{ kein Körper}$$

$$K(u) = \left\{ \frac{\sum_{i=0}^n \lambda_i u^i}{\sum_{j=0}^m \mu_j u^j} \right\} \subseteq L$$

$$\text{Hier: } K(u) \cong \mathbb{Q}(K(u)) \cong \mathbb{Q}(K[x]) = \left\{ \frac{p(x)}{q(x)} \right\}_{q(x) \neq 0}$$

Insbes.  $\dim_K K(u) = \infty$ .

Körper der rationalen Funktionen über  $K$

Bsp.:  $u = \sqrt[4]{2} \in \mathbb{R}_{>0}, K = \mathbb{Q}$

$\deg_K(u) = 1$  (mit  $p(x) = x - u$ ),  $\mathbb{R}(u) = \mathbb{R}$ )

aber was ist  $\deg_{\mathbb{Q}}(u)$ ?

Kandidat wäre  $x^4 - 2$ . Ist faktisch Minimalpolynom da irreduzibel

nach Eisenstein.  $(\mathbb{Q}(\sqrt[4]{2})) = \{ \lambda_0 + \lambda_1 \sqrt[4]{2} + \lambda_2 \sqrt[4]{2}^2 + \lambda_3 \sqrt[4]{2}^3; \lambda_0, \lambda_1, \lambda_2, \lambda_3 \in \mathbb{Q} \}$   
 $\Rightarrow \mathbb{Q}[x]/\langle x^4 - 2 \rangle$

Idealer Körper größer  $\mathbb{Q}$  der  $\sqrt[4]{2}$  enthält.

Was ist nun  $(1 + \sqrt[4]{2})^{-1}$ ? Benötigt euklidischer Algorithmus:

$$x^4 - 2 = (x^3 - x^2 + x - 1)(1+x) - 1$$

$$\Rightarrow 1 = (x^3 - x^2 + x - 1)(1+x) - \cancel{(x^4 - 2)} + \langle x^4 - 2 \rangle$$

$$+ \langle x^4 - 2 \rangle \Rightarrow \langle x^3 - x^2 + x - 1 \rangle = (1+x + \langle x^4 - 2 \rangle)^{-1}$$

$$\Rightarrow (\sqrt[4]{2})^{-1} = (\sqrt[4]{2})^3 \cdot \cancel{\sqrt[4]{2}} + \sqrt[4]{2} - 1$$

~ mit algebraischen Elementen kann man wieder reden.

$$\sqrt[4]{2} \leftrightarrow x + \langle x^4 - 2 \rangle$$

### 12.3 Endliche und algebraische Körpererweiterungen

Def.  $L \supseteq K$  endliche Körpererweiterung, wenn  $|L:K| := \dim_K L < \infty$ .

Bsp.  $\mathbb{C} \supseteq \mathbb{R}$  endliche Körpererweiterung.

Von:  $u \in L$  algebraisch/ $K$  ( $\Leftrightarrow K(u) \supseteq K$  endliche (J. Dimension vorliegt))

d.h. man muss noch Minimalpolynom rufen, Körpererweiterung

um algebraisch zu zeigen.

Möglich offensichtlich:  $u_1$  algebraisch/ $K$  weil  $u_2$  algebraisch/ $K$ ,  $u_1 + u_2$  algebraisch/ $K$ ?

Zg. Entscheidende Bedeutung:

$$\underbrace{K \subseteq E \subseteq L}_{E:K < \infty, |L:E| < \infty} \text{ Körpererweiterung} \Rightarrow |L:K| = |L:E| \cdot |E:K| < \infty.$$

$$E:K < \infty, |L:E| < \infty$$

Anwendungen:

(1)  $u \in L$  algebraisch/ $K$ ,  $L/K$  endlich  $\Rightarrow \deg_K(u) = |L(u):K| \mid |L:K|$  Beweis:  $E = L(u)$

(2)  $u_1, \dots, u_n \in L$  algebraisch/ $K \Rightarrow K(u_1, \dots, u_n)$  endlich/ $K$  mit  $|K(u_1, \dots, u_n):K| \leq \prod_{i=1}^n \deg_K(u_i) < \infty$

Bew. Induktion nach  $n$ :  $n=1$  ✓

$$(n-1) \rightarrow n: |K(u_1, \dots, u_n):K| = |K(u_1, \dots, u_{n-1}, u_n):K(u_1, \dots, u_{n-1})| \cdot |K(u_n):K|$$

$$= E(u_n) = L \quad \begin{matrix} \text{Ind. von } E(u_n) \\ \leq \prod_{i=1}^{n-1} \deg_K(u_i) \end{matrix}$$

$$|E(u_n):E| = \deg_E(u_n) = \deg_{K(u_1, \dots, u_{n-1})}(u_n) \mid m_{K(u_1, \dots, u_{n-1}), u_n}(x)$$

$$\leq \deg_{K(u_1, \dots, u_{n-1})}(x) \quad \begin{matrix} \text{Linear Algebra wg. } \rightarrow \\ \text{Unter-}K\text{-Vektorraum} \end{matrix}$$

$$= \deg_K(u_n) \quad \square$$

(3)  $K \subseteq L$  Körpererweiterung.

