Algebra (Bachelor)
Wintersemester 2020/21

Birgit Richter, Version: 21. Januar 2021

Fachbereich Mathematik der Universität Hamburg, Bundesstrasse 55, 20146 Hamburg, Germany

Inhaltsverzeichnis

KAPITEL I

Gruppen

Vorlesung 1

Sie kennen das Konzept von Gruppen aus der linearen Algebra. Wir wiederholen die Grundlagen und gehen erst einmal einen Schritt zurück. Textteile, die Wiederholungen von Bekanntem sind, markiere ich mit blau.

I.1. Monoide und Gruppen

Definition I.1.1.

(a) Eine *Verknüpfung* auf einer nichtleeren Menge S ist eine Abbildung

$$*\colon S \times S \to S, \quad (s,t) \mapsto s * t.$$

(b) Eine Verknüpfung $*$ heißt *assoziativ*, falls für alle $s,t,u \in S$ gilt:

$$(s * t) * u = s * (t * u).$$

(c) Eine Verknüpfung $*$ heißt *kommutativ*, falls für alle $s,t \in S$ gilt:

$$s * t = t * s.$$

Beispiel I.1.2. Es sei $S = M(n \times n, K)$ die Menge der $n \times n$-Matrizen über einem Körper K. Dann definiert

$$*\colon M(n \times n, K) \times M(n \times n, K) \to M(n \times n, K), \quad (A,B) \mapsto AB - BA$$

eine Verknüpfung auf $M(n \times n, K)$, die nicht assoziativ ist. Hat K nicht die Charakteristik 2, so ist sie auch nicht kommutativ.

Bemerkung I.1.3. Ist eine Verknüpfung $*$ auf einer Menge S assoziativ, so brauchen wir mehrfache Produkte nicht zu klammern. Ausdrücke der Form $s_1 * \ldots * s_n$ liefern wohldefinierte Elemente von S.

Definition I.1.4.

(a) Es sei $(S,*)$ eine Menge mit Verknüpfung. Ein Element $e \in S$ heißt *neutrales Element* von S, wenn für alle $s \in S$ gilt:

$$s * e = s = e * s.$$

(b) Ein *Monoid* ist eine nichtleere Menge mit einer assoziativen Verknüpfung, so dass S ein neutrales Element besitzt.

Bemerkung I.1.5. Ein neutrales Element ist immer eindeutig: Wir nehmen an, dass sowohl e als auch e' neutral sind in $(S,*)$. Dann gilt $e' = e' * e$ wegen der Neutralität von e, aber $e' * e = e$ wegen der Neutralität von e', also erhalten wir insgesamt $e' = e$.

Sie kennen viele Monoide:

Beispiele I.1.6.

- Die natürlichen Zahlen mit Null, $\mathbb{N}_0$, bilden mit der Verknüpfung $* = +$ ein Monoid. Hierbei ist 0 das neutrale Element.
- Die natürlichen Zahlen (mit oder ohne Null) bilden mit der Multiplikation ebenfalls ein Monoid.
- Die Menge der Matrizen $M(n \times n, K)$ bilden ebenfalls sowohl mit der Addition von Matrizen als auch mit der Multiplikation von Matrizen ein Monoid. Im ersten Fall ist die Nullmatrix das neutrale Element, im zweiten Fall ist es die $n \times n$-Einheitsmatrix E_n.

Definition I.1.7. Eine *Gruppe* ist ein Monoid $(G, *)$ mit einem neutralen Element $e \in G$, in dem es für jedes $g \in G$ ein Element $h \in G$ gibt mit $g * h = e$.

Lemma I.1.8. *Das Element h zu $g \in G$ mit $g * h = e$ ist eindeutig bestimmt und es gilt auch $h * g = e$.*

Beweis. Zu h gibt es wiederum ein h' mit $h * h' = e$. Wir wenden $(-) * h'$ auf die Gleichung $g * h = e$ an und erhalten

$$g * h * h' = h'.$$

Die linke Seite ist aber gleich g, weil $h * h' = e$ gilt. Damit gilt $g = h'$, also $h * g = e$. Wir nehmen an, wir finden ein weiteres Element $\tilde{g}$ mit der Eigenschaft $g * \tilde{g} = e$. Anwenden von $h * (-)$ ergibt dann $\tilde{g} = h$ und somit ist h eindeutig. □

Bemerkung I.1.9. Deshalb nennen wir h *das* Inverse von g und schreiben $h = g^{-1}$. Falls wir uns die Verknüpfung als Addition vorstellen, benutzen wir $-g$.

Wir hatten schon die *Socken-und-Schuhe Regel* für die Bestimmung des Inversen einer Verknüpfung:

$$(g_1 * g_2)^{-1} = g_2^{-1} * g_1^{-1}.$$

Sie kennen bereits etliche Beispiele von Gruppen.

Beispiele I.1.10.

- Die ganzen Zahlen $\mathbb{Z}$ mit der Addition als Verknüpfung bilden eine Gruppe. Ebenso die rationalen Zahlen, $\mathbb{Q}$, die reellen Zahlen, $\mathbb{R}$, und die komplexen Zahlen, $\mathbb{C}$.
- Ist $X \neq \varnothing$ eine Menge, so bezeichne Σ_X die Menge der bijektiven Abbildungen $f\colon X \to X$. Dann ist Σ_X zusammen mit der Verkettung von Abbildungen eine Gruppe. Sie heißt die *Gruppe der Permutationen von X*.

  Insbesondere ist für $\mathbf{n} = \{1, \ldots, n\}$ die Menge aller bijektiven Abbildungen $\{f\colon \mathbf{n} \to \mathbf{n}, f \text{ bijektiv}\}$ eine Gruppe mit der Komposition von Abbildungen. Sie heißt die symmetrische Gruppe auf n Elementen und wir benutzen die Notation Σ_n. Sie wissen aus der linearen Algebra, dass Σ_n die Mächtigkeit $n!$ hat.
- Aus der linearen Algebra wissen Sie, dass die Menge der invertierbaren $n \times n$-Matrizen über einem Körper K, $GL_n(K)$, eine Gruppe bildet. Für den Spezialfall $n = 1$ bekommen Sie die multiplikative Gruppe des Körpers K, $(K \setminus \{0\}, \cdot)$.
- Ist S eine nichtleere Menge und ist G eine Gruppe, so ist die Menge aller Abbildungen von S nach G wiederum eine Gruppe: Sind $f, g\colon S \to G$, so definieren wir $f * g$ als die Abbildung, die ein $s \in S$ abbildet auf

  $$(f * g)(s) = f(s) * g(s).$$

  Hierbei bezeichnet $f(s) * g(s)$ die Verknüpfung in G von $f(s)$ mit $g(s)$. Machen Sie sich in diesem Beispiel die Gruppenstruktur explizit klar: Was ist das neutrale Element? Was ist das inverse Element zu f?

  Was erhalten Sie für $S = \mathbf{n}$? Was wäre eine sinnvolle Konvention für $S = \varnothing$?

Satz I.1.11. *Es sei $(G, *)$ eine nichtleere Menge mit einer assoziativen Verknüpfung, so dass gilt:*

(a) *Es gibt ein $e \in G$, so dass für alle $g \in G$ gilt: $e * g = g$.*
(b) *Für alle $g \in G$ gibt es ein $h \in G$ mit $h * g = e$.*

Dann ist G eine Gruppe.

In der obigen Situation nennt man e ein *linksneutrales Element* und h ein *linksinverses Element zu g*.

Beweis. Zu einem beliebigen $g \in G$ gibt es ein $h \in G$ mit $h * g = e$ und zu diesem h wiederum gibt es ein $k \in G$ mit $k * h = e$. Dann ist aber auch

$$g = e * g = (k * h) * g = k * (h * g) = k * e.$$

Da $e * e = e$ gilt nach Annahme, erhalten wir damit

$$g = k * e = k * (e * e) = (k * e) * e = g * e.$$

Somit ist e also auch rechtsneutral und $g = k * e = k$, so dass h auch ein rechtsinverses Element von g ist. Damit ist e ein neutrales Element in G und h das inverse Element von g. □

Bemerkung I.1.12.

- Es sei $(G, *)$ eine Gruppe und $g, h \in G$. Dann folgt für $x, y \in G$ aus $g * x = g * y$ schon $x = y$ und aus $x * h = y * h$ ebenfalls $x = y$. Wenden Sie g^{-1} von links beziehungsweise h^{-1} von rechts an.
- Die Notation für Verknüpfungen in Gruppen variiert:
  Stellen wir uns $*$ als Multiplikation vor, so schreiben wir statt $g * h$ oft $g \cdot h$ oder nur gh. Das neutrale Element wird dann oft als 1 notiert.
  Interpretieren wir $*$ dagegen als Addition, so steht $g + h$ für $g * h$ und 0 für e.
- Ist $n \in \mathbb{Z}$, so definieren wir für eine Gruppe $(G, \cdot)$ und ein $g \in G$:

$$g^0 = 1, g^1 = g \text{ und für } n \in \mathbb{N} : g^n = g^{n-1} \cdot g.$$

  Für negatives n setzen wir

$$g^n := (g^{-n})^{-1}.$$

  Mit dieser Konvention gilt die übliche Rechenregel

$$g^n \cdot g^m = g^{n+m} \text{ für alle } n, m \in \mathbb{Z}.$$

Im Folgenden schreiben wir Gruppen meistens multiplikativ und lassen das Symbol für die Verknüpfung weg.

I.2. Untergruppen und Homomorphismen

Definition I.2.1. Es sei $(G, \cdot)$ eine Gruppe. Eine Teilmenge $H \subset G$ heißt *Untergruppe*, falls gilt:

(a) Für alle $h, h' \in H$ gilt: $h \cdot h' \in H$.
(b) Für alle $h \in H$ ist $h^{-1} \in H$.
(c) Für das neutrale Element $1 \in G$ gilt $1 \in H$.

Das heißt, dass H unter der Verknüpfung und Inversenbildung abgeschlossen ist. Wir benutzen die Notation $H < G$, falls H eine Untergruppe von G ist.

Beispiele I.2.2.

- Für jede Gruppe $(G, \cdot)$ mit neutralem Element e sind $(\{e\}, \cdot)$ und $(G, \cdot)$ Untergruppen.
- Für $(G, \cdot) = (\mathbb{R}, +)$ ist sowohl $(\mathbb{Q}, +)$ als auch $(\mathbb{Z}, +)$ eine Untergruppe und $(\mathbb{Z}, +) \subset (\mathbb{Q}, +)$ ist Untergruppe.
- $(\mathbb{N}_0, +) \subset (\mathbb{Z}, +)$ ist *keine* Untergruppe.
- Sie wissen aus der linearen Algebra, dass

$$SL_n(K) := \{A \in GL_n(K), \det(A) = 1\}$$

  eine Untergruppe von $GL_n(K)$ ist.
- Ist $(G, \cdot)$ eine Gruppe, so ist

$$\langle g \rangle := \{g^n, n \in \mathbb{Z}\}$$

  eine Untergruppe von G. Sie heißt die *von $g \in G$ erzeugte Untergruppe*.

Bemerkung I.2.3. Ist G eine Gruppe und ist $(H_i)_{i \in I}$ eine beliebige Familie von Untergruppen $H_i < G$, so ist $\bigcap_{i \in I} H_i$ wiederum eine Untergruppe von G.
Es sei p eine Primzahl. Was ist die Untergruppe $\bigcap_{i \in \mathbb{N}} p^i\mathbb{Z}$ von $(\mathbb{Z}, +)$?

Vorlesung 2

Wir betrachten Abbildungen zwischen Gruppen, welche die Gruppenstruktur respektieren:

Definition I.2.4.

(a) Es seien $(G, \cdot)$ und $(G', *)$ Gruppen. Eine Abbildung $f\colon G \to G'$ heißt *Gruppenhomomorphismus* (oder kurz *Homomorphismus*), falls für alle $g_1, g_2 \in G$ gilt:

$$f(g_1 \cdot g_2) = f(g_1) * f(g_2).$$

(b) Ein injektiver Gruppenhomomorphismus ist ein *Monomorphismus*, ein surjektiver Gruppenhomomorphismus ist ein *Epimorphismus* und ein bijektiver Gruppenhomomorphismus heißt *Isomorphismus*.

(c) Zwei Gruppen G und G' heißen *isomorph*, falls es einen Isomorphismus zwischen ihnen gibt. Wir benutzen die Notation $G \cong G'$ dafür.

(d) Ein Gruppenhomomorphismus $f\colon G \to G$ heißt ein *Endomorphismus*.

Bemerkung I.2.5. Sie kennen schon etliche Fakten über Homomorphismen:

- Sind $f\colon G_1 \to G_2$ und $f'\colon G_2 \to G_3$ Homomorphismen, so auch $f' \circ f\colon G_1 \to G_3$.
- Ist $f\colon G \to G'$ ein Homomorphismus, so bildet f das neutrale Element von G auf das neutrale Element von G' ab.
- Das Inverse von $f(g)$ ist $f(g^{-1})$:

  $$(f(g))^{-1} = f(g^{-1}).$$

  Hierfür rechnen wir nach:

  $$f(g)f(g^{-1}) = f(gg^{-1}) = f(1_G) = 1_{G'}.$$

- Ein Homomorphismus $f\colon G \to G'$ ist genau dann ein Monomorphismus, falls $\ker(f) = \{1_G\}$. Hierbei ist $\ker(f) = \{g \in G, f(g) = 1_{G'}\}$ der *Kern von* f.

  Auch hier wiederholen wir kurz den Beweis: Ist $\ker(f) = \{1_G\}$ und ist $f(g_1) = f(g_2)$, so ist

  $$1_{G'} = f(g_1)f(g_2)^{-1} = f(g_1 g_2^{-1})$$

  . Also ist $g_1 g_2^{-1} \in \ker(f)$ und damit $g_1 g_2^{-1} = 1_G$. Das impliziert aber $g_1 = g_2$.

  Es sei umgekehrt f injektiv und es sei $g \in \ker(f)$. Da immer auch $1_G \in \ker(f)$ ist, haben wir

  $$f(g) = 1_{G'} = f(1_G).$$

  Die Injektivität von f impliziert dann $g = 1_G$.
- Nach Definition ist $f\colon G \to G'$ genau dann ein Epimorphismus, falls $\text{Bild}(f) = G'$.

Beispiele I.2.6.

- Für $(G, \cdot) = (G', *) = (\mathbb{Z}, +)$ und für ein festes $m \in \mathbb{Z}$ ist die Abbildung

  $$f\colon \mathbb{Z} \to \mathbb{Z}, \quad x \mapsto mx$$

  ein Homomorphismus, weil

  $$f(x + y) = m(x + y) = mx + my = f(x) + f(y).$$

- Es sei $\mathbb{R}_{>0} := \{x \in \mathbb{R}, x > 0\}$. Für $(G, \cdot) = (\mathbb{R}, +)$ und $(G', *) = (\mathbb{R}_{>0}, \cdot)$ definiert die Exponentialfunktion $f(x) = e^x$ einen Homomorphismus, weil

  $$f(x + y) = e^{x+y} = e^x \cdot e^y = f(x) \cdot f(y).$$

- Die Determinantenabbildung

  $$\det\colon (GL_n(K), \cdot) \to (K \setminus \{0\}, \cdot)$$

  ist ein Homomorphismus.
- Ist G eine Gruppe, so können wir

  $$\mathsf{Aut}(G) := \{f\colon G \to G, f \text{ Endomorphismus und bijektiv}\}$$

  betrachten. Diese Menge ist mit der Verkettung von Abbildungen selbst wieder eine Gruppe, die *Automorphismengruppe von* G.

Satz I.2.7. *Ist $f\colon G \to G'$ ein Homomorphismus, so ist* $\ker(f)$ *eine Untergruppe von G und* $\mathrm{Bild}(f)$ *ist eine Untergruppe von G'.*

BEWEIS. Sind $g, \tilde{g} \in \ker(f)$, so ist

$$f(g\tilde{g}) = f(g)f(\tilde{g}) = 1_{G'}1_{G'} = 1_{G'},$$

also auch das Produkt.

Mit $g \in \ker(f)$ gilt für g^{-1}:

$$f(g^{-1}) = (f(g))^{-1} = (1_{G'})^{-1} = 1_{G'},$$

also auch $g^{-1} \in \ker(f)$.

Das neutrale Element von G ist immer im Kern von f. Damit ist $\ker(f)$ eine Untergruppe.

Es ist $f(1_G) = 1_{G'}$, also ist $1_{G'} \in \mathrm{Bild}(f)$.

Sind g_1', g_2' im Bild von f, so gibt es $g_1, g_2 \in G$ mit $f(g_1) = g_1'$ und $f(g_2) = g_2'$. Daraus folgt

$$g_1'g_2' = f(g_1)f(g_2) = f(g_1g_2)$$

und damit ist $g_1'g_2'$ ebenfalls im Bild von f.

Ist g' im Bild von f, so gibt es ein $g \in G$ mit $f(g) = g'$. Dann gilt auch

$$(g')^{-1} = f(g)^{-1} = f(g^{-1})$$

und $(g')^{-1}$ ist im Bild von f. □

Wir betrachten das folgende wichtige Beispiel eines Homomorphismus.

Definition I.2.8. Es sei G eine Gruppe und $g \in G$ ein beliebiges Element. Die Abbildung

$$c_g\colon G \to G, \quad h \mapsto ghg^{-1}$$

heißt die *Konjugation mit $g \in G$.*

Bemerkung I.2.9.

- Konjugieren wir mit 1_G, so passiert gar nichts:

  $$c_{1_G}(h) = 1_G h 1_G^{-1} = h,$$

  das heißt, dass c_{1_G} die identische Abbildung ist.
- Für jedes $g \in G$ ist c_g ein Homomorphismus:

  $$c_g(h_1h_2) = gh_1h_2g^{-1} = gh_1g^{-1}gh_2g^{-1} = c_g(h_1)c_g(h_2).$$
- Für jedes $g \in G$ ist c_g bijektiv mit Inversem $c_{g^{-1}}$:

  $$c_{g^{-1}}(c_g(h)) = g^{-1}ghg^{-1}g = h \text{ und } c_g(c_{g^{-1}}(h)) = gg^{-1}hgg^{-1} = h \text{ für alle } h \in G.$$

  Damit ist $c_g \in \mathsf{Aut}(G)$ für alle $g \in G$.

Wir jonglieren und lassen g in c_g laufen.

Lemma I.2.10. *Die Abbildung*

$$c\colon G \to \mathsf{Aut}(G), \quad g \mapsto c_g$$

ist ein Homomorphismus.

BEWEIS. Wir rechnen nach:

$$c_{g_1g_2}(h) = g_1g_2h(g_1g_2)^{-1} = g_1g_2hg_2^{-1}g_1^{-1} = c_{g_1}(c_{g_2}(h)).$$

□

Definition I.2.11.

(a) Das Bild von c heißt die *Gruppe der inneren Automorphismen von G*. Die Notation hierfür ist $\mathsf{Inn}(G)$.

(b) Der Kern von c heißt das *Zentrum von G*, $Z(G)$.

Wie sieht der Kern von c explizit aus? Ein $g \in G$ ist im Zentrum von G, falls c_g die identische Abbildung ist, also $c_g(h) = h$ für alle $h \in G$. Das ergibt:

$$ghg^{-1} = h \text{ für alle } h \in G$$

also

$$gh = hg \text{ für alle } h \in G.$$

Dies sind alle $g \in G$, die mit allen Elementen aus G kommutieren:

$$Z(G) = \{g \in G, gh = hg \text{ für alle } h \in G\}.$$

Überlegen Sie sich, dass für alle $f \in \mathsf{Aut}(G)$ gilt:

$$f \circ c_g \circ f^{-1} = c_{f(g)}.$$

Beispiel I.2.12. Als Beispiel bestimmen wir die Automorphismengruppe von $(\mathbb{Z}, +)$. Da hier jedes Element mit jedem kommutiert, ist $Z(\mathbb{Z}) = \mathbb{Z}$ und $\mathsf{Inn}(\mathbb{Z})$ ist trivial.

Jeder Homomorphismus $f\colon \mathbb{Z} \to \mathbb{Z}$ ist durch den Wert $f(1)$ festgelegt, weil $f(n) = nf(1)$ für alle $n \in \mathbb{Z}$ gilt. Wir definieren $f_+\colon \mathbb{Z} \to \mathbb{Z}$ durch $f_+(1) = 1$. Damit ist f_+ die identische Abbildung, $\mathrm{id}_\mathbb{Z}$, und somit natürlich ein Automorphismus.

Analog sei f_- definiert durch $f_-(1) = -1$. Dann ist $f(n) = -n$ für alle $n \in \mathbb{Z}$ und f_- ist das Negative der Identität, $-\mathrm{id}_\mathbb{Z}$ auf $\mathbb{Z}$. Wir haben damit $f_\pm \in \mathsf{Aut}(\mathbb{Z})$.

Das ist auch schon alles: Ist $f(1) = n$ und $n \neq \pm 1$, so ist das Bild von f gleich $n\mathbb{Z}$ und dies ist eine echte Untergruppe von $\mathbb{Z}$. Damit ist f nicht surjektiv. Also gilt $\mathsf{Aut}(\mathbb{Z}) = \{\pm\mathrm{id}\}$. Dies ist eine Gruppe mit nur zwei Elementen. Es gilt

$$f_- \circ f_+ = f_- = f_+ \circ f_-, \quad f_- \circ f_- = f_+ \text{ und } f_+ \circ f_+ = f_+.$$

Was ist $\mathsf{Aut}(\mathsf{Aut}(\mathbb{Z})) = \mathsf{Aut}(\{\pm\mathrm{id}_\mathbb{Z}\})$?

Vorlesung 3

I.3. Zyklische Gruppen und Gruppenordnungen

Für eine Menge S bezeichnen wir mit $|S|$ die Mächtigkeit von S. Ist G eine Gruppe, so nennen wir $|G|$ die *Gruppenordnung*. Zu einer Gruppe G und einem $g \in G$ hatten wir schon

$$\langle g \rangle = \{g^m, m \in \mathbb{Z}\}$$

betrachtet. Wir schaun uns $\langle g \rangle$ nun genauer an:

Definition I.3.1. Es sei G eine Gruppe.

Ein $g \in G$ hat die *Ordnung* $n \in \mathbb{N}$, falls $|\langle g \rangle| = n$. Hat $\langle g \rangle$ keine endliche Ordnung, so heißt g *von unendlicher Ordnung*.

Wir benutzen die Notation

$$\mathsf{ord}(g) = \begin{cases} n, & |\langle g \rangle| = n \in \mathbb{N} \\ \infty, & |\langle g \rangle| \text{ nicht endlich.} \end{cases}$$

Beispiele I.3.2.

- Es sei $A = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \in GL_3(\mathbb{Q})$. Da $A \neq E_3$ und $A^2 = E_3$, ist die Ordnung von A zwei.
- Wir betrachten $G = (\mathbb{C} \setminus \{0\}, \cdot)$ und für $n \in \mathbb{N}$, $n \neq 1$

  $$\zeta_n = e^{2\pi i/n}.$$

  Dann ist

  $$\langle \zeta_n \rangle = \{\zeta_n, \zeta_n^2, \ldots, \zeta_n^{n-1}, \zeta_n^n = e^{2\pi i} = 1\}$$

  und somit ist $\mathsf{ord}(\zeta_n) = n$. Konkrete Beispiele sind $\zeta_2 = -1$ und $\zeta_4 = i$.

- Was passiert für $\zeta = e^{2\pi i\varphi}$, falls $\varphi \in (0,1)$ eine irrationale Zahl ist? Was gilt dann für die Ordnung von ζ?

Satz I.3.3. *Es sei G eine Gruppe und $g \in G$.*

(a) *Ist $\mathsf{ord}(g) < \infty$, so gibt es ein kleinstes $n \in \mathbb{N}$ mit $g^n = 1$ und $\langle g\rangle = \{g^i, 0 \leqslant i \leqslant n-1\}$. Es gilt $g^m = 1$ genau dann, wenn es ein $a \in \mathbb{Z}$ gibt mit $m = an$.*
(b) *Ist $\mathsf{ord}(g) = \infty$, so sind alle Elemente g^i für $i \in \mathbb{Z}$ verschieden.*
(c) *Ist $\mathsf{ord}(g) = n \in \mathbb{N}$, so gilt*

$$\mathsf{ord}(g^i) = \frac{n}{\mathsf{ggT}(n,i)}.$$

Beweis. Zu (a): Ist die Ordnung von g endlich, so ist die Menge

$$\{m \in \mathbb{N}, g^m = 1\}$$

nicht leer und hat ein Minimum. Das ist das gesuchte n. Ist $m \in \mathbb{Z}$ beliebig, so können wir m mit Rest durch n teilen und erhalten

$$m = an + r \text{ mit } 0 \leqslant r < n \text{ und } a \in \mathbb{Z}.$$

Damit ist

$$g^m = g^{an}g^r = g^r.$$

Da aber $r < n$ ist, kann g^m nur dann 1 sein, wenn $r = 0$ ist, also $m = an$. Ist $g^i = g^j$, so muss i kongruent zu j sein modulo n, weil $g^{i-j} = 1$. Somit sind die Elemente $g^0, g, \ldots, g^{n-1}$ paarweise verschieden und

$$\langle g\rangle = \{g^i, 0 \leqslant i \leqslant n-1\}.$$

Zu (b): Ist $g^i = g^j$ für $i \neq j \in \mathbb{Z}$, so ist $g^{i-j} = 1$ und g hat endliche Ordnung. Sind die g^i alle paarweise verschieden, so ist insbesondere kein $g^i = g^0 = 1$ für $i \neq 0$. Somit hat g keine endliche Ordnung.

Zu (c): Da $\mathsf{ord}(g^i) = \mathsf{ord}(g^{-i})$ ist, können wir annehmen, dass $i \in \mathbb{N}_0$ ist. Es sei $\mathsf{ord}(g^i) = m$, also gilt $(g^i)^m = g^{im} = 1$. Da die Ordnung von g gleich n ist, muss also n das Produkt im teilen. Damit teilt aber $n/\mathsf{ggT}(n,i)$ die Zahl m und für die Ordnung von g^i gilt

$$\mathsf{ord}(g^i) \geqslant \frac{n}{\mathsf{ggT}(n,i)}.$$

Beachten Sie, dass $n/\mathsf{ggT}(n,i) \in \mathbb{Z}$ gilt. Da aber

$$(g^i)^{\frac{n}{\mathsf{ggT}(n,i)}} = g^{\frac{in}{\mathsf{ggT}(n,i)}} = (g^n)^{\frac{i}{\mathsf{ggT}(n,i)}} = 1$$

ist, ist auch $\mathsf{ord}(g^i) \leqslant \frac{n}{\mathsf{ggT}(n,i)}$ und insgesamt erhalten wir die Behauptung. □

Definition I.3.4. Ist G eine Gruppe und ist $G = \langle g\rangle$ für ein $g \in G$, so heißt G eine *zyklische Gruppe*. Ist zusätzlich $\mathsf{ord}(g) = n$, so heißt G eine *zyklische Gruppe der Ordnung n*.

Satz I.3.5.
(a) *Ist $G = \langle g\rangle$ zyklisch, so ist auch jede Untergruppe von G zyklisch.*
(b) *Gilt $\mathsf{ord}(g) = n \in \mathbb{N}$, so gibt es für jedes $d \in \mathbb{N}$, welches n teilt, eine Untergruppe $H < G$ mit $|H| = d$ und es gilt $H = \langle g^{n/d}\rangle$. Alle Untergruppen von G sind von dieser Form.*

Beweis. Zu (a): Ist $H < G$ die triviale Gruppe, so ist die Behauptung klar, weil $H = \langle g^0\rangle$.

Wir können also annehmen, dass es ein $h \in H$ gibt mit $h \neq 1$. Da $H < \langle g\rangle$, ist also $h \in \langle g\rangle$. Somit gibt es ein $i \in \mathbb{Z}$ mit $h = g^i$. Da H eine Untergruppe ist, liegt auch g^{-i} in H. Wir setzen

$$j := \min\{i > 0, g^i \in H\}.$$

Wir behaupten, dass $H = \langle g^j\rangle$ gilt. Ist $g^i \in H$, so schreiben wir $i = aj + r$ mit $a \in \mathbb{Z}$ und $0 \leqslant r \leqslant j-1$. Da $g^i = g^{aj}g^r$ und $g^{aj} \in H$, muss auch $g^r \in H$ gelten. Aber j war minimal, so dass $r = 0$ sein muss. Damit ist jedes $g^i \in H$ von der Form $g^i = (g^j)^a$ und $H = \langle g^j\rangle$ ist zyklisch.

Zu (b): Ist $\mathsf{ord}(g) = n \in \mathbb{N}$, so betrachte $1 = g^n \in H = \langle g^j \rangle$. Damit teilt j die Zahl n und $|H| = n/j$. Alle Untergruppen von G sind also von dieser Form. Umgekehrt hat für jedes $d \in \mathbb{N}$ mit $d|n$ die Gruppe $\langle g^{n/d} \rangle$ genau d Elemente.

□

Beispiele I.3.6.

- Betrachten wir $G = (\mathbb{Z}, +)$, so entspricht g^i in diesem Beispiel ig, weil wir $\mathbb{Z}$ mit der Addition betrachten. Die Gruppe $\mathbb{Z}$ ist zyklisch mit $\mathbb{Z} = \langle 1 \rangle$ und $\mathsf{ord}(1) = \infty$. Die Untergruppen von $\mathbb{Z}$ sind von der Form $m\mathbb{Z}$ mit $m \in \mathbb{N}_0$.
- Ist $\zeta_6 = e^{2\pi i/6}$, so ist $G = \langle \zeta_6 \rangle$ eine zyklische Gruppe mit 6 Elementen. Die Zahl 6 hat die Teiler $1, 2, 3, 6$ und diese Teiler entsprechen den Untergruppen $\langle \zeta_6^6 \rangle = \{1\}$, $\langle \zeta_6^3 \rangle$, $\langle \zeta_6^2 \rangle$ und $\langle \zeta_6 \rangle = G$.

  Welche Elemente $g \in G$ haben Ordnung 6, das heißt $g^r = 1$ nur für $r \in 6\mathbb{Z}$? Wir wissen $g = \zeta_6^i$ für ein i. Also wollen wir $\zeta_6^{ir} = 1$ nur für $r \in 6\mathbb{Z}$. Das ergibt die Bedingung, dass 6 die Zahl ir genau dann teilt, wenn 6 die Zahl r teilt. Also muss gelten

$$\mathsf{ggT}(i, 6) = 1.$$

  Wir erhalten also, dass nur die Elemente ζ_6 und ζ_6^5 Ordnung 6 haben in G.

Wir suchen also Zahlen, die teilerfremd sind zu einer gegebenen Zahl:

Definition I.3.7. Die *Eulersche φ-Funktion* ordnet einem $n \in \mathbb{N}$ die Anzahl aller $1 \leqslant i \leqslant n$ mit $\mathsf{ggT}(n, i) = 1$ zu.

Leonhard Euler (1707–1783)

Für Gruppen erhalten wir, dass es für ein $g \in G$ mit $\mathsf{ord}(g) = n \in \mathbb{N}$ genau $\varphi(n)$ Elemente in $\langle g \rangle$ gibt, die Ordnung n haben.