$\Rightarrow \{u \in L \mid u \text{ algebraisch}/K\}$  Teilkörper von  $L$

Bew.  $u_1, u_2 \in L$ , algebraisch/ $K$   $\Rightarrow K(u_1, u_2)$  endlich/ $K$

$$K(u_1+u_2), K(u_1 \cdot u_2), K(u_1^{-1})$$

Linear Algebra wg.  $\rightarrow \Rightarrow K(u_1+u_2), K(u_1 \cdot u_2), K(u_1^{-1})$  endlich/ $K$

Unter- $K$ -Vektorraum  $\Rightarrow u_1+u_2, u_1 \cdot u_2, u_1^{-1}$  algebraisch/ $K$ .  $\square$

Bsp.  $\mathbb{Q} \subseteq A := \{z \in \mathbb{C} : z \text{ algebraisch}/K\} \subsetneq \mathbb{C}$  algebraischer Abschluss von  $\mathbb{Q}$ .

$$A \supseteq \mathbb{Q}(\sqrt[n]{2}) \supsetneq \mathbb{Q} \Rightarrow \dim_{\mathbb{Q}} A = \infty.$$

ferner,  $A$  ist abzählbar unendlich (es gibt abzählbar viele algebraische Zahlen).

Bew. "entscheidende Bedeutung":  $K \subseteq E \subseteq L$ . Sei  $e_1, \dots, e_m \in E$ -Basis von  $E$ ,

$\overbrace{m \in \omega}^{K \subseteq E \subseteq L} \quad f_1, \dots, f_n \in L$ -Basis von  $L$ .

Bsp.  $\{e_i, f_j\}_{i,j}$  ist  $K$ -Basis von  $L$ .

$$z \in L \Rightarrow \exists x^i \sum_{j=1}^n \lambda_j f_j \in E: z = \sum_{j=1}^n \lambda_j f_j$$

$$\Rightarrow \forall j \exists p_j \in K: \lambda_j = \sum_{i=1}^m p_i e_i$$

$$\Rightarrow z = \sum_{i=1}^m \sum_{j=1}^n p_i e_i f_j$$

$$\sum_{i,j} \mu_{ij} e_{ij} = 0 = \sum_j (\sum_i \mu_{ij} e_i) f_j \Rightarrow \forall j \sum_i \mu_{ij} e_i = 0 \Rightarrow \forall j \forall i: \mu_{ij} = 0. \square$$

(Eine Algebra ist zugleich Ring und Unterraum.)

Def.  $L \supseteq K$  algebraisch (Körpererweiterung) /  $K$ , wenn jedes Element in  $L$  algebraisch /  $K$ .  
Bew.  $L \supseteq K$  endlich ( $K \Rightarrow$  algebraisch /  $K$ ) ( $\Leftarrow$  gilt nicht, siehe A oben)  
(denn:  $\# L = \#(K(u)) \cdot \# K$  mit  $\# K < \infty$ )

Prop.  $\begin{cases} L \\ E \\ K \end{cases}$  algebraisch  $\Rightarrow \begin{cases} L \\ E \\ K \end{cases}$  algebraisch

Bew. Sei  $u \in L \Rightarrow m_{E,u}(x) = \sum_{i=0}^n e_i x^i \in K(e_0, \dots, e_n)[x] =: G$   
 $\Rightarrow u$  algebraisch /  $G \Rightarrow |G(u):G| < \infty \Rightarrow e_0, \dots, e_n$  algebraisch /  $K$   
 $\Leftrightarrow |G:K| < \infty \stackrel{\text{Bsp.}}{\Rightarrow} |K(u):K| \leq |G(u):K| = |G(u):G| \cdot |G:K| < \infty$   
 $\Rightarrow u$  algebraisch /  $K$ .