I.4. Nebenklassen und normale Untergruppen

Ist $(S, *)$ eine Menge mit Verknüpfung und sind X, Y Teilmengen von S, so sei

$$X * Y = \{x * y, x \in X, y \in Y\}. \tag{I.4.1}$$

Wenn Sie möchten, dann können Sie dies als eine Verknüpfung auf der Potenzmenge von S auffassen.

Für Gruppen G mit $X, Y \subset G$ schreiben wir wieder kürzer

$$XY = \{xy, x \in X, y \in Y\}$$

und wir kürzen $\{x\}Y$ mit xY und $Y\{x\}$ mit Yx ab.

Definition I.4.1. Ist G eine Gruppe und $H < G$ eine Untergruppe, so betrachten wir in der Potenzmenge von G die Teilmengen

$$G/H := \{gH, g \in G\}$$

und

$$H\backslash G := \{Hg, g \in G\}.$$

Die Elemente von G/H heißen *Linksnebenklassen von H in G* und die Elemente von $H\backslash G$ heißen *Rechtsnebenklassen von H in G*.

Lemma I.4.2. *Es sei G eine Gruppe und $H < G$ eine Untergruppe.*

Jedes Element von G gehört genau zu einer Linksnebenklasse in G/H und genau zu einer Rechtsnebenklassen in $H\backslash G$.

Beweis. Wir führen den Beweis nur für Linksnebenklassen. Wir wissen, dass $1 \in H$. Damit ist $g = g \cdot 1 \in gH$. Wir nehmen an, dass g auch Element von $\tilde{g}H$ ist. Dann gibt es ein $h \in H$, so dass

$$g = \tilde{g}h.$$

Damit folgt aber

$$gH = \tilde{g}hH = \tilde{g}H.$$

Hier haben wir benutzt, dass $hH = H$ ist für alle $h \in H$. Somit ist gH die einzige Linksnebenklasse, die g enthält. □

Satz I.4.3 (Satz von Lagrange)**.** *Es sei G eine endliche Gruppe und $H < G$ eine Untergruppe. Dann gilt*

$$|G| = |H| \cdot |G/H| = |H| \cdot |H\backslash G|.$$

Joseph-Louis de Lagrange (1736–1813)

Beweis. Jedes $g \in G$ gehört genau zu einer Nebenklasse und jede Nebenklasse gH oder Hg hat genau $|H|$ Elemente. □

Korollar I.4.4. *In jeder endlichen Gruppe ist die Ordnung jeder Untergruppe ein Teiler der Gruppenordnung. Insbesondere teilt* $\mathsf{ord}(g)$ *die Zahl $|G|$ für alle $g \in G$.*

Definition I.4.5. Die Mächtigkeit von $|G/H|$ nennt man den *Index von H in G*. Dieser wird mit $[G : H]$ notiert.

Beispiel I.4.6. Wir betrachten die symmetrische Gruppe Σ_3 mit $3! = 6$ Elementen. Es sei $(1, 2)$ die Permutation, die 1 auf 2, 2 auf 1 abbildet und 3 fest läßt. Wenn Sie $(1, 2)$ mit sich selbst verketten, erhalten Sie die identische Abbildung: $(1, 2) \circ (1, 2) = \mathrm{id}$. Wenn wir die zyklische Gruppe betrachten, die von $(1, 2)$ erzeugt wird, dann erhalten wir eine Gruppe mit zwei Elementen:

$$\langle (1, 2) \rangle = \{(1, 2), \mathrm{id}\}.$$

Der Satz von Lagrange besagt in diesem Beispiel, dass

$$|\Sigma_3/\langle (1, 2) \rangle| = |\Sigma_3|/|\langle (1, 2) \rangle| = 6/2 = 3.$$

Bezeichnen wir mit $(1, 2, 3)$ die Permutation, die 1 auf 2, 2 auf 3 und 3 auf 1 abbildet, dann hat dieses Element Ordnung 3 und

$$|\Sigma_3/\langle (1, 2, 3) \rangle| = 6/3 = 2.$$

Wenn wir $\langle (1, 2, 3) \rangle$ mit H abkürzen, dann ist $(1, 2) \notin H$. Nach Lagrange wissen wir schon, dass wir Σ_3 disjunkt zerlegen können als H vereinigt mit $(1, 2)H$. Explizit ergibt dies:

$$\begin{aligned} \Sigma_3 = H \cup (1, 2)H &= \{(1, 2, 3), (1, 2, 3)^2, \mathrm{id}\} \cup \{(1, 2) \circ (1, 2, 3), (1, 2) \circ (1, 2, 3)^2, (1, 2)\} \\ &= \{(1, 2, 3), (1, 2, 3)^2, \mathrm{id}\} \cup \{(2, 3), (1, 3), (1, 2)\}, \end{aligned}$$

wobei $(2, 3)$ die Permutation ist, die 2 und 3 vertauscht, und $(1, 3)$ die Permutation ist, die 1 und 3 vertauscht.

Vorlesung 4

Lemma I.4.7. *Ist G eine Gruppe und $H < G$ eine Untergruppe, so sind äquivalent:*

(a) *Für alle $g \in G$ ist $gH = Hg$.*
(b) *Für alle $g \in G$ ist $g^{-1}Hg = H$.*
(c) *Für alle $g \in G$ und für alle $h \in H$ ist $g^{-1}hg \in H$.*

Beweis. Es ist klar, dass (a) ⇒ (b) ⇒ (c) gilt. Wir müssen also nur zeigen, dass aus (c) (a) folgt. Wir nehmen also an, dass (c) gilt. Nach Definition ist $gh \in gH$ für alle $g \in G$ und $h \in H$. Wir schreiben gh um als

$$gh = (g^{-1})^{-1}hg^{-1}g.$$

Nach Annahme ist $(g^{-1})^{-1}hg^{-1}$ ein Element in H, also gilt $gh \in Hg$ und somit $gH \subset Hg$. Analog ist $hg = gg^{-1}hg \in gH$ für alle $h \in H$ und $g \in G$, also $Hg \subset gH$. Insgesamt erhalten wir $gH = Hg$ für alle $g \in G$. □

Definition I.4.8. Eine Untergruppe $H < G$, welche die Bedingungen aus Lemma I.4.7 erfüllt, heißt eine *normale Untergruppe von G*. Die Notation hierfür ist $H \lhd G$.

Beispiele I.4.9.

- Ist eine Gruppe G abelsch, gilt also $gh = hg$ für alle $g, h \in G$, so ist *jede* Untergruppe normal, weil $g^{-1}hg = h$ ist für alle $g \in G$ und $h \in H$.

- Die spezielle lineare Gruppe $SL_n(K)$ ist normal in $GL_n(K)$: $SL_n(K)$ ist der Kern der Determinantenabbildung. Ist $A \in GL_n(K)$ und $B \in SL_n(K)$, so ist

$$\det(A^{-1}BA) = \det(A)^{-1}\det(B)\det(A) = \det(A)^{-1}\det(A) = 1.$$

  Das gilt viel allgemeiner.

Satz I.4.10. *Ist $f\colon G \to G'$ ein Gruppenhomomorphismus, so ist der Kern von f eine normale Untergruppe von G.*

BEWEIS. Ist $g \in G$ und $h \in \ker(f)$, so ist

$$f(g^{-1}hg) = f(g)^{-1}f(h)f(g) = f(g)^{-1}f(g) = 1_{G'}$$

und somit ist $g^{-1}hg \in \ker(f)$. □

Beispiele I.4.11.

- Die Determinantenabbildung $\det\colon GL_n(K) \to K \setminus \{0\}$ gibt $SL_n(K) \lhd GL_n(K)$ wie oben.
- Sie kennen aus der linearen Algebra das Signum einer Permutation, sign. Zu einer Permutation $\sigma \in \Sigma_n$ war $\operatorname{sign}(\sigma)$ als $\det(E_\sigma)$ definiert. Da sign ein Homomorphismus

$$\operatorname{sign}\colon \Sigma_n \to \{\pm 1\}$$

  ist, ist sign durch den Wert auf Transpositionen festgelegt: Ist (i,j) die Permutation, die i und j vertauscht für $i \neq j$, so ist $\operatorname{sign}(i,j) = -1$.

  Wir lernen später eine andere Beschreibung kennen. Der Kern der Signumsabbildung heißt die *alternierende Gruppe auf n Elementen*, A_n.

  Wie viele Elemente hat A_3?

Bemerkung I.4.12. Ist $H \lhd G$, also $gH = Hg$ für alle $g \in G$, so nennt man gH und Hg *Nebenklasse* und H heißt dann ein *Normalteiler von G*.

Definition I.4.13. Hat eine Gruppe G nur $\{1\}$ und G als Normalteiler, so heißt G *einfach*.

Bemerkung I.4.14. Vorsicht: Einfache Gruppen sind bei weitem nicht einfach im umgangssprachlichen Sinn. Es gibt eine Klassifikation der endlichen einfachen Gruppen. Diese zerfallen in 17 Serien von Gruppen und 26 Einzelfälle, die sogenannten *sporadischen Gruppen*.

`https://de.wikipedia.org/wiki/Endliche_einfache_Gruppe#Klassifikation`

Die größte dieser sporadischen Gruppen ist die sogenannte Monster-Gruppe M (auch Fischer–Griess Monster nach Bernd Fischer (1936–2020) und Robert Griess (*1945) oder *friendly giant* genannt) mit

$$|M| = 2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71.$$

`https://de.wikipedia.org/wiki/Monstergruppe`

Satz I.4.15. *Ist G eine Gruppe und $H \lhd G$ eine normale Untergruppe, so ist G/H wiederum eine Gruppe, die sogenannte* Restklassen- oder auch Faktorgruppe von G nach H.

BEWEIS. Wir definieren für $g, \tilde{g} \in G$ die Verknüpfung $gH * \tilde{g}H$ als die Verknüpfung der Elemente $gH, \tilde{g}H$ in der Potenzmenge von G wie in (I.4.1):

$$(gH)(\tilde{g}H) = \{xy, x \in gH, y \in \tilde{g}H\}.$$

Da $H\tilde{g} = \tilde{g}H$ ist, erhalten wir wiederum eine Nebenklasse als Ergebnis:

$$(gH)(\tilde{g}H) = g\tilde{g}HH = g\tilde{g}H.$$

Damit ist die Verknüpfung

$$(gH, \tilde{g}H) \mapsto g\tilde{g}H$$

eine wohldefinierte Verknüpfung auf G/H. Sie ist assoziativ, weil die Verknüpfung in G assoziativ ist, $H = 1H$ ist das neutrale Element und das inverse Element zu gH ist $g^{-1}H$. □

Beispiel I.4.16. Wir wissen schon, dass $\mathbb{Z}$ zyklisch ist mit $\mathbb{Z} = \langle 1 \rangle$ und mit Satz I.3.5 ist damit auch jede Untergruppe zyklisch, also von der Form $m\mathbb{Z}$ mit einem $m \in \mathbb{N}_0$. Diese sind normal, weil $\mathbb{Z}$ abelsch ist. Die möglichen Restklassengruppen von $\mathbb{Z}$ sind also $\mathbb{Z}/m\mathbb{Z}$. Der Fall $m = 0$ gibt $0\mathbb{Z} = 0$ und $\mathbb{Z}/0\mathbb{Z} = \mathbb{Z}$. Sonst hat $\mathbb{Z}/m\mathbb{Z}$ genau m Elemente:

$$\mathbb{Z}/m\mathbb{Z} = \{0 + m\mathbb{Z}, 1 + m\mathbb{Z}, \ldots, (m-1) + m\mathbb{Z}\}.$$

Für $m = 2$ interessieren Sie sich nur dafür, ob eine Zahl gerade oder ungerade ist: Die Restklasse der 0 enthält alle geraden Zahlen, die Restklasse der 1 enthält die ungeraden Zahlen.

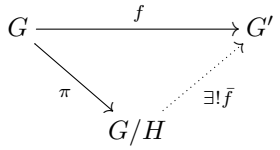
Den Fall $m = 24$ benutzen Sie im Alltag, wenn Sie über Uhrzeiten reden.

Definition I.4.17. Es sei G eine Gruppe und $H \lhd G$. Die Abbildung $\pi\colon G \to G/H$, $\pi(g) = gH$ heißt der *kanonische Epimorphismus* oder auch die *kanonische Projektion*.

Bemerkung I.4.18. Die Abbildung π ist in der Tat ein Homomorphismus, so ist die Gruppenstruktur auf G/H gerade definiert. Der Kern von π ist H:

$$\pi(g) = H \Leftrightarrow gH = H \Leftrightarrow g \in H.$$

Satz I.4.19 (Universelle Eigenschaft der Restklassengruppe)**.** *Sind G und G' Gruppen, $H \lhd G$ und $f\colon G \to G'$ ein Homomorphismus. Ist $H \subset \ker(f)$, so gibt es einen eindeutigen Homomorphismus $\bar{f}\colon G/H \to G'$ mit $\bar{f} \circ \pi = f$.*



Wie bei Quotientenvektorräumen in der linearen Algebra kann man sich diese Eigenschaft so merken, dass f die normale Untergruppe sowieso ignoriert, und daher eine wohldefinierte Abbildung auf G/H induziert.

Beweis. Da π surjektiv ist, ist $\bar{f}$ durch die Forderung, dass $\bar{f} \circ \pi = f$ ist, schon eindeutig festgelegt: Ist $gH \in G/H$, so ist $gH = \pi(g)$ und somit

$$\bar{f}(gH) = \bar{f}(\pi(g)) = f(g).$$

Ist $gH = \tilde{g}H$, so gibt es ein $h \in H$ mit $\tilde{g} = gh$. Dann ist

$$\bar{f}(\tilde{g}H) = f(\tilde{g}) = f(gh) = f(g)f(h).$$

Da aber $H \subset \ker(f)$, haben wir $f(h) = 1_{G'}$ und somit $f(\tilde{g}) = f(g)$. Das zeigt, dass $\bar{f}$ wohldefiniert ist. Da $g_1Hg_2H = g_1g_2H$ gilt, ist $\bar{f}$ ein Homomorphismus. □

Wie im Kontext von Vektorräumen und linearen Abbildungen können Sie auch im Kontext von Gruppen und Homomorphismen jeden Homomorphismus durch einen Isomorphismus ersetzen:

Satz I.4.20 (Isomorphiesatz)**.** *Ist $f\colon G \to G'$ ein Homomorphismus, so ist $\bar{f}\colon G/\ker(f) \to \mathrm{Bild}(f)$ ein Isomorphismus.*

Beweis. Da f surjektiv ist auf das Bild von f ist $\bar{f}$ ebenfalls surjektiv. Der Kern von $\bar{f}$ besteht aus allen Restklassen $g\ker(f)$ mit $\bar{f}(g\ker(f)) = 1_{G'}$, aber

$$\bar{f}(g\ker(f)) = f(g).$$

Damit gilt

$$\ker(\bar{f}) = \{g\ker(f), f(g) = 1_{G'}\} = \ker(f)$$

und $\ker(f)$ ist das neutrale Element in $G/\ker(f)$. Somit ist $\bar{f}$ ein Monomorphismus. □

Als Folgerung erhalten wir einige Rechenregeln für Restklassengruppen, die man sich als Kürzungsregeln merken kann:

Korollar I.4.21. *Es sei G eine Gruppe.*

(a) *Ist $H < G$ und $N \lhd G$, so ist $H/N \cap H$ isomorph zu NH/N.*

(b) *Sind H, H' normale Untergruppen von G und ist $H' < H$, so ist H/H' eine normale Untergruppe von G/H' und*

$$(G/H')/(H/H') \cong G/H.$$

BEWEIS. Für (a) zeigen wir zunächst, dass NH eine Untergruppe von G ist. Wir benutzen dazu das Kriterium, welches Sie in einer Übungsaufgabe erarbeitet haben. Es seien also $n_1, n_2 \in N$ und $h_1, h_2 \in H$. Dann ist

$$n_1h_1(n_2h_2)^{-1} = n_1h_1h_2^{-1}n_2^{-1} = n_1h_1h_2^{-1}n_2^{-1}h_2h_1^{-1}h_1h_2{-}1.$$

Wegen der Normalität von N in G gilt $h_1h_2^{-1}n_2^{-1}h_2h_1^{-1} \in N$. Da N eine Untergruppe ist, ist auch

$$n_1h_1h_2^{-1}n_2^{-1}h_2h_1^{-1} \in N$$

und damit insgesamt $n_1h_1h_2^{-1}n_2^{-1}h_2h_1^{-1}h_1h_2{-}1$ in NH.