Bsp. -  $|\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}(\sqrt{2})| \stackrel{\mathbb{Q}(\sqrt[4]{2})}{=} ? \Rightarrow$  entscheidende  $2 \cdot 2 = 4$   
 $= |\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}| = \frac{4}{2} = 2$   
-  $|\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}| = ? \leq \deg \mathbb{Q}(\sqrt{2}) \cdot \deg \mathbb{Q}(\sqrt{3}) = 2 \cdot 2 = 4$

$$\begin{pmatrix} \mathbb{Q}(\sqrt[4]{2}, \sqrt{3}) \\ \mathbb{Q}(\sqrt[4]{2}) \\ \mathbb{Q} \end{pmatrix} \leq 4$$

$$\Rightarrow \text{Ang. } |\mathbb{Q}(\sqrt[4]{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})| = 1 \quad (L \supseteq K \Rightarrow L = K)$$

$$\Rightarrow \mathbb{Q}(\sqrt[4]{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2})$$

$$\Rightarrow \sqrt{3} \in \mathbb{Q}(\sqrt{2})$$

$$\Rightarrow |\mathbb{Q}(\sqrt[4]{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})| = 2 \cdot 2 = 4 \quad |\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}| = 4.$$

$$- \deg \mathbb{Q}(\sqrt{2} + \sqrt{3}) = |\mathbb{Q}(\sqrt{2} + \sqrt{3}) : \mathbb{Q}| \stackrel{\text{Bsp.}}{\leq} |\mathbb{Q}(\sqrt{2} + \sqrt{3}) : \mathbb{Q}| \leq 4$$

$$\in \{1, 2, 4\}$$

$$\text{Bsp. } \mathbb{Q}(\sqrt{2} + \sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$$

$$(\sqrt{2} + \sqrt{3})(\sqrt{2} - \sqrt{3}) = 2 \cdot 3 = -1 \Rightarrow \sqrt{2} - \sqrt{3} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$$

$$\Rightarrow (\sqrt{2} - \sqrt{3}) + (\sqrt{2} + \sqrt{3}) = 2\sqrt{2} \in \mathbb{Q}(\sqrt{2} + \sqrt{3}) \Rightarrow \frac{1}{2} \cdot 2\sqrt{2} = \sqrt{2} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$$

$$\Rightarrow \sqrt{3} = ((\sqrt{2} + \sqrt{3}) - \sqrt{2}) \in \mathbb{Q}(\sqrt{2} + \sqrt{3}) \Rightarrow \mathbb{Q}(\sqrt{2} + \sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3}) \quad \square$$

## 12.4 Zerfällungskörper

Sei  $f(x) \in K[x]$ .

Def.  $L \supseteq K$  Erweiterungskörper heißt Zerfällungskörper (splitting field) von  $f(x)$  über  $K$ , wenn  
-  $f(x) = C \cdot \prod_{i=1}^n (x - \alpha_i)$  mit  $C, \alpha_1, \dots, \alpha_n \in L$   
-  $L = K(\alpha_1, \dots, \alpha_n)$  gilt.  
(dieser kleinste Körper, der die Nullstellen von  $f$  enthält)

## Algebra

03.07.2018

Satz. (1) Zerfällungskörper existieren.  
(2)  $L$  Zerfällungskörper von  $f(x) \in K[x] \Rightarrow |L:K| \leq (\deg f(x))!$   
(3) Ist  $L$  wie in (2) gegeben, dann existiert ein Ringisomorphismus  
r.d.  $L \xrightarrow{\sim} L'$  kommutiert.

Bew. von (1), und (2) per Induktion nach  $n := \deg f(x)$ .

$n=1$ :  $L = K$

$n \geq 1$ : Sei  $p(x)$  irreduzibler Faktor von  $f(x)$  in  $K[x]$ .  
Sei  $L' \supseteq K$  mit  $\alpha_n \in L'$ :  $p(\alpha_n) = 0$ , ohne Eindeindung  $L' = K(\alpha_n)$

$\exists g(x) \in K[x]: p(x) = g(x)(x - \alpha_n) \Rightarrow$  ex.  $f(x) = g(x)(x - \alpha_n)$ ,  $\deg g(x) = n-1$

$\Rightarrow$  ex.  $L = L'(\alpha_1, \dots, \alpha_{n-1})$  und  $g(x) = \underset{\in L'}{\underbrace{c \cdot \prod_{i=1}^{n-1} (x - \alpha_i)}}$   
 $= K(\alpha_1, \dots, \alpha_n)$  Zerfällungskörper für  $f(x)$ .