Die Untergruppe N ist normal in G. Daher ist sie erst recht normal in $NH < G$. Wir bilden H nach NH/N ab, indem wir $f\colon H \to NH/N$ definieren als

$$f(h) = hN.$$

Wir können f auffassen als eine Verkettung von Homomorphismen; die Inklusion von H nach NH gefolgt von der Projektion $NH \to NH/N$. Daher ist f ein Homomorphismus. Ist h im Kern von f, so ist $hN = N$ und damit ist $h \in N$. Nach Annahme ist h ein Element in H, so dass es ein Element aus $H \cap N$ ist.

Die Normalität von N impliziert weiterhin, dass jedes nhN geschrieben werden kann als $nhN = hh^{-1}nhN = hN$, so dass f surjektiv ist. Die Behauptung folgt nun mit dem Isomorphiesatz.

Für (b) überlegen wir zunächst, dass aus $H' < H$, $H' \lhd G$ und $H \lhd G$ schon folgt, dass $H' \lhd H$ gilt. Insbesondere macht die Restklassengruppe H/H' Sinn.

Wir definieren

$$f\colon G/H' \to G/H, \quad f(gH') = gH.$$

Die Abbildung f ist ein Homomorphismus. Sie ist sichtbar surjektiv und für den Kern von f berechnen wir

$$\begin{aligned}\ker(f) &= \{gH', gH = H\}\\ &= \{gH', g \in H\}\\ &= \{hH', h \in H\} = H/H'.\end{aligned}$$

□

Bemerkung I.4.22. Vorsicht! Die Eigenschaft der Normalität ist nicht transitiv: Ist $N_1 \lhd N_2$ und $N_2 \lhd G$, so folgt nicht, dass N_1 normal ist in G. Sie überlegen sich in den Übungsaufgaben ein Beispiel.

Vorlesung 5

I.5. Produkte und semidirekte Produkte von Gruppen

Produkte von Gruppen sind so definiert, wie Sie das erwarten:

Definition I.5.1. Es seien $G_1, \dots, G_n$ Gruppen. Die Produktmenge

$$\prod_{i=1}^{n} G_i = G_1 \times \dots \times G_n = \{(g_1, \dots, g_n), g_i \in G_i\}$$

ist mit der komponentenweisen Verknüpfung, dem neutralen Element $(1_{G_1}, \dots, 1_{G_n})$ und der komponentenweisen Inversenbildung eine Gruppe, die das *Produkt der Gruppen* $G_1, \dots, G_n$ genannt wird.

Machen Sie sich bitte die Gruppenstruktur explizit klar.

Bemerkung I.5.2. Da die Verknüpfung komponentenweise definiert ist, gilt für das Zentrum des Produkts

$$Z(\prod_{i=1}^{n} G_i) = \prod_{i=1}^{n} Z(G_i).$$

Insbesondere ist das Produkt genau dann abelsch, wenn alle G_i abelsch sind.

Sie können die obige Definition auf beliebige Familien von Gruppen ausdehnen und für eine Familie $(G_i)_{i\in I}$ das Produkt $\prod_{i\in I} G_i$ wie oben definieren.

Satz I.5.3. *Es seien $G_1, \ldots, G_n$ Gruppen und $N_i \lhd G_i$ sei jeweils ein Normalteiler in G_i. Dann ist $N = N_1 \times \ldots \times N_n$ ein Normalteiler von $G = G_1 \times \ldots \times G_n$ und*

$$G/N \cong G_1/N_1 \times \ldots \times G_n/N_n.$$

Beweis. Es sei $\pi_i \colon G_i \to G_i/N_i$ für $1 \leqslant i \leqslant n$ jeweils die kanonische Projektion. Dann ist

$$\pi \colon G \to G_1/N_1 \times \ldots \times G_n/N_n, \quad (g_1, \ldots, g_n) \mapsto (\pi_1(g_1), \ldots, \pi_n(g_n))$$

ein Epimorphismus. Der Kern von π ist genau $N = N_1 \times \ldots \times N_n$. Damit ist N ein Normalteiler von G und mit dem Isomorphiesatz folgt die Behauptung. □

Es gilt immer, dass $G_i \lhd G_i$ und $\{1_{G_i}\} \lhd G_i$. Damit erhalten wir:

Korollar I.5.4. *Ist $G = G_1 \times G_2$, so ist G_1 isomorph zu $G/\{1_{G_1}\} \times G_2$ und G_2 ist isomorph zu $G/G_1 \times \{1_{G_2}\}$.*

Oft ist es nicht offensichtlich, dass man eine gegebene Gruppe als Produkt von Gruppen schreiben kann. Dazu ist das folgende Konzept hilfreich.

Definition I.5.5. Ist G eine Gruppe und sind $N_i \lhd G$ Normalteiler für $1 \leqslant i \leqslant n$. Dann heißt G das *innere Produkt von $N_1, \ldots, N_n$*, falls gilt:

(a) $G = N_1 \cdot \ldots \cdot N_n$,
(b) $N_i \cap (N_1 \cdot \ldots \cdot N_{i-1} \cdot N_{i+1} \cdot \ldots \cdot N_n) = \{1_G\}$ für alle $1 \leqslant i \leqslant n$.

Für $n = 2$ läßt sich also jedes Element in G als Produkt von Elementen aus N_1 und N_2 schreiben und der Schnitt von N_1 und N_2 besteht nur aus dem neutralen Element.

Satz I.5.6. *Ist $G = N_1 \cdot \ldots \cdot N_n$ inneres Produkt der N_i, so ist G isomorph zu $\prod_{i=1}^n N_i$.*

Beweis. Es sei $g_i \in N_i$. Wir definieren eine Abbildung

$$\phi \colon \prod_{i=1}^n N_i \to G$$

durch $\phi(g_1, \ldots, g_n) = g_1 \cdot \ldots \cdot g_n$. Wegen (a) ist dies ein Element aus G.

Ist $g_i \in N_i$ und $g_j \in N_j$ für $i \neq j$, so ist

$$g_i g_j g_i^{-1} g_j^{-1} = g_i(g_j g_i^{-1} g_j^{-1}) = (g_i g_j g_i^{-1}) g_j^{-1}.$$

Da die N_k normale Untergruppen von G sind, besagt die erste Umformulierung, dass $g_i g_j g_i^{-1} g_j^{-1}$ ein Element von N_i ist und die zweite identifiziert es als Element von N_j. Also ist $g_i g_j g_i^{-1} g_j^{-1} \in N_i \cap N_j = \{1_G\}$ und somit

$$g_i g_j = g_j g_i.$$

Wir können also die g_i im Produkt permutieren. Damit ist ϕ ein Homomorphismus.

Da $G = N_1 \cdot \ldots \cdot N_n$ ist, ist ϕ surjektiv. Ist $\phi(g_1, \ldots, g_n) = 1_G$, so gilt für jedes g_i, dass

$$g_i = \Big(\prod_{\substack{j=1 \\ j\neq i}}^n g_j \Big)^{-1} \in N_i \cap (N_1 \cdot \ldots \cdot N_{i-1} \cdot N_{i+1} \cdot \ldots \cdot N_n) = \{1_G\}.$$

Dies zeigt die Injektivität von ϕ. □

Wir wollen Restklassengruppen von $\mathbb{Z}$ als Produkte schreiben. Dazu brauchen wir die folgende Hilfsaussage, die viele andere Anwendungen hat.

Satz I.5.7 (Satz von Bézout)**.** *Es seien $a, b \in \mathbb{Z}$ mit $\mathsf{ggT}(a, b) = d$. Dann gibt es ganze Zahlen r, s mit $d = ra + sb$.*

Étienne Bézout (1730–1783).

BEWEIS. Wir betrachten die Menge

$$a\mathbb{Z} + b\mathbb{Z} \subset \mathbb{Z}.$$

Dies ist eine nicht-triviale Untergruppe von $\mathbb{Z}$ und daher von der Form $d\mathbb{Z}$ für ein $d \in \mathbb{N}$. Insbesondere ist d ein Element von $a\mathbb{Z} + b\mathbb{Z}$. Wir können d also schreiben als $d = ar + bs$ mit $r, s \in \mathbb{Z}$.

Ist x eine ganze Zahl, die a und b teilt, dann teilt x somit auch d. Damit ist d der größte gemeinsame Teiler von a und b. □

Mit dem Satz von Bézout können wir einige Gruppen der Form $\mathbb{Z}/k\mathbb{Z}$ vereinfachen:

Satz I.5.8. *Sind $m, n \in \mathbb{N}$ und $\mathsf{ggT}(m, n) = 1$. Dann ist*

$$\mathbb{Z}/nm\mathbb{Z} \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}.$$

Beachten Sie, dass die Verknüpfung in $\mathbb{Z}$ die Addition ist.

BEWEIS. Wir kürzen die Nebenklasse $i + mn\mathbb{Z} \in \mathbb{Z}/nm\mathbb{Z}$ mit $\bar{i}$ ab. Die Elemente $\bar{n}$ und $\bar{m}$ sind nicht-trivial in $\mathbb{Z}/nm\mathbb{Z}$ und es gilt genauer

$$\mathsf{ord}(\bar{n}) = m \text{ und } \mathsf{ord}(\bar{m}) = n.$$

Die Gruppen $\langle\bar{n}\rangle$ und $\langle\bar{m}\rangle$ sind Untergruppen von $\mathbb{Z}/nm\mathbb{Z}$ und weil $\mathbb{Z}$ und somit $\mathbb{Z}/nm\mathbb{Z}$ abelsch ist, sind diese Untergruppen Normalteiler von $\mathbb{Z}/nm\mathbb{Z}$.

Der Schnitt der beiden Untergruppen $\langle\bar{n}\rangle \cap \langle\bar{m}\rangle$ ist eine Untergruppe U sowohl von $\langle\bar{n}\rangle$ als auch von $\langle\bar{m}\rangle$ Nach dem Satz von Lagrange I.4.3 teilt dann die Mächtigkeit von U sowohl m als auch n. Da aber n und m teilerfremd sind, gilt. dass $|U| = 1$ ist, somit ist

$$\langle\bar{n}\rangle \cap \langle\bar{m}\rangle = \{\bar{0}\}.$$

Der Satz von Bézout besagt, dass es $r, s \in \mathbb{Z}$ gibt, so dass

$$1 = nr + ms.$$

Also ist für alle $\ell \in \mathbb{Z}$

$$\ell = \ell rn + \ell sm$$

und in $\mathbb{Z}/nm\mathbb{Z}$ können wir $\bar{\ell}$ schreiben als

$$\bar{\ell} = \overline{\ell rn} + \overline{\ell sm}$$

und somit ist $\langle\bar{n}\rangle + \langle\bar{m}\rangle = \mathbb{Z}/nm\mathbb{Z}$.

Mit Satz I.5.6 erhalten wir

$$\mathbb{Z}/nm\mathbb{Z} \cong \langle\bar{n}\rangle \times \langle\bar{m}\rangle.$$

Als eine zyklische Gruppe der Ordnung m ist $\langle\bar{n}\rangle$ isomorph zu $\mathbb{Z}/m\mathbb{Z}$ und $\langle\bar{m}\rangle$ ist isomorph zu $\mathbb{Z}/n\mathbb{Z}$. □

Beispiel I.5.9. Vorsicht! Die Voraussetzung, dass n und m teilerfremd sind ist wirklich notwendig in Satz I.5.8. Zum Beispiel ist $\mathbb{Z}/4\mathbb{Z}$ *nicht* isomorph zu $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Die Gruppe $\mathbb{Z}/4\mathbb{Z}$ hat die Elemente $\{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$ und sie ist zyklisch der Ordnung 4. In $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ haben wir dagegen die Elemente

$$e = (\bar{0}, \bar{0}), a_1 = (\bar{0}, \bar{1}), a_2 = (\bar{1}, \bar{0}) \text{ und } a_3 = (\bar{1}, \bar{1})$$

und es gelten die Relationen

$$a_1 + a_2 = a_3, a_1 + a_3 = a_2, a_2 + a_3 = a_1.$$

Diese Gruppe ist isomorph zur *Kleinschen Vierergruppe*, die Sie aus einer Übungsaufgabe kennen. Insbesondere ist diese Gruppe nicht zyklisch. Felix Christian Klein (1849–1925).

Ein klassisches elementares Resultat ist der folgende Satz:

Satz I.5.10 (Chinesischer Restsatz)**.** *Es seien $n, m \in \mathbb{N}$ teilerfremde Zahlen und $a, b \in \mathbb{Z}$ beliebig. Dann gibt es ein $r \in \mathbb{Z}$ mit*

$$\bar{r} = \bar{a} \in \mathbb{Z}/m\mathbb{Z} \text{ und } \bar{r} = \bar{b} \in \mathbb{Z}/n\mathbb{Z}.$$

Man sagt auch, dass dieses r die simultanen Kongruenzbedingungen erfüllt: Es ist kongruent zu a modulo m und kongruent zu b modulo n, das heißt, dass es den gleichen Rest wie a und b ergibt beim Teilen durch m beziehungsweise n. Wir schreiben auch

$$r \equiv a \bmod m \text{ und } r \equiv b \bmod n.$$

Beweis. Wir betrachten den Gruppenhomomorphismus

$$\varrho\colon \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}, \quad x \mapsto (x + m\mathbb{Z}, x + n\mathbb{Z}).$$

Der Kern von ϱ sind die Vielfachen von nm, also $\ker(\varrho) = nm\mathbb{Z}$. Mit dem Isomorphiesatz ist das Bild von ϱ damit isomorph zu $\mathbb{Z}/nm\mathbb{Z}$, aber dies ist isomorph zu $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ nach Satz I.5.8. Also ist ϱ surjektiv. Insbesondere gibt es für das Element $(\bar{a}, \bar{b}) \in \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ ein Urbild $r \in \mathbb{Z}$. □

Vorsicht! Das Element r ist nicht eindeutig, weil ϱ einen nicht-trivialen Kern hat.

Nicht alle Gruppen lassen sich als Produkte von Gruppen schreiben:

Beispiel I.5.11. Es sei G die Menge aller Abbildungen

$$T_{a,b}\colon \mathbb{R} \to \mathbb{R}, \quad T_{a,b}(t) = at + b, \quad a \in \mathbb{R} \setminus \{0\}, b \in \mathbb{R}.$$

Mit der Verkettung von Abbildungen wird G zu einer Gruppe. Wir betrachten die Untergruppen

$$N := \{T_{1,b}, b \in \mathbb{R}\}, \quad H := \{T_{a,0}, a \neq 0\}.$$

Dies sind die Untergruppen der Translationen beziehungsweise Streckungen in G. In diesem Fall ist N ein Normalteiler von G, aber H ist nur eine Untergruppe. Es gilt trotzdem $N \cap H = \{T_{1,0}\}$ und $T_{1,0}$ ist die identische Abbildung, also das neutrale Element. Jedes $T_{a,b}$ läßt sich eindeutig schreiben als

$$T_{a,b} = T_{1,b} \circ T_{a,0}.$$

Definition I.5.12. Ist G eine Gruppe mit $N \lhd G$ und $H < G$, dann heißt G das *semidirekte Produkt von N und H*, $G = N \rtimes H$, falls

(a) $G = NH$
(b) $H \cap N = \{1_G\}$.

Bitte verdeutlichen Sie sich den Unterschied zur Definition des inneren Produktes!

Die Gruppe aus Beispiel I.5.11 ist also das semidirekte Produkt aus der normalen Untergruppe der Translationen mit der Untergruppe der Streckungen.

Bemerkung I.5.13.

- Jedes $g \in G = N \rtimes H$ kann eindeutig geschrieben werden als $g = nh$ mit $n \in N$ und $h \in H$: Wäre
$$g = n_1h_1 = n_2h_2 \text{ mit } n_1, n_2 \in N, h_1, h_2 \in H,$$
so ergibt dies die Gleichheit $n_2^{-1}n_1 = h_2h_1^{-1}$, bei der die linke Seite in N liegt und die rechte in H. Da aber $H \cap N = \{1_G\}$ ist, erhalten wir $n_1 = n_2$ und $h_1 = h_2$.
- Für $G = N \rtimes H$ erhalten wir eine Abbildung
$$c\colon H \to \mathsf{Aut}(N), \quad h \mapsto c_h,$$
weil N normal ist. Es gilt

(I.5.1) $$n_1h_1n_2h_2 = n_1h_1n_2h_1^{-1}h_1h_2 = n_1c_{h_1}(n_2)h_1h_2.$$

- Die Abbildung von Mengen $N \times H \to G$, $(n, h) \mapsto nh$ ist also immer bijektiv. Aus (I.5.1) lesen wir ab, dass sie genau dann auch ein Homomorphismus (und damit ein Isomorphismus) ist, falls c_h die identische Abbildung in $\mathsf{Aut}(N)$ ist für alle $h \in H$, weil dann $n_1h_1n_2h_2 = n_1n_2h_1h_2$ ist.
- Wir können mit diesen Überlegungen eine extrinsische Variante des semidirekten Produktes herleiten: Sind zwei beliebige Gruppen N und H gegeben zusammen mit einem $f\colon H \to \mathsf{Aut}(N)$, so definieren wir auf der Menge $N \times H$ die Verknüpfung

(I.5.2) $$(n_1, h_1) \cdot (n_2, h_2) := (n_1f(h_1)(n_2), h_1h_2) \text{ für } n_1, n_2 \in N, h_1, h_2 \in H.$$

Satz I.5.14. *Sind N und H Gruppen und ist $f\colon H \to \mathsf{Aut}(N)$ ein Homomorphismus, so definiert* (I.5.2) *eine Gruppenstruktur G auf der Menge $N \times H$ und G ist als Gruppe isomorph zu*

$$G \cong \tilde{N} \rtimes \tilde{H},$$

wobei $\tilde{N} = N \times \{1_H\}$ und $\tilde{H} = \{1_N\} \times H$.

Vorlesung 6

Beweis. Wir rechnen nach, dass (I.5.2) eine Gruppenstruktur ergibt.

Das Element $(1_N, 1_H)$ ist das neutrale Element:

$$(n,h)(1_N,1_H) = (nf(h)(1_N), h1_H).$$

Da $f(h) \in \mathsf{Aut}(N)$ ist, muss es 1_N wieder auf 1_N abbilden. Damit ist das obige Produkt gleich (n,h).

Das inverse Element zu (n,h) ist $(f(h)^{-1}(n^{-1}), h^{-1})$:

$$\begin{aligned}(n,h)(f(h)^{-1}(n^{-1}),h^{-1}) &= (nf(h)(f(h)^{-1}(n^{-1}), hh^{-1})\\ &= (nn^{-1}, hh^{-1})\\ &= (1_N, 1_H).\end{aligned}$$

Sie rechnen nach, dass die Verknüpfung assoziativ ist.

Wir betrachten die Abbildung $\varrho\colon G \to H$, die (n,h) auf h abbildet. Dann ist ϱ ein Homomorphismus mit Kern $\tilde{N}$. Somit ist $\tilde{N}$ ein Normalteiler von G.

Die Definition der Gruppenstruktur besagt, dass $\tilde{H}$ eine Untergruppe von G ist. Wir rechnen nun nach, dass $G = \tilde{N} \rtimes \tilde{H}$ gilt:

Der Schnitt von $\tilde{N}$ und $\tilde{H}$ ist $\{(1_N, 1_H)\} = \{1_G\}$.

Es gilt $\tilde{N}\tilde{H} = G$, weil

$$(n,1_H)(1_N,h) = (nf(1_H)(1_N), 1_H h) = (n,h).$$

□

Bemerkung I.5.15. Wir haben in dem obigen Satz eine Gruppe G als semidirektes Produkt $\tilde{N} \rtimes \tilde{H}$ identifiziert. Oft vereinfacht man die Notation wieder und schreibt nur $N \rtimes H$, auch wenn das natürlich sehr verwirrend sein kann.

I.6. Operationen von Gruppen auf Mengen

Gruppen tauchen häufig als Symmetriegruppen geometrischer Objekte auf. So bilden zum Beispiel die Drehungen des $\mathbb{R}^3$, die auf dem Ikosaeder als Symmetrien wirken, eine Gruppe, die isomorph ist zur alternierenden Gruppe A_5.

Wir hatten für eine nichtleere Menge X die Menge der bijektiven Abbildungen $f\colon X \to X$ mit Σ_X bezeichnet. Jede Gruppe G hat eine unterliegende Menge.

Definition I.6.1. Es sei G eine Gruppe. Für ein $g \in G$ sei $L_g \in \Sigma_G$ gegeben durch

$$L_g\colon G \to G, \quad h \mapsto gh.$$

Hier ist L_g wirklich ein Element von Σ_G. Die Umkehrabbildung zu L_g ist $L_{g^{-1}}$ und L_{1_G} ist die identische Abbildung.

Damit taucht jede Gruppe als Symmetriegruppe auf:

Satz I.6.2. *Jede Gruppe G ist isomorph zu einer Untergruppe von Σ_G.*

Beweis. Wir variieren in der obigen Definition das $g \in G$ und definieren

$$L\colon G \to \Sigma_G, \quad g \mapsto L_g.$$

Damit ist L ein Homomorphismus:

$$L_{g_1 g_2}(h) = g_1 g_2 h = L_{g_1}(g_2 h) = L_{g_1} \circ L_{g_2}(h).$$

Ist $g \in \ker(L)$, so ist $L_g(h) = gh = h$ für alle $h \in G$. Dies impliziert aber, dass $g = 1_G$ ist. Somit ist L injektiv und G ist isomorph zum Bild von G unter L. Da $\mathrm{Bild}(L) < \Sigma_G$ gilt, folgt die Behauptung. □

Wir wollen Gruppen auf allgemeinen Mengen wirken lassen:

Definition I.6.3. Es sei G eine Gruppe und X eine nichtleere Menge. Dann *operiert G auf X*, wenn es eine Abbildung

$$G \times X \to X, \quad (g, x) \mapsto gx$$

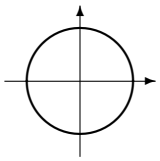
gibt mit

(a) $(gh)x = g(hx)$ für alle $g, h \in G$ und $x \in X$.
(b) $1_G x = x$.

Eine Menge X mit einer G-Operation heißt *G-Menge*.

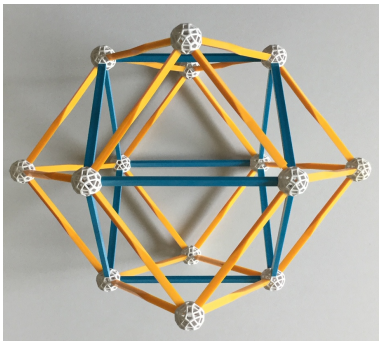
Beispiel I.6.4. Betrachten wir den griechischen Buchstaben Φ als Teilmenge des $\mathbb{R}^2$, wobei der senkrechte Strich in Φ auf der y-Achse liegt und Φ achsensymmetrisch eingebettet ist. Dann ist Φ eine $\mathbb{Z}/2\mathbb{Z}$-Menge, weil $\mathbb{Z}/2\mathbb{Z}$ durch die Spiegelung an der y-Achse auf Φ operiert. Das Element $\bar{0} \in \mathbb{Z}/2\mathbb{Z}$ operiert als identische Abbildung und $\bar{1}$ durch die Spiegelung.

Beispiel I.6.5. Wir betrachten $S^1 = \{z \in \mathbb{C}, |z| = 1\}$, die Einheitskreislinie in $\mathbb{C}$.



Diese ist eine $O(2)$-Menge, weil Drehungen und Spiegelungen des $\mathbb{R}^2$ die S^1 wieder auf sich abbilden. Die Elemente aus $O(2)$ sind ja gerade die längenerhaltenden linearen Abbildungen des $\mathbb{R}^2$ auf sich.

Beispiel I.6.6. Das Rhombendodekaeder `https://en.wikipedia.org/wiki/Rhombic_dodecahedron` ist ein Polyeder mit zwölf rhombenförmigen Flächen.



In dem Foto sehen Sie, dass Sie ihn aus einem Würfel wachsen lassen können. Welche Symmetrien erkennen Sie? Sind die Symmetrien des eingeschriebenen Würfels die gleichen wie die des Rhombendodekaeders?

Beispiel I.6.7. Das Ikosaeder `https://de.wikipedia.org/wiki/Ikosaeder` ist ein regelmäßiges Polyeder mit 20 Flächen, die aus regelmäßigen Dreiecken bestehen. Die Symmetriegruppe $I \subset SO(3)$ ist die berühmte (reine) Ikosaedergruppe. Sie ist isomorph zur A_5. Felix Klein hat ein ganzes Buch über sie geschrieben [**2**]. Welche Symmetrien entsprechen den 5-Zykeln? Welche den 3-Zykeln?

Bemerkung I.6.8. Eine Gruppe G operiert genau dann auf einer nichtleeren Menge X, wenn es einen Homomorphismus $\varrho\colon G \to \Sigma_X$ gibt: Ist ϱ gegeben, so setzen wir $gx := \varrho(g)(x)$. Die Tatsache, dass ϱ ein Homomorphismus ist, besagt, dass die Eigenschaften (a) und (b) einer Operation erfüllt sind. Umgekehrt, ist X eine G-Menge, so definieren wir $\varrho(g)$ durch $\varrho(g)(x) = gx$ für alle $x \in X$. Die Axiome einer Gruppenoperation besagen dann, dass ϱ ein Homomorphismus ist.

Satz I.6.9. *Es sei G eine Gruppe und X eine G-Menge. Dann definiert*

$$R_G = \{(x, y) \in X \times X, \exists g, gx = y\}$$

eine Äquivalenzrelation auf X.

BEWEIS. Sind $(x,y) \in R_G$ und $(y,z) \in R_G$, so gibt es $g_1, g_2 \in G$ mit

$$g_1 x = y, \quad g_2 y = z.$$

Dann ist aber $g_2 g_1 x = z$, so dass $(x,z) \in R_G$ und R_G ist transitiv.

Da $1_G x = x$ ist $(x,x) \in R_G$ für alle $x \in X$ und die Relation ist reflexiv.

Ist $gx = y$, dann ist $g^{-1} y = x$. Dies zeigt die Symmetrie von R_G. □

Definition I.6.10. Ist X eine G-Menge, so heißen die Äquivalenzklassen der Relation R_G die *Bahnen* beziehungsweise die *Orbits* der Operation.

Wir benutzen die Notation

$$[x] = \{y \in X, (x,y) \in R_G\}.$$

Dies läßt sich elementar schreiben als

$$[x] = \{y \in X, \exists g \in G : gx = y\}$$

und dies wird oft mit Gx notiert.

Sie wissen, dass Äquivalenzrelationen die Menge in disjunkte Teilmengen zerlegt. Hier bekommen wir die Zerlegung von X in Bahnen:

$$X = \bigsqcup_x [x] = \bigsqcup_x Gx,$$

wobei x über ein Repräsentantensystem läuft.

Beispiel I.6.11. Betrachten wir die Operation der $SO(2)$ auf $\mathbb{R}^2$

$$SO(2) \times \mathbb{R}^2 \to \mathbb{R}^2, \quad (A,x) \mapsto Ax$$

so ist für ein festes $0 \neq x \in \mathbb{R}^2$ die Bahn genau die Kreislinie

$$\{y \in \mathbb{R}^2, |y| = |x|\}.$$

Für $x = 0$ besteht die Bahn $SO(2)0$ nur aus dem Nullpunkt.

Beispiele I.6.12.

- Es sei G eine beliebige Gruppe und $X \neq \varnothing$ eine beliebige Menge. Wir können die Operation betrachten, die gegeben ist durch

  $$gx = x \text{ für alle } g \in G, x \in X.$$

  Dies definiert eine Operation von G auf X, die sogenannte *triviale Operation.*
- Jede Gruppe G operiert auf sich selbst durch die Verknüpfung in G:

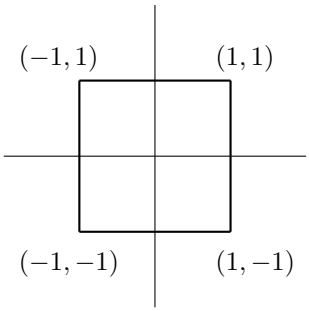
  $$G \times G \to G, (g,h) \mapsto gh.$$

- Ist V ein Vektorraum und ist $GL(V)$ die Gruppe der Automorphismen von V, so operiert $GL(V)$ auf V durch $(f,v) \mapsto f(v)$.
- Es sei X_n ein regelmäßiges n-Eck, welches symmetrisch um $(0,0)$ in den $\mathbb{R}^2$ eingebettet ist. Wir betrachten die Drehmatrix

  $$R_n = \begin{pmatrix} \cos(2\pi/n) & -\sin(2\pi/n) \\ \sin(2\pi/n) & \cos(2\pi/n) \end{pmatrix}.$$

  Dann operiert die Gruppe $\langle R_n \rangle$ auf X_n, indem wir R_n wie gewohnt auf dem $\mathbb{R}^2$ operieren lassen. Die Gruppe $\langle R_n \rangle$ hat genau n Elemente.

  Für $n = 4$ erhalten wir X_4, welches wir uns als Quadrat mit den Ecken $(1,1)$, $(1,-1)$, $(-1,1)$ und $(-1,-1)$ vorstellen.



In diesem Beispiel ist die Bahn des Punktes $(0,1)$ unter der Gruppenoperation

$$\langle R_4\rangle(0,1) = \{(0,1),(-1,0),(0,-1),(1,0)\}.$$

- Ist $H < G$ eine Untergruppe, so ist die Menge G/H der Linksnebenklassen eine G-Menge, indem wir setzen

$$G \times G/H \to G/H, \quad (g, \tilde{g}H) \mapsto g\tilde{g}H.$$

Vorlesung 7

Definition I.6.13. Es sei X eine G-Menge. Der *Stabilisator von $x \in X$* ist die Menge

$$G_x := \{g \in G, gx = x\}.$$

Bemerkung I.6.14. Rechnen Sie nach, dass für alle $x \in X$ der Stabilisator eine Untergruppe von G ist. Für den Stabilisator sind auch die Begriffe *Isotropiegruppe* und *Standgruppe* üblich.

Die Bahn eines Elementes läßt sich mit dem Stabilisator in Beziehung setzen:

Satz I.6.15. *Es sei G eine Gruppe und X eine G-Menge. Dann gibt es für jedes $x \in X$ eine Bijektion von Mengen*

$$G/G_x \cong Gx$$

zwischen den Linksnebenklassen von G_x in G und der Bahn von x unter der G-Operation.

Vorsicht: Da G_x im Allgemeinen keine normale Untergruppe ist und da Gx nur eine Menge ist, ist behauptete Bijektion wirklich nur eine Bijektion von Mengen.