# Algebra

03.07.2018

Bew.  $|K:K| = |L:L'| \cdot |L':L| \leq n!$ .. (Übung)  $\square$   
 (3) direkter Beweis  $i.i \leq (n-1)!$

Bsp.  $f(x) = x^3 - 2 \in \mathbb{Q}[x]$  irreduzibel

Sei  $\alpha := \sqrt[3]{2} \in \mathbb{R} \supseteq \mathbb{Q} \Rightarrow |\mathbb{Q}(\alpha)| = 3$ ,  $f(x) = m_{\mathbb{Q}(\alpha)}(x)$   
 Ist  $\mathbb{Q}(\alpha)$  Zerfällungskörper für  $f(x)$ ?

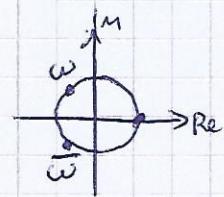
Nein! Denn  $\omega = e^{i\frac{\pi}{3}}$ ,  $\bar{\omega} = e^{-i\frac{\pi}{3}}$ , 1 sind 3-te Einheitswurzeln  
 $\Rightarrow [\alpha, \alpha\omega, \alpha\omega^2]$  sind komplexe Nullstellen von  $f(x)$ .

Aber:  $\mathbb{Q}(\alpha, \alpha\omega, \alpha\omega^2) \not\subseteq \mathbb{R}$ , aber  $\mathbb{Q}(\alpha) \subseteq \mathbb{R}$ .

$\Rightarrow \mathbb{Q} \subsetneq \mathbb{Q}(\alpha) \subsetneq \mathbb{Q}(\alpha, \alpha\omega, \alpha\omega^2)$ , also  $? = 2$

$\frac{3}{3} \quad \frac{2}{2} \quad \Rightarrow$  Grad des Zerfällungskörpers ist 6  
 Satz (2):  $\leq 3! = 6$

$\mathbb{Q}(\alpha, \omega)$  (wird zu zwei Nullstellen erweitert)



## 13. Endliche Körper

### 13.1 Existenz & Eindeutigkeit $i_1(F_i)$

Sei  $F$  endlicher Körper. Erinnerung:  $\text{char}(F) = p$  Primzahl

$\Rightarrow \{0, 1, \dots, (p-1) \cdot 1\}$  ist Teilkörper von  $F$ , genannt Primkörper von  $F$ ,

$K := \frac{\mathbb{Z}}{p} \cong \mathbb{Z}_p$  isomorph zu  $\mathbb{Z}_p$ .

$(\mathbb{Z} \rightarrow F \text{ ist Ringhomomorphismus mit Kern } = p\mathbb{Z}, \text{ Bild } = K, )$   
 $z \mapsto z \cdot 1 \text{ mit Monomorphiesatz folgt } K \cong \mathbb{Z}_p$

$\Rightarrow F$  ist  $K$ -Vektorraum der Dimension  $|F:K| = n$ .

Wähle  $K$ -Basis von  $F$ :  $f_1, \dots, f_n \Rightarrow F = \{ \sum_{i=1}^n \lambda_i f_i : \lambda_i \in K \} \cong K^n$  als

$|F| = p \cdot \dots \cdot p = p^n$ ,  $\Rightarrow$  Jeder endliche Körper hat  $n$ -dimensionale  $K$ -Vektorraum

Primzahlpotenzordnung. (Es gibt keinen Körper der Ordnung 6.)

**Satz** (1) Für jede Primzahl  $p$  und  $n \in \mathbb{N}_{\geq 1}$  existiert ein Körper mit  $p^n$  Elementen.

(2) Jeder solche Körper ist einzigartig bis auf Isomorphismen und heißt Galois-Körper  $GF(p^n)$  der Ordnung  $p^n$ . (Es gibt genau einen Körper der Ordnung 4.)

**Bsp.**  $p^n = 4 = 2^2$ :  $x^2 + x + 1$  irreduzibel in  $\mathbb{Z}_2[x]$  (die beiden Nullstellen in  $\mathbb{Z}_2$ )  
 $\Rightarrow L = \mathbb{Z}_2[x]/\langle x^2 + x + 1 \rangle$  ist Erweiterungskörper von  $\mathbb{Z}_2$  mit  $|L:\mathbb{Z}_2| = 2$ .  
 $\Rightarrow |L| = 4 \Rightarrow L \cong GF(4)$

**Bsp.**  $p^n = 8 = 2^3$ ,  $K := \mathbb{Z}_2$ ,  $n=3$ .  $x^3 + x^2 + 1$  irreduzibel in  $\mathbb{Z}_2[x] \Rightarrow GF(8) \cong \mathbb{Z}_2[x]/\langle x^3 + x^2 + 1 \rangle$