Beweis. Wir definieren eine Abbildung $\psi\colon G/G_x \to Gx$ durch

$$\psi(gG_x) := gx.$$

Diese Abbildung ist wohldefiniert: Ist $g_1G_x = g_2G_x$, so gibt es ein $h \in G_x$ mit $g_2 = g_1h$. Damit ist

$$\psi(g_2G_x) = g_2x = g_1hx = g_1x = \psi(g_1G_x),$$

weil $hx = x$.

Nach Konstruktion ist ψ surjektiv. Nehmen wir an, dass

$$\psi(g_1G_x) = \psi(g_2G_x)$$

gilt für $g_1, g_2 \in G$. Dann ist nach Definition von ψ $g_1x = g_2x$ und somit $g_2^{-1}g_1x = x$. Damit ist aber $g_2^{-1}g_1 \in G_x$ und $g_1G_x = g_2G_x$. □

Korollar I.6.16 (Bahnenformel)**.** *Ist G eine endliche Gruppe und ist X eine G-Menge, so gilt für alle $x \in X$:*

$$|G| = |G_x||Gx|.$$

Insbesondere teilt die Mächtigkeit jeder Bahn $|Gx|$ die Gruppenordnung und es gilt $|Gx| = [G : G_x]$.

Beispiel I.6.17. Betrachten wir wiederum das Beispiel $\Phi \subset \mathbb{R}^2$ aus Beispiel I.6.4. Die Punkte in Φ, die auf der y-Achse liegen, werden von $\mathbb{Z}/2\mathbb{Z}$ nicht bewegt. Hier erhalten wir Bahnen der Mächtigkeit 1. Alle anderen Punkte in Φ werden von $\mathbb{Z}/2\mathbb{Z}$ bewegt und wir erhalten für diese Punkte Bahnen der Mächtigkeit 2.

Definition I.6.18.

(a) Ein *Repräsentantensystem einer G-Menge X* ist eine Teilmenge $Y \subset X$, so dass gilt:
- Für alle $x \in X$ gibt es ein $y \in Y$ mit $Gx = Gy$.
- Für alle $y_1, y_2 \in Y$ gilt: Ist $y_1 \neq y_2$, so gilt $Gy_1 \cap Gy_2 = \varnothing$.

(b) Ist X eine G-Menge, so heißt $x \in X$ ein *Fixpunkt der G-Operation*, falls $|Gx| = 1$, also $gx = x$ für alle $g \in G$. Mit $\mathsf{Fix}_G(X)$ bezeichnen wir die Menge aller Fixpunkte der G-Operation auf X.

Satz I.6.19. *Ist G eine endliche Gruppe und ist X eine endliche G-Menge, dann gilt:*

(a)
$$|X| = \sum_{y \in Y} [G : G_y] = |\mathsf{Fix}_G(X)| + \sum_{\substack{y \in Y, \\ [G:G_y] > 1}} [G : G_y].$$
Hierbei ist Y ein Repräsentantensystem der G-Menge X.

(b) *Ist $|G| = p^r$ mit $r \in \mathbb{N}$ und einer Primzahl p, dann ist*
$$|X| \equiv |\mathsf{Fix}_G(X)| \text{ mod } p.$$
Insbesondere gibt es mindestens einen Fixpunkt, falls p und $|X|$ teilerfremd sind.

Beweis. Zu (a): Da X die disjunkte Vereinigung der Bahnen ist, erhalten wir sofort
$$|X| = \sum_{y \in Y} |Gy|.$$
Nach der Bahnenformel I.6.16 gilt $|Gy| = [G : G_y]$. Da y nur genau dann ein Fixpunkt ist, wenn $|Gy| = 1$, muss jeder Fixpunkt in Y enthalten sein.

Zu (b): Wir haben nach (a)
$$|X| - |\mathsf{Fix}_G(X)| = \sum_{\substack{y \in Y, \\ [G:G_y] > 1}} [G : G_y].$$
Mit dem Satz von Lagrange wissen wir, dass hier gilt
$$[G : G_y] = p^i \text{ für ein } 1 \leqslant i \leqslant r.$$
Damit ist aber
$$|X| - |\mathsf{Fix}_G(X)| \equiv 0 \text{ mod } p.$$
□

Definition I.6.20. Es sei X eine G-Menge.

(a) Ist $X = Gx$ für ein $x \in X$, so heißt die G-Operation *transitiv*.

(b) Ist die Abbildung $\varrho\colon G \to \Sigma_X$, die zur Gruppenoperation gehört, injektiv, so heißt die G-Operation *treu*.

Bemerkung I.6.21. Diese Begriffe sind zentral für Gruppenoperationen. Was bedeutet transitiv? Ist $X = Gx$ für ein $x \in X$, dann ist jedes $y \in X$ von der Form gx. Wir können also alle Elemente $y \in X$ durch die Gruppenwirkung von x ausgehend erreichen. Ist $y_1 = g_1 x$ und $y_2 = g_2 x$, so erhalten wir auch
$$y_1 = g_1 x = g_1 g_2^{-1} g_2 x = g_1 g_2^{-1} y_2.$$
Somit ist x mit seiner Eigenschaft nicht speziell: Wir können jedes Element nehmen, um X als Bahn darzustellen, und je zwei Elemente in X sind durch die G-Operation ineinander überführbar: Für alle $y_1, y_2 \in X$ gibt es ein $g \in G$ mit $y_1 = g y_2$.

Für die Treuheit einer Operation betrachten wir den Homomorphismus
$$\varrho\colon G \to \Sigma_X, \quad \varrho(g)(x) = gx.$$
Ist ϱ injektiv, so wird nur 1_G auf id_X abgebildet. Die Operation ist also genau dann treu, wenn es für alle $g \neq 1_G$ ein $x \in X$ gibt mit $gx \neq x$. Kein Element $1_G \neq g \in G$ operiert also trivial.

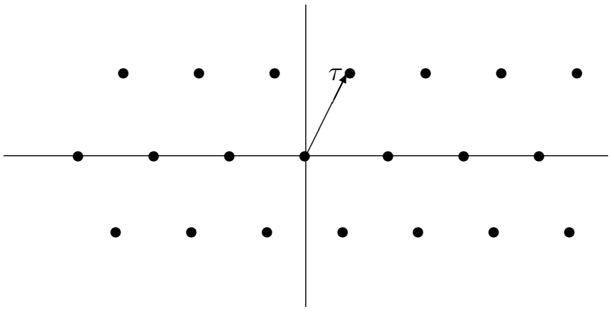
Ein wichtiges Beispiel für Gruppenoperationen kommt von Gittern:

Beispiel I.6.22. Es sei

$$\mathcal{H} := \{z \in \mathbb{C}, \mathrm{Im}(z) > 0\}$$

die obere Halbebene in $\mathbb{C}$. Wir definieren für ein festes $\tau \in \mathcal{H}$ das *Gitter*

$$\Gamma_\tau := \mathbb{Z} + \mathbb{Z}\tau = \{x + y\tau, x, y \in \mathbb{Z}\}.$$



Das Gitter Γ_τ operiert auf $\mathbb{C}$ durch die Translation um Gittervektoren:

$$\Gamma_\tau \times \mathbb{C} \to \mathbb{C}, \quad (x + y\tau, z) \mapsto x + y\tau + z.$$

Ist $x + y\tau + z = z$, so ist $x + y\tau = 0$, also ist die Operation treu. Ist sie auch transitiv?

Ein wichtiges Beispiel innerhalb der Welt der Gruppen ist das Folgende:

Beispiel I.6.23. Es sei G eine Gruppe und

$$\mathcal{U}(G) := \{H, H < G\}$$

sei die Menge aller Untergruppen von G. Wir definieren die Operation

$$G \times \mathcal{U}(G) \to \mathcal{U}(G), \quad (g, H) \mapsto gHg^{-1}.$$

Definition I.6.24. Die Bahnen der Operation aus Beispiel I.6.23 heißen die *Konjugationsklassen von Untergruppen von G*.

Wann ist $H \in \mathsf{Fix}_G(\mathcal{U}(G))$? Das ist genau dann der Fall, wenn für alle $g \in G$ gilt: $gHg^{-1} = H$ und dies ist genau dann wahr, wenn H eine normale Untergruppe von G ist, also

$$\mathsf{Fix}_G(\mathcal{U}(G)) = \{N \in \mathcal{U}(G), N \lhd G\}.$$

Was ist der Stabilisator eines $H \in \mathcal{U}(G)$, also G_H? Dies sind alle $g \in G$ mit $gHg^{-1} = H$.

Definition I.6.25. Es sei G eine Gruppe und $H < G$. Der *Normalisator von H in G* ist $G_H = \{g \in G, gHg^{-1} = H\}$. Die Notation ist $N_G(H)$.

Der Name *Normalisator* kommt von den folgenden Eigenschaften von $N_G(H)$.

Satz I.6.26. *Es sei G eine Gruppe und $H < G$. Dann gilt*

(a) *$N_G(H)$ ist eine Untergruppe von G.*
(b) *Die Untergruppe H ist ein Normalteiler von $N_G(H)$.*

Beweis. Für (a) zeigen wir, dass mit $g, \tilde{g} \in N_G(H)$ auch $g\tilde{g}^{-1} \in N_G(H)$ gilt. Wir wissen

$$g\tilde{g}^{-1}H(g\tilde{g}^{-1})^{-1} = g\tilde{g}^{-1}H\tilde{g}g^{-1}.$$

Da $\tilde{g}^{-1}H\tilde{g} = (\tilde{g}H\tilde{g}^{-1})^{-1}$, wobei hier die Inversenbildung elementweise erfolgt, ist $\tilde{g}^{-1}H\tilde{g} = H$. Damit ist aber auch insgesamt $g\tilde{g}^{-1}H(g\tilde{g}^{-1})^{-1} = H$, weil g ebenfalls in $N_G(H)$ ist.
Die zweite Behauptung, $H \lhd N_G(H)$ gilt nach Konstruktion von $N_G(H)$. □

Vorlesung 8

I.7. Die symmetrischen Gruppen

Wir hatten die Menge $\mathbf{n} = \{1, \dots, n\}$ für $n \in \mathbb{N}$ definiert und $\Sigma_n = \Sigma_{\mathbf{n}}$ eingeführt. Dies sind die bijektiven Selbstabbildungen von $\mathbf{n}$. Sie wissen, dass $|\Sigma_n| = n!$ gilt. Wir untersuchen die Struktur von Σ_n in diesem Abschnitt genauer.

Definition I.7.1. Ist $\sigma \in \Sigma_X$, so heißt

$$\mathsf{supp}(\sigma) := \{x \in X, \sigma(x) \neq x\}$$

der *Träger von* σ.

Der Träger sammelt also alle Elemente, die von σ bewegt werden. Die Gruppen Σ_X sind für X mit $|X| > 2$ nicht abelsch, aber falls sich zwei Elemente nicht ins Gehege kommen, dann kommutieren sie:

Lemma I.7.2. *Sind* $\sigma, \xi \in \Sigma_X$ *und ist* $\mathsf{supp}(\sigma) \cap \mathsf{supp}(\xi) = \varnothing$*, so gilt* $\sigma \circ \xi = \xi \circ \sigma$*.*

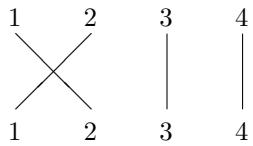
Beweis. Wir rechnen das stur nach: Ist $x \in X \setminus (\mathsf{supp}(\sigma) \cup \mathsf{supp}(\xi))$, so ist $\sigma(\xi(x)) = x = \xi(\sigma(x))$.
Wir nehmen an, dass $x \in \mathsf{supp}(\sigma)$. Dann ist $x \notin \mathsf{supp}(\xi)$, also ist $\xi(x) = x$.
Da σ eine Bijektion ist, ist $\sigma(x)$ auch ein Element von $\mathsf{supp}(\sigma)$. Damit kann es nicht in $\mathsf{supp}(\xi)$ liegen, weil der Schnitt leer ist. Also gilt dann

$$\xi(\sigma(x)) = \sigma(x).$$

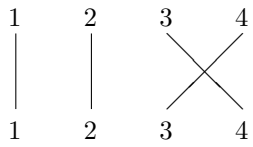
Das ist aber gleich $\sigma(\xi(x))$.
Analog rechnen Sie den Fall nach, dass x im Träger von ξ enthalten ist. □

Beispiel I.7.3. In Σ_4 betrachten wir die Transpositionen $\sigma = (1, 2)$ und $\xi = (3, 4)$. Das Element σ vertauscht also 1 und 2 und hat 3 und 4 als Fixpunkte, während ξ die Elemente 3 und 4 vertauscht und 1 und 2 fix läßt. Dann haben σ und ξ disjunkte Träger und $\sigma \circ \xi = \xi \circ \sigma$.

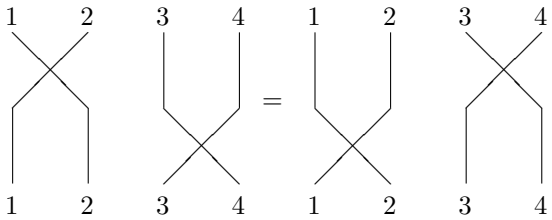
Sie können sich Permutationen für kleine n auch gut zeichnerisch klarmachen, indem Sie Diagramme benutzen, die von einer Kopie von $\mathbf{n}$ oben (Definitionsbereich) zu einer Kopie von n unten laufen. In unserem Beispiel können Sie $\sigma \in \Sigma_4$ zeichnen als



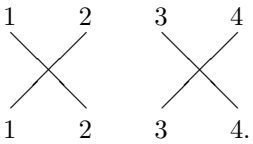
und ξ als



Dann ist die Relation $\xi \circ \sigma = \sigma \circ \xi$ ausdrückbar durch das Bild



und beides ist gleich



Definition I.7.4. Ein $\sigma \in \Sigma_X$ heißt ein *n-Zykel*, falls der Träger n-elementig ist, $\mathsf{supp}(\sigma) = \{x_1, \dots, x_n\}$, und falls es eine Umnummerierung der x_i gibt zu $y_1, \dots, y_n$, so dass $\sigma(y_i) = y_{i+1}$ gilt für $1 \leqslant i \leqslant n-1$ und $\sigma(y_n) = y_1$.

Wir benutzen die Notation $\sigma = (y_1, \dots, y_n)$ für einen solchen n-Zykel.

Beispiel I.7.5. Wir betrachten $\sigma \in \Sigma_6$ mit der Wertetabelle

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 2 & 4 & 1 & 6 \end{pmatrix}.$$

Dann ist der Träger von σ gleich $\{1, 2, 3, 5\}$ und σ ist ein 4-Zykel und zwar $\sigma = (1, 3, 2, 5)$. Wir hätten σ auch schreiben können als $(3, 2, 5, 1)$ oder $(2, 5, 1, 3)$ oder $(5, 1, 3, 2)$.

Definition I.7.6. Wir nennen 2-Zykel wie gewohnt *Transpositionen.*

Lemma I.7.7. *Ist $\sigma = (y_1, \dots, y_n)$ ein n-Zykel in Σ_N und ist $\xi \in \Sigma_N$ ein beliebiges Element, so gilt*

$$\xi\sigma\xi^{-1} = (\xi(y_1), \dots, \xi(y_n)).$$

Beweis. Es gilt

$$\xi\sigma\xi^{-1}(\xi(y_i)) = \xi\sigma(y_i) = \begin{cases} \xi(y_{i+1}), & i \leqslant n-1, \\ \xi(y_1), & i = n. \end{cases}$$

Alle Elemente in $\{1, \dots, N\}$, die nicht von der Form $\xi(y_i)$ sind, liegen nicht im Träger von $\xi\sigma\xi^{-1}$. □

Satz I.7.8. *Jedes $\sigma \in \Sigma_n$, $\sigma \neq \mathrm{id}_{\mathbf{n}}$, kann als Produkt von Zykeln mit disjunktem Träger geschrieben werden. Bis auf Reihenfolge der Faktoren ist diese Darstellung eindeutig.*

Beweis. Elemente $i_1, i_2 \in \mathbf{n}$ heißen äquivalent bezüglich σ, falls es ein $j \in \mathbb{Z}$ gibt mit $\sigma^j(i_1) = i_2$. Dies definiert eine Äquivalenzrelation. (Rechnen Sie das nach!)