**Bew.** **Hauptbeobachtung:** Ist  $F$  Körper mit  $|F| = p^n$ , so ist  $F$  Zerfällungskörper von  $x^{p^n} - x$  über  $\mathbb{Z}_p$ . Sogar mehr:  $F = \{ \alpha \in F : \alpha^{p^n} = \alpha \}$

**Bew.** Sei also  $u \in F$ ,  $u \neq 0$ .  $\underbrace{(F \setminus \{0\})}_{\text{Gruppe}}$  mit  $|F \setminus \{0\}| = p^n - 1$  folgt  $u^{p^n - 1} = 1$  (Lagrange/Kleiner Satz von Fermat)

$$\Rightarrow u^{p^n} = u \Rightarrow u^{p^n} - u = 0$$

$\Rightarrow x^{p^n} - x$  hat  $p^n$  viele Nullstellen in  $F$ , also faktorisiert  $x^{p^n} - x$  in  $F$  in Linearfaktoren und  $F = \{ \alpha_1, \dots, \alpha_n \} = \mathbb{Z}_p(\alpha_1, \dots, \alpha_n)$   $\square$

**Kor.** (2) gilt. (Eindeutigkeit)

**Bew.** Seien  $F, \tilde{F}$  Körper mit  $|F| = |\tilde{F}| = p^n \Rightarrow \text{char}(F) = \text{char}(\tilde{F}) = p$   
 und  $K_F \cong \mathbb{Z}_p \cong K_{\tilde{F}}$   $\xrightarrow{\text{Beweis}}$   $F$  und  $\tilde{F}$  Zerfällungskörper von  $x^{p^n} - x$  über  $\mathbb{Z}_p$   
 $\xrightarrow{\text{Endlichheit}} \tilde{F} \cong F$ .  $\square$

**Bew. für (1):** Definiere  $F$  als einen Zerfällungskörper von  $x^{p^n} - x$  über  $\mathbb{Z}_p$  (existiert).

Wir zeigen, dass  $|F| = p^n$ . Beh.  $\{ \alpha \in F : \alpha^{p^n} = \alpha \}$  ist Teilkörper von  $F$ . ( $\supseteq \mathbb{Z}_p$ )

**Bew.** Seien  $\alpha, \beta \in \{ \alpha \in F : \alpha^{p^n} = \alpha \} \Rightarrow (\alpha + \beta)^{p^n} \stackrel{(1)}{=} \alpha^{p^n} + \beta^{p^n}$  (folgt aus dem Binomialkoeffizienten)  
 $\xrightarrow{\text{Freshman's Dream}} \dots$  abgefahren.  $= \alpha + \beta \Rightarrow$  Koeffizienten weiter getestet

$$(Idee: (\alpha + \beta)^4 = \alpha^4 + 4\alpha^3\beta + 6\alpha^2\beta^2 + 4\alpha\beta^3 + \beta^4)$$

getestet von  $p$

Ker.  $F = \{\alpha \in F : \alpha^{p^n} = \alpha\}$

Es fehlt noch zu  $x^{p^n} - x$  hat keine mehrfachen Nullstellen in  $F$ .

Bew. Ang.  $x^{p^n} - x = (x-\alpha)^2 \cdot g(x)$  in  $F[x]$

$$\rightarrow \Rightarrow \frac{\partial}{\partial x} (x^{p^n} - x) = \frac{\partial}{\partial x} ((x-\alpha)^2 \cdot g(x)) = 2(x-\alpha)g(x) + (x-\alpha)^2 \cdot g'(x)$$

$$p^n \cdot x^{p^n-1} - 1 \text{ setze } \alpha \text{ ein} \Rightarrow p^n \cdot \alpha^{p^n-1} - 1 = 0 \text{ in } \mathbb{Z}_p \quad \square$$

"Der Trick ist ableiten-  
lich weiß, das  
ist ganz sinnvoll  
in einer Algebra-  
Vorlesung..."

### 13.2 Teilkörper von $GF(p^n)$

Sei  $F := GF(p^n)$ .

Satz Für jeden positiven Teiler  $m$  von  $n$  existiert ein eindeutiger Teilkörper mit  $p^m$  Elementen in  $F$ , nämlich  $\{\alpha \in F : \alpha^{p^m} = \alpha\}$ .  
Es existieren keine weiteren Teilkörper.