Wir können also $\{1, \dots, n\}$ zerlegen als

$$\{1, \dots, n\} = \bigsqcup_{k=1}^{s} X_k,$$

wenn X_k die Äquivalenzklassen bezeichnet.

Ist $|X_k| = 1$ für ein $1 \leqslant k \leqslant s$, so ist $X_k = \{i_t\}$ mit $i_t \notin \mathsf{supp}(\sigma)$. Es sei also $|X_k| \geqslant 2$. Setze

$$\sigma_k(j) = \begin{cases} j, & j \notin X_k, \\ \sigma(j), & j \in X_k. \end{cases}$$

Ist $j \in X_k$ und ist $r_k \in \mathbb{N}$ minimal mit der Eigenschaft, dass $\sigma^{r_k}(j) = j$, so ist

$$X_k = \{j, \sigma(j), \ldots, \sigma^{r_k-1}(j)\}.$$

Definiere $y_\ell = \sigma^\ell(j)$, also

$$X_k = \{y_1, \ldots, y_{r_k}\}.$$

Dann ist

$$\sigma(y_\ell) = \begin{cases} y_{\ell+1}, & \ell < r_k \\ y_1, & \ell = r_k \end{cases}$$

und die Einschränkung von σ auf X_k ist

$$\sigma|_{X_k} = (y_1, \ldots, y_{r_k})$$

und das ist gleich σ_k. Wir können σ damit als Produkt schreiben

$$\sigma = \sigma_1 \circ \ldots \circ \sigma_s.$$

Da die Träger der σ_is disjunkt sind, kommutieren die Faktoren. □

Vorlesung 9

Wir zerlegen Permutationen in Transpositionen:

Korollar I.7.9.

(a) *Die Gruppe Σ_n (für $n \geqslant 2$) wird von Transpositionen erzeugt: Jedes $\sigma \in \Sigma_n$ kann als Produkt von Transpositionen geschrieben werden.*

(b) *Jedes $\sigma \in \Sigma_n$ kann als Produkt von Transpositionen der Form*

(i) $(1,2), (1,3), \ldots, (1,n)$ *beziehungsweise*
(ii) $(1,2), (2,3), \ldots, (n-1,n)$
geschrieben werden.

Beweis. Ist $\sigma = \mathrm{id}_{\mathbf{n}}$, so ist nichts zu zeigen. Wir schreiben sonst σ als Produkt von Zykeln mit disjunktem Träger und müssen die Behauptung damit nur für Zykel beweisen. Einen Zykel $(i_1, \ldots, i_s)$ können wir explizit als Produkt von Transpositionen

$$(i_1, \ldots, i_s) = (i_1, i_2) \circ \ldots \circ (i_{s-1}, i_s)$$

schreiben. Damit folgt (a).

Für (b) (i) schreiben wir eine beliebige Transposition (j,k) mit $j \neq 1 \neq k$ als

$$(j,k) = (1,j)(1,k)(1,j).$$

Ist $k = 1$ oder $j = 1$, so folgt die Behauptung aus $(j,k) = (k,j)$.

Für (b) (ii) verfahren wir ähnlich: Ist (j,k) eine Transposition, so ist ohne Einschränkung $j < k$. Ist $k = j+1$, so ist nichts zu zeigen. Ist $k > j+1$, so ist

$$(j,k) = (j,j+1)(j+1,k)(j,j+1).$$

Die äußeren Transpositionen sind schon von der gewünschten Form und in der inneren hat sich der Abstand um eins verringert. □

Beispiel I.7.10. Es sei $\sigma \in \Sigma_{10}$ gegeben als

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 6 & 4 & 10 & 8 & 9 & 3 & 2 & 5 & 7 & 1 \end{pmatrix}.$$

Um die Zykelzerlegung von σ zu erhalten, folgen Sie den Werten der 1 unter den Potenzen von σ. Wenn Sie wieder bei 1 ankommen, nehmen Sie einen Wert, der noch nicht vorgekommen ist; hier zum Beispiel die 2. Das ergibt

$$\sigma = (1, 6, 3, 10)(2, 4, 8, 5, 9, 7).$$

Wir können $(1, 6, 3, 10)$ als Produkt von Transpositionen schreiben

$$(1, 6, 3, 10) = (1, 6)(6, 3)(3, 10).$$

Möchten Sie zum Beispiel die Form wie in (b) (i) erreichen, dann ergibt das

$$(6, 3) = (1, 6)(1, 3)(1, 6), \quad (3, 10) = (1, 3)(1, 10)(1, 3).$$

Sie können zur Übung den zweiten Zykel in σ aufdröseln.

Vorsicht: Die Zerlegung in Transpositionen ist natürlich hochgradig nicht eindeutig!
Wir kommen jetzt zur alternativen Definition des Signums einer Permutation.

Definition I.7.11. Das *Signum einer Permutation* $\sigma \in \Sigma_n$ ist

$$\operatorname{sign}(\sigma) = \prod_{1 \leqslant i < j \leqslant n} \frac{\sigma(i) - \sigma(j)}{i - j}.$$

Lemma I.7.12. *Das Signum definiert einen Homomorphismus*

$$\operatorname{sign}\colon \Sigma_n \to \{\pm 1\}.$$

Den Beweis machen Sie in einer Übungsaufgabe.
Die folgende Definition haben wir schon gesehen:

Definition I.7.13. Der Kern von sign in Σ_n heißt die *alternierende Gruppe auf n Elementen* und wird mit A_n notiert. Die Elemente in A_n heißen manchmal auch *gerade Permutationen*.

Bemerkung I.7.14. Jede Transposition (i, j) mit $i < j$ hat $\operatorname{sign}(i, j) = -1$, weil

$$\operatorname{sign}(i, j) = \frac{j - i}{i - j}.$$

Da $(i, j) = (j, i)$, haben wir alle Fälle abgedeckt. Damit muss in der Zerlegung eines $\sigma \in A_n$ immer eine gerade Anzahl von Transpositionen vorkommen.

Ist $\sigma \in \Sigma_n$ ein k-Zykel, also $\sigma = (i_1, \ldots, i_k)$, so gilt

$$\operatorname{sign}(\sigma) = (-1)^{k+1}.$$

Das folgt aus dem Beweis von (a) des Korollars I.7.9.

Beispiele I.7.15.

- Für $n = 1$ ist die Indexmenge des Produktes in der Definition von sign leer und wir erhalten $A_1 = \Sigma_1 = \{\mathrm{id}_{\mathbf{1}}\}$.
- Die Gruppe Σ_2 hat zwei Elemente, $\mathrm{id}_{\mathbf{2}}$ und $(1, 2)$. Nur $\mathrm{id}_{\mathbf{2}}$ hat sign $= +1$, also ist $A_2 = \{\mathrm{id}_{\mathbf{2}}\}$ die triviale Gruppe.
- Die Σ_3 hat die Elemente

  $$\Sigma_3 = \{\mathrm{id}_{\mathbf{3}}, (1, 2), (1, 3), (2, 3), (1, 2, 3), (1, 3, 2)\}$$

  und A_3 ist

  $$A_3 = \{\mathrm{id}_{\mathbf{3}}, (1, 2, 3), (1, 3, 2)\} = \langle (1, 2, 3) \rangle.$$

  Dies ist eine zyklische Gruppe der Ordnung 3.

Da die Gruppen A_n immer Normalteiler in Σ_n sind, ist die Gruppe Σ_3 also nicht einfach. Es ist leicht zu sehen, dass alle Gruppen A_n für $n \geqslant 3$ nicht-trivial sind, so dass die symmetrischen Gruppen Σ_n für $n \geqslant 3$ nicht einfach sind.

Satz I.7.16. *Für jedes $n \geqslant 3$ wird die Gruppe A_n durch 3-Zykel erzeugt.*

BEWEIS. Wir wissen schon, dass in der Zerlegung jedes Elements $\sigma \in A_n$ in Transpositionen $\sigma = \tau_1 \circ \ldots \circ \tau_m$ die Anzahl der τ_i gerade sein muss. Damit wird die Gruppe A_n für $n \geqslant 3$ von Paaren von Transpositionen erzeugt. Sind $s, t, u, v \in \mathbb{N}$ paarweise verschieden, so gilt

$$(s,t)(u,v) = (s,t,u)(t,u,v).$$

Für $(s,t)(s,u)$ erhalten wir

$$(s,t)(s,u) = (s,u,t).$$

□

Beispiel I.7.17. Wir sehen uns die Gruppe A_4 genauer an. Die Kleinsche Vierergruppe ist

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

und Sie wissen schon, dass $K_4 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Wir behaupten, dass K_4 ein Normalteiler von A_4 ist. Die nicht-trivialen Elemente der K_4 sind von der Form $(i,j)(k,\ell)$, wobei $\{1,2,3,4\} = \{i,j,k,\ell\}$. Es sei $\sigma \in A_4$. Dann gilt mit Lemma I.7.7

$$\sigma(i,j)(k,\ell)\sigma^{-1} = \sigma(i,j)\sigma^{-1}\sigma(k,\ell)\sigma^{-1} = (\sigma(i),\sigma(j))(\sigma(k),\sigma(\ell)).$$

Da σ bijektiv ist, ist diese Permutation wiederum in K_4.

Die Gruppe A_4 ist also nicht einfach. Damit ist sie eine Ausnahme.

Satz I.7.18. *Die Gruppen A_n sind einfach für $n \leqslant 3$ und $n \geqslant 5$.*

Damit kennen Sie eine unendliche Familie endlicher einfacher Gruppen. Zyklische Gruppen mit Primzahlordnung sind natürlich auch einfach.

Da A_1 und A_2 die triviale Gruppe sind, ist in diesen Fällen nichts zu zeigen. Die A_3 ist eine zyklische Gruppe der Ordnung 3 und kann daher wegen des Satzes von Lagrange keine nicht-trivialen Untergruppen haben.

Es sind also die Fälle für $n \geqslant 5$ zu zeigen. Dafür brauchen wir eine Hilfsaussage:

Lemma I.7.19. *Für $n \geqslant 5$ sind je zwei 3-Zykel konjugiert in A_n.*

BEWEIS. Sind (a,b,c) und (i,j,k) 3-Zykel in A_n für $n \geqslant 5$, so sei

$$\gamma = (a,i)(b,j)(c,k) \in \Sigma_n.$$

Dann gilt mit Lemma I.7.7

$$\gamma(a,b,c)\gamma^{-1} = (i,j,k)$$

und somit sind (a,b,c) und (i,j,k) konjugiert zueinander in Σ_n.

Hat γ schon $\mathrm{sign}(\gamma) = 1$ (zum Beispiel wenn $a = i$), so sind wir fertig.

Da $n \geqslant 5$ ist, gibt es noch $r, s \in \mathbf{5} \setminus \{a,b,c\}$. Gilt $\mathrm{sign}(\gamma) = -1$, so ersetzen wir γ durch $\xi = \gamma(r,s)$. Dann ist $\xi \in A_n$ und $\xi(a,b,c)\xi^{-1} = (i,j,k)$ gilt immer noch. □

BEWEIS DES SATZES I.7.18. Wir nehmen an, dass A_n für $n \geqslant 5$ einen Normalteiler $N \lhd A_n$ mit $N \neq \{\mathrm{id}_{\mathbf{n}}\}$ besitzt. Die Beweisidee ist, zu zeigen, dass N einen 3-Zykel enthalten muss. Damit enthält N alle 3-Zykel, aber diese erzeugen A_n, so dass $N = A_n$ gelten muss.

Es sei $\mathrm{id}_{\mathbf{n}} \neq \sigma \in N$ mit der Eigenschaft, dass σ eine Permutation in $N \setminus \{\mathrm{id}_{\mathbf{n}}\}$ ist, die maximal viele Fixpunkte in $\mathbf{n}$ hat. Das heißt, ist $\xi \in N$, so dass

$$|\{i \in \mathbf{n}, \xi(i) = i\}| > |\{i \in \mathbf{n}, \sigma(i) = i\}|$$

gilt, dann ist $\xi = \mathrm{id}_{\mathbf{n}}$. Wir zerlegen $\{1, \ldots, n\}$ in die $\langle\sigma\rangle$-Orbits $X_1, \ldots, X_j$. Da $\sigma \neq \mathrm{id}_{\mathbf{n}}$, muss es ein $1 \leqslant i \leqslant j$ geben mit $|X_i| > 1$.

Wir nehmen an, dass für alle $1 \leqslant i \leqslant j$, gilt, dass $|X_i| = 2$ oder $|X_i| = 1$. Da $\mathrm{sign}(\sigma) = +1$ ist, muss es dann mindestens zwei Bahnen X_{i_1} und X_{i_2} mit zwei Elementen geben. Damit ist die Einschränkung von σ auf $X_{i_1} \cup X_{i_2}$ von der Form

$$\sigma|_{X_{i_1} \cup X_{i_2}} = (a,b)(s,t).$$

Es sei $k \in \mathbf{n}$ mit $k \neq a, b, s, t$, so dass k kein Fixpunkt von σ ist. Wir setzen $\xi = (s,t,k)$. Dann ist das Element

$$\sigma' := \xi\sigma\xi^{-1}\sigma^{-1}$$

ein Element von N, weil $\xi\sigma\xi^{-1} \in N$ wegen der Normalität von N.

Es gilt

$$\sigma'(a) = \xi\sigma\xi^{-1}\sigma^{-1}(a) = \xi\sigma\xi^{-1}(b) = \xi\sigma(b) = \xi(a) = a.$$

Ebenso hat σ' die Fixpunkte $i \in \mathbf{n} \setminus \{a, b, s, t, k\}$ von σ als Fixpunkte, so dass σ' mehr Fixpunkte hat als σ, aber σ' ist nicht die identische Abbildung, weil $\sigma'(k) \neq k$.

Das ist ein Widerspruch, also muss es mindestens eine Bahn X_ℓ geben mit $|X_\ell| \geqslant 3$: $X_\ell = \{i, j = \sigma(i), k = \sigma^2(i), \ldots\}$.

Ist $\sigma \neq (i, j, k)$, so muss es mindestens noch zwei Elemente s, t geben, so dass $\sigma(s) \neq s$ und $\sigma(t) \neq t$. (Sonst hätte σ negatives Signum.) Wir setzen wieder $\xi = (k, s, t)$ für diese s, t und sehen, dass $\tilde{\sigma} = \xi^{-1}\sigma^{-1}\xi\sigma$ wiederum in N liegt, nicht die identische Abbildung ist, aber i als zusätzlichen Fixpunkt hat.

Damit ist σ ein 3-Zykel. □

Vorlesung 10

I.8. Die Sylowsätze

Wenn Ihnen jemand sagt, dass eine Gruppe G genau 60 Elemente hat, und Sie dann fragt, wie die Gruppe aussieht, was sagen Sie dann? Die Sylowsätze (Peter Ludwig Mejdell Sylow (1832–1918)) geben keine vollständige Klassifikation endlicher Gruppen, aber sie beschreiben Strukturen, die diese Gruppen haben müssen, so dass sie helfen, endliche Gruppen zu verstehen.

Definition I.8.1. Es sei p eine Primzahl. Eine endliche Gruppe G heißt eine *p-Gruppe*, falls $|G| = p^k$ für ein $k \in \mathbb{N}$.

Beispiele I.8.2.