Bsp.:  $GF(p^6)$

$$\begin{matrix} GF(p^2) \\ GF(p^3) \\ GF(p) = \mathbb{Z}_p \end{matrix}$$

Bew.  $L \subseteq F$  Teilkörper  $\Rightarrow \mathbb{Z}_p = K_F \leq L \leq F$

$$\Rightarrow m := |\mathbb{Z}_p| / |K_F| = n \quad (\text{zeigt "keine weiteren" Bedingung}).$$

$$\Rightarrow |L| = p^m \Rightarrow L \models \{ \alpha \in L : \alpha^{p^m} = \alpha \} = \{ \alpha \in F : \alpha^{p^m} = \alpha \} \quad (\text{denn } x^{p^m} - x \text{ hat } \leq p^m \text{ Nullstellen})$$

### Algebra

05.07.2013

Satz  $m \mid n \Rightarrow$  existiert eindeutiger Teilkörper von  $F = GF(p^n)$  mit  $p^m$  Elementen, nämlich  $\{\alpha \in F : \alpha^{p^m} = \alpha\}$ . Seien erfüllen beide weiteren Teilkörper.

Bew.  $L \subseteq F$  Teilkörper  $\Rightarrow L = \{\alpha \in F : \alpha^{p^m} = \alpha\}, |L| = p^m$  s.o.

Fehlt noch: Existenz

Sei  $m \mid n$ . Def.  $L := \{\alpha \in F : \alpha^{p^m} = \alpha\}$  ist Teilkörper (s.o.)

Z.z.  $x^{p^m} - x$  faktorisiert über  $F$  (denn dann sind alle  $p^m$  verschiedene (s.o.) Nullstellen in  $F$ , damit  $|L| = p^m$ .)

Beh.  $(x^{p^m} - x) \mid (x^{p^n} - x)$  in  $\mathbb{Z}_p[x]$  (damit auch in  $\mathbb{Z}_p[x]$ )

Aquivalent  $(x^{p^m-1} \cdot 1) \mid (x^{p^n-1} - 1) \quad (*)$

Triv.  $z^l - 1 = (z-1)(1+z+z^2+\dots+z^{l-1})$

Sei  $n=m \cdot k$  mit  $k \in \mathbb{N}$

$$z=p^m \Rightarrow (p^m)^k - 1 = (p^m-1)(1+p^m+(p^m)^2+\dots+(p^m)^{k-1})$$

$$l=k \quad (p^m-1) \Rightarrow (p^m-1) \mid (p^n-1) \text{ in } \mathbb{Z}$$

Sei  $p^{n-k} - 1 = (p^m-1) \cdot r$  mit  $r \in \mathbb{N}$ .

$$z = x^{p^{n-k}}, l=r \Rightarrow (x^{p^{n-k}} - 1)^r - 1 = (x^{p^{m-1}} - 1)(1+(x^{p^{m-1}})^{r-1}+\dots+(x^{p^{m-1}})^{r-1}) \Rightarrow (*) \quad \square$$

### 13.3 Multiplikative Struktur

Satz  $(GF(p^n), \cdot)$  ist zyklisch.

Ker.  $GF(p^n) = \{0, 1, u, u^2, \dots, u^{p^n-2}\} = \mathbb{Z}_p(u)$  für ein  $u \in GF(p^n)$ .

Bew. Für jedes  $n \in \mathbb{N}_>$  existiert ein irreducibles Polynom vom Grad  $n$  in  $\mathbb{Z}_p[x]$ .

$GF(p^n)$  hat multiplikativer Erzeuger  $u \Rightarrow GF(p^n) = \mathbb{Z}_p(u)$

$\Rightarrow \text{Grad } Z_{p,u}(x)$  hat Grad  $|Z_p(u) : \mathbb{Z}_p| = n$ .  $\square$

Bew. Beh. Sei  $G$  endliche Untergruppe von  $(F^\times, \cdot)$  für einen Körper  $F$ .

Dann ist  $G$  zyklisch.

Wdh.  $G$  ist dann endliche abelsche Gruppe  $\xrightarrow{\text{z.v. normform}}$  ex.  $g \in G : o(g) = \text{lkg}(o(g))$  y.E.G.  
 $\Rightarrow o(g) \mid o(g) \forall g \in G \Rightarrow o(g) = 1 \forall g \in G$   
 $\Rightarrow$  alle Elemente in  $G$  sind Nullstellen von  $x^{o(g)} - 1 \in F[x]$  y.v. aller Ordnungen  
 $\Rightarrow |G| \leq o(g) \leq \text{Grad } \text{Lagrange} \Rightarrow |G| = o(g) \Rightarrow G = \langle g \rangle \quad \square$

"super  
einfaches  
Beweis"

13.4 Endliche Zerfällungskörper

Prop.  $K$  endlicher Körper,  $f(x) \in K[x]$  irreduzibel.

Sei  $L$  ZK Körpererweiterung, die Menge  $\{x\}$  von  $f(x)$  enthält.

Dann ist  $K(u)$  ( $\subseteq L$ ) schon Zerfällungskörper von  $f(x)$  über  $K$ .

(1. A. fñr dñs.  $\mathbb{Q}(\sqrt{2})$  ist kein Zerfällungskörper von  $x^3 - 2 \in \mathbb{Q}[x]$ , da  $|Q| = \infty$ )

Bew. Sei  $n = \deg f(x)$ ,  $|K| = q \Rightarrow |K(u)| : |K| = n \Rightarrow |K(u)| = q^n \Rightarrow K(u) \cong GF(q^n)$   
 $\Rightarrow K(u)$  Zerfällungskörper von  $x^{q^n} - x$  über  $\mathbb{Z}_p$  ( $q = p^e$ ,  $p = \text{char}(K)$ ,  $\mathbb{Z}_p \subseteq K$ )  
und  $u$  Nullstelle von  $x^{q^n} - x \Rightarrow f(x) = m_{K(u)}(x) | (x^{q^n} - x)$ .  
 $\Rightarrow K(u)$  enthält alle Nullstellen von  $f(x)$ .  $\square$

Vor. Sei  $K = GF(q)$ ,  $q$  Primzahlpotenz. Dann gilt:

$$\{\text{normierte irreduzible Polynome vom Grad } n \text{ über } K\} = \{\text{normierte irreduzible Teiler von } x^{q^n} - x \text{ vom Grad } n\}$$

13.5 Rechnen in  $GF(p^n)$ 

Wir brauchen bloß ein irreduzibles Polynom vom Grad  $n$  über  $\mathbb{Z}_p$ . Bsp.  $GF(16)$

$$x^4 + x + 1 \in \mathbb{Z}_2[x] \quad (\text{irreduzibel, da beide Nullstellen von } (x^2 + x + 1)^2 \text{ sind})$$

$$\Rightarrow GF(16) \cong \mathbb{Z}_2[x]/\langle x^4 + x + 1 \rangle$$

$$1.\text{Form: } GF(16) = \left\{ \sum_{i=0}^3 \lambda_i x^i : \lambda_i \in \{0, 1\} \right\} \quad (\text{Addition einfach, aber Multiplikation schwierig})$$

Beschreibe also die multiplikative Struktur:  $(GF(16))^*, \cdot \cong \mathbb{Z}_{15}$

Ist  $\bar{x}$  Erzeuger von  $(GF(16))^*$ ? (Kriterium, da  $GF(16) = \mathbb{Z}_2(\bar{x})$ .)

$$\bar{x} \neq 1, \bar{x}^3 \neq 1, \bar{x}^5 = \bar{x} \cdot \bar{x}^4 = \bar{x}(-\bar{x}-1) = \bar{x}^2 + \bar{x} \neq 1$$

$$\Rightarrow \bar{o}(\bar{x}) = 15 \text{ in } GF(16)^* \Rightarrow \bar{x}, \bar{x} \text{ ist Erzeuger.}$$

$$2.\text{Form: } GF(16) = \{0, 1, \bar{x}, \dots, \bar{x}^{14}\} \quad (\text{Multiplikation einfach, Addition schwierig})$$

$$\bar{x}^4 = \bar{x}+1. \text{ Was ist } \bar{x}^{10} + \bar{x}^7?$$

$$\bar{x}^{10} = \bar{x}^4 \cdot \bar{x}^4 \cdot \bar{x}^2 = (\bar{x}+1)^2 \cdot \bar{x}^2 = \bar{x}^2 + \bar{x} + 1$$

$$\bar{x}^7 = \bar{x}^3 + \bar{x} + 1$$

$$\bar{x}^{10} + \bar{x}^7 = \bar{x}^3 + \bar{x}^2 = \bar{x}^6$$

$$(1.\text{Form}) \quad (2.\text{Form})$$

$$\text{Teilkörper von } GF(16) \supseteq E: |E: \mathbb{Z}_2| \mid |GF(16): \mathbb{Z}_2| = 4$$

schwierig, interessant für Kryptografie!

$$\Rightarrow |E| \in \{2, 4, 16\}$$

$$\text{Bei } |E|=4. \quad E^x \cong \mathbb{Z}_3. \quad E^x \leq GF(16)^* = \langle \bar{x} \rangle$$

$$\Rightarrow E^x = \{1, \bar{x}^5, \bar{x}^{10}\} \Rightarrow E = \{0, 1, \bar{x}^5, \bar{x}^{10}\} = \{0, 1, \bar{x}^2 + \bar{x}, \bar{x}^2 + \bar{x} + 1\}$$

$$(2.\text{Form}) \quad (1.\text{Form})$$

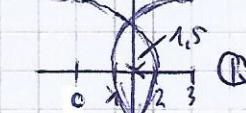
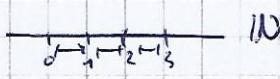
"Ist das nicht  
wunderlich?"

Ausblick: Geometrische Konstruktionen

Def.  $\alpha \in \mathbb{R}$  ist konstruierbar (mit Zirkel & Lineal), wenn man beginnend

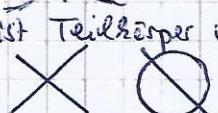
vom Ursprung (der Ebene) mit Hilfe eines unmarkierten, beliebig langen Lineals ("ein Stück") eines Zirkels, und eines Geradensegments der Länge 1 ein Geradensegment der Länge  $l|\alpha|$  in endlich vielen Schritten konstruieren kann.

Bsp.:



durch Kreisgleichung  
auch  $\sqrt{5}$  konstruierbar

Prop.  $\{\alpha \in \mathbb{R} : \alpha \text{ konstruierbar}\}$  ist Teilkörper von  $\mathbb{R}$ .  
Beweis: Im Sand spielen.



$$\Rightarrow \mathbb{Q} \subseteq \mathbb{Q}(\alpha_1) \subseteq \mathbb{Q}(\alpha_2) \subseteq \dots \subseteq \mathbb{Q}(\alpha_n)$$

Satz  $\alpha \in \mathbb{R}$  konstruierbar

$\Leftrightarrow$  existiert Teilkörper  $L \subseteq \mathbb{R}$  mit  $\alpha \in L$   
und  $\mathbb{Q} \subseteq \underbrace{\mathbb{Q}(\alpha_1)}_2 \subseteq \underbrace{\mathbb{Q}(\alpha_1, \alpha_2)}_2 \subseteq \dots \subseteq \underbrace{\mathbb{Q}(\alpha_1, \dots, \alpha_e)}_2 = L$  (Körperumfang)  
(Grad 2)

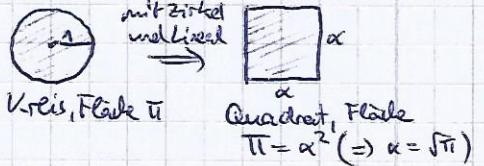
Kor.  $|L: \mathbb{Q}|$  ist 2er-Potenzordnung und  $\alpha$  ist algebraisch über  $\mathbb{Q}$ .  
(Hauptkriterium:  $\alpha$  konstruierbar  $\Rightarrow$  ja konstruierbar, vgl. Satz von Thales)

Kor. Damit kann man folgende Probleme der Antike lösen, die damals als mysteriös galten:

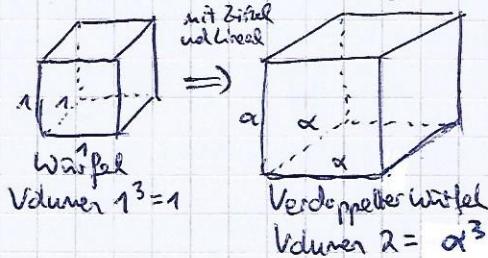
- Es gibt keine "Quadratur des Kreises".

Bew:  $\alpha$  konstruierbar  $\Rightarrow \alpha^2 = \pi$  konstruierbar

$$\Rightarrow \pi \text{ algebraisch über } \mathbb{Q}. \quad \text{Kreis, Fläche } \pi \quad \text{Quadrat, Fläche } \pi = \alpha^2 \quad (= \alpha = \sqrt{\pi})$$



- Es gibt keine "Verdopplung des Würfels".



Beweis:  $\alpha = \sqrt[3]{2}$  konstruierbar  
 $|L: \mathbb{Q}(\sqrt[3]{2})|: |L: \mathbb{Q}|$  ist 2er-Potenz  
 $= 3$ , da  $x^3 - 2$  irreduzibel über  $\mathbb{Q}$   
aber 3 ist keine 2er-Potenz.  $\square$

~ LE FIN ~