- $G = \mathbb{Z}/p^k\mathbb{Z}$ ist eine p-Gruppe für $k \in \mathbb{N}$.
- Die Symmetriegruppe des Quadrats ist die Diedergruppe D_8 mit $|D_8| = 8 = 2^3$. Sie ist zusammengesetzt aus der Untergruppe, die von der Drehung im $\mathbb{R}^2$ um 90 Grad erzeugt ist, und einer Spiegelung.

Lemma I.8.3. *Es sei G eine endliche abelsche Gruppe und p sei eine Primzahl, die $|G|$ teilt. Dann gibt es ein $g \in G$ mit Ordnung p.*

Beweis. Wir machen Induktion über $|G|$. Ist $|G| = p$, so ist G eine zyklische Gruppe der Ordnung p.

Nehmen wir an, es gibt ein $1_G \neq h \in G$ mit $\mathsf{ord}(h) = m$. Teilt p die Zahl m, so hat $h^{m/p}$ die Ordnung p.

Teilt p dagegen m nicht, so betrachten wir die Untergruppe $\langle h\rangle$. Da G abelsch ist, gilt $\langle h\rangle \lhd G$. Mit Lagrange wissen wir

$$|G| = |\langle h\rangle||G/\langle h\rangle|.$$

Dann teilt aber p die Zahl $|G/\langle h\rangle|$ und $G/\langle h\rangle$ ist eine Gruppe mit weniger Elementen als G. Per Induktionsvoraussetzung gibt es ein $g \in G$ mit

$$\mathsf{ord}(g\langle h\rangle) = p, g\langle h\rangle \in G/\langle h\rangle.$$

Es sei n die Ordnung von g in G. Da

$$(g\langle h\rangle)^n = g^n\langle h\rangle = \langle h\rangle$$

gilt, muss p n teilen. Damit hat aber $g^{n/p}$ die Ordnung p in G. □

Wir haben gebraucht, dass G abelsch ist, damit $\langle h\rangle$ normal ist. Wir sehen gleich, dass diese Voraussetzung nicht nötig ist.

Definition I.8.4. Es sei G eine Gruppe und $g \in G$. Der *Zentralisator von g in G* ist

$$Z_G(g) := \{h \in G, gh = hg\}.$$

Bemerkung I.8.5. Die Gruppe G operiert auf sich selbst durch Konjugation

$$G \times G \to G, \quad (g_1, g_2) \mapsto g_1 g_2 g_1^{-1}.$$

Damit ist der Stabilisator G_g von g für diese Gruppenoperation gerade $Z_G(g)$. Also ist $Z_G(g)$ eine Untergruppe von G.

Wir können jetzt das allgemeine Resultat formulieren:

Satz I.8.6 (Satz von Cauchy)**.** *Es sei p eine Primzahl und G sei eine endliche Gruppe mit $p \mid |G|$. Dann enthält G ein Element der Ordnung p.*

Baron Augustin-Louis Cauchy (1789–1857).

Beweis. Wir machen wieder Induktion über $|G|$ und brauchen für $|G| = p$ nichts zu zeigen. Es sei jetzt also $|G| > p$ und $p \mid |G|$. Gibt es ein $H < G$ mit $H \neq \{1_G\}, G$ und $p \mid |H|$, so gibt es ein $h \in H$ mit $\mathsf{ord}(h) = p$ und wir sind fertig.

Wir nehmen also an, dass für alle $H < G$ mit $H \neq \{1_G\}, G$ gilt, dass p die Ordnung $|H|$ nicht teilt.

Ist G abelsch, so wissen wir mit Lemma I.8.3, dass die Behauptung gilt. Wir können also annehmen, dass G nicht abelsch ist. Dann ist das Zentrum von G, $Z(G)$ nicht ganz G. Ist $g \notin Z(G)$, so gilt

$$\{1_G\} \neq Z_G(g) < G$$

und $Z_G(g) \neq G$. Nach unserer Annahme teilt also p die Ordnung $|Z_G(g)|$ nicht. Da aber p die Ordnung von G teilt, muss gelten

$$p \mid [G : Z_G(g)], \text{ weil } |G| = |Z_G(g)|[G : Z_G(g)].$$

Wie betrachten die Konjugationsoperation von G auf sich und wenden Satz I.6.19 an:

$$|G| = |\mathsf{Fix}_G(G)| + \sum_{y \notin \mathsf{Fix}_G(G)} [G : Z_G(y)].$$

Hierbei ist $\mathsf{Fix}_G(G) = Z(G)$ und y läuft über ein Repräsentantensystem für die Konjugationsklassen.

Da wir wissen, dass gilt $p \mid |G|$ und $p \mid [G : Z_G(y)]$ für alle y wie oben, muss auch gelten $p \mid |Z(G)|$. Damit ist $Z(G)$ entweder die triviale Untergruppe oder ganz G. Da p nicht die 1 teilt, muss $Z(G) = G$ gelten. Dann ist G aber abelsch und wir können Lemma I.8.3 anwenden. □

Satz I.8.7. *Ist G eine Gruppe mit $|G| = p^k$ für eine Primzahl p und ein $k \in \mathbb{N}$, so ist das Zentrum von G nicht trivial.*

Beweis. Wir benutzen wieder die Operation von G auf sich durch Konjugation, so dass $\mathsf{Fix}_G(G) = Z(G)$. Mit Satz I.6.19 wissen wir, dass gilt

$$|G| \equiv |Z(G)| \bmod p.$$

Damit gilt $Z(G) \equiv 0 \bmod p$ und somit gilt $p \mid |Z(G)|$. □

Die Idee der Sylowsätze ist es, die Primfaktorzerlegung der Gruppenordnung zu benutzen, um dann Informationen bezüglich jeder vorkommenden Primzahl zu untersuchen. Ist $|G|$ endlich und teilt eine Primzahl p die Ordnung, dann können wir $|G|$ schreiben als $|G| = p^m q$, so dass $\mathsf{ggT}(p, q) = 1$.

Definition I.8.8. Es sei G eine endliche Gruppe und p eine Primzahl. Ist $|G| = p^m q$ mit $\mathsf{ggT}(p, q) = 1$, so heißt eine Untergruppe $H < G$ eine *p-Sylowuntergruppe von G*, falls $|H| = p^m$ ist.

Im Folgenden ist p immer eine Primzahl. Erinnern Sie sich bitte an den Normalisator einer Untergruppe (siehe Definition I.6.25).

Lemma I.8.9. *Es sei G endlich mit $|G| = p^m q$ und $\mathsf{ggT}(p, q) = 1$. Ist $H < G$ mit $|H| = p^k$ für $1 \leqslant k \leqslant m$ und ist $H < N_G(S)$ für eine p-Sylowuntergruppe $S < G$, dann gilt schon $H < S$.*

Beweis. Nach Definition ist $S \lhd N_G(S)$ und nach Voraussetzung gilt $HS < N_G(S)$. Mit der Kürzungsregel aus Korollar I.4.21 gilt

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

Damit ist aber HS/S entweder trivial oder eine p-Gruppe, weil $|H| = p^k$. Andererseits gilt

$$[HS : S] \mid [G : S],$$

weil $HS < G$, und $[G : S]$ ist teilerfremd zu p. Somit muss HS/S trivial sein, also $S = HS$ und somit $H < S$. □

Satz I.8.10 (Sylowsätze)**.** *Es sei G endlich mit $|G| = p^m q$, p prim, $m \geqslant 1$ und $\mathsf{ggT}(p, q) = 1$. Dann gilt:*

(a) *Für alle k mit $1 \leqslant k \leqslant m$ gibt es ein $H < G$ mit $|H| = p^k$.*
(b) *Ist $H < G$ mit $|H| = p^k$ für $1 \leqslant k \leqslant m$ und ist S eine p-Sylowuntergruppe von G, dann gibt es ein $g \in G$, so dass $H < gSg^{-1}$. Insbesondere sind je zwei p-Sylowuntergruppen zueinander konjugiert.*
(c) *Ist s die Anzahl der p-Sylowuntergruppen von G, so gilt*

$$s \mid q \text{ und } s \equiv 1 \text{ mod } p.$$

Beweis. Für (a) machen wir Induktion über $|G|$. Wir lassen G wieder auf sich selbst durch Konjugation operieren und es sei Y ein Repräsentatensystem der Bahnen mit mehr als einem Element, so dass

$$|G| = |Z(G)| + \sum_{y \in Y} [G : Z_G(y)].$$

Teilt p nicht $|Z(G)|$, so muss es mindestens ein $y \in Y$ geben, so dass $[G : Z_G(y)]$ ebenfalls von p nicht geteilt wird. Für dieses y benutzen wir die Formel

$$|G| = p^m q = [G : Z_G(y)] \cdot |Z_G(y)|,$$

die zeigt, dass $|Z_G(y)| = p^m r$ ist für $r < q$. Nach Induktionsvoraussetzung hat also $Z_G(y)$ eine Untergruppe der Ordnung p^k für jedes $1 \leqslant k \leqslant m$ und dies gibt die gewünschten Untergruppen von G.

Nehmen wir an, dass $p \mid |Z(G)|$, so gibt es nach Satz I.8.6 ein $g \in Z(G)$ mit $\mathsf{ord}(g) = p$. Es ist $\langle g \rangle < G$ und diese Untergruppe ist sogar normal, weil g ein Element des Zentrums ist. Es gilt $|G| = |\langle g \rangle||G/\langle g \rangle|$, so dass $|G/\langle g \rangle| = p^{m-1}q$. Nach Induktionsvoraussetzung hat $G/\langle g \rangle$ Untergruppen H_k mit $|H_k| = p^k$ für $1 \leqslant k \leqslant m-1$. Jedes H_k ist von der Form $U_k/\langle g \rangle$ für ein $U_k < G$ und

$$|U_k| = |H_k||\langle g \rangle| = p^k \cdot p = p^{k+1}.$$

Die Untergruppen $\langle g \rangle, U_1, \ldots, U_{m-1}$ haben somit die Ordnungen $p, p^2, \ldots, p^m$.

Für (b) sei $H < G$ mit $|H| = p^k$ für ein k mit $1 \leqslant k \leqslant m$ und es sei S eine p-Sylowuntergruppe von G. Wir betrachten die Operation von H auf den Linksnebenklassen

$$H \times G/S \to G/S, \quad (h, gS) \mapsto hgS.$$

Wir wissen, dass $|G/S| = q$ ist und mit Satz I.6.19 gilt

$$|\mathsf{Fix}_H(G/S)| \equiv q \bmod p.$$

Daher ist die Fixpunktmenge $\mathsf{Fix}_H(G/S)$ nicht leer. Es sei also gS ein Fixpunkt, also $hgS = gS$ für alle $h \in H$. Dann ist

$$g^{-1}hg \in S \text{ für alle } h \in H,$$

so dass $H \subset gSg^{-1}$ ist. Da gSg^{-1} eine Untergruppe von G ist, gilt auch $H < gSg^{-1}$.

Für (c) sei MS sei die Menge aller p-Sylowuntergruppen und $S \in MS$. Aus (b) wissen wir, dass jedes $S' \in MS$ zu S konjugiert ist. Wir setzen $s := |MS|$ und betrachten die Operation

$$G \times MS \to MS, \quad (g, S') \mapsto g(S')g^{-1}.$$

Mit dieser Operation ist der Normalisator von S in G, $N_G(S)$, gerade der Stabilisator von S, G_S. Mit der Bahnenformel folgt dann

$$|G/G_S| = |MS| = s,$$

weil die Operation transitiv ist. Wir haben

$$q = [G : S] = [G : N_G(S)][N_G(S) : S] = |G/G_S|[N_G(S) : S] = s[N_G(S) : S].$$

Also teilt s die Zahl q.

Zu zeigen bleibt, dass $s \equiv 1 \bmod p$ ist. Wir lassen dazu S auf MS operieren:

$$S \times MS \to MS, \quad (x, S') \mapsto x(S')x^{-1}.$$

Ein $S' \in MS$ ist genau dann ein Fixpunkt dieser Operation, wenn gilt

$$x(S')x^{-1} = S' \text{ für alle } x \in S$$

und dies ist genau dann der Fall, wenn $S \subset N_G(S')$. Aber S ist eine p-Gruppe, so dass wir mit Lemma I.8.9 erhalten, dass $S < S'$ gilt. Aber $|S| = |S'|$, so dass $S = S'$ gelten muss. Also ist S selbst der einzige Fixpunkt dieser Operation und mit Satz I.6.19 folgt

$$s = |MS| \equiv 1 \bmod p.$$

□

Beispiel I.8.11. Wir betrachten $G = \Sigma_4$. Hier ist $|\Sigma_4| = 4! = 24 = 2^3 \cdot 3$, so dass nur die Primzahlen 2 und 3 relevant sind. Die 3-Sylowuntergruppen von Σ_4 haben Mächtigkeit 3 und für ihre Anzahl $s = s_3$ gilt

$$s_3 \mid 8 \text{ und } s_3 \equiv 1 \bmod 3.$$

Die Teiler von 8 sind $1, 2, 4, 8$ und davon erfüllen 1 und 4 die zweite Bedingung. Wir wissen aber, dass jeder 3-Zykel in Σ_4 eine Untergruppe der Ordnung 3 erzeugt, also haben wir $s_3 = 4$ und

$$S_1 = \langle(1,2,3)\rangle, S_2 = \langle(1,2,4)\rangle, S_3 = \langle(1,3,4)\rangle, S_4 = \langle(2,3,4)\rangle.$$

Im Folgenden geben wir eine beispielhafte Anwendung der Sylowsätze.

Satz I.8.12. *Sind p_1 und p_2 Primzahlen mit $p_1 < p_2$ und $p_1 \nmid (p_2 - 1)$. Dann ist jede Gruppe G der Ordnung $|G| = p_1 p_2$ zyklisch, also $G \cong \mathbb{Z}/p_1p_2\mathbb{Z}$.*

Beweis. Es sei $S_1 < G$ eine p_1-Sylowuntergruppe von G und S_2 sei eine p_2-Sylowuntergruppe von G. Dann ist der Schnitt $S_1 \cap S_2$ nur $\{1_G\}$. Ist s_i jeweils die Anzahl der p_i-Sylowuntergruppen, so wissen wir nach den Sylowsätzen, dass

$$s_1 \mid p_2, s_1 \equiv 1 \bmod p_1, s_2 \mid p_1 \text{ und } s_2 \equiv 1 \bmod p_2.$$

Da $p_1 < p_2$, muss damit $s_2 = 1$ sein und S_2 ist eine normale Untergruppe von G. Dagegen könnte s_1 a priori 1 oder p_2 sein. Wäre es p_2, so wäre $p_2 \equiv 1 \bmod p_1$, so dass $p_1 \mid (p_2 - 1)$, was im Widerspruch zur Annahme steht. Also ist $s_1 = 1$ und S_1 ist auch normal.

Es ist S_1S_2 eine Untergruppe von G, aber $S_1 \subsetneq S_1S_2$ und $S_2 \subsetneq S_1S_2$, so dass gelten muss $G = S_1S_2$. Damit ist aber $G = S_1 \times S_2$. Da $|S_1| = p_1$ und $|S_2| = p_2$ gilt, sind beide Gruppen zyklisch der Ordnung p_1 beziehungsweise p_2. Daher gilt

$$S_1 \cong \mathbb{Z}/p_1\mathbb{Z}, \quad S_2 \cong \mathbb{Z}/p_2\mathbb{Z} \text{ und } G = S_1 \times S_2 \cong \mathbb{Z}/p_1p_2\mathbb{Z},$$

weil p_1 und p_2 teilerfremd sind. □

Beispiel I.8.13. Beispiele für solche Zahlenpaare sind $p_1 = 3$ und $p_2 = 5$ oder $p_2 = 11$, weil $3 \nmid 4$ und $3 \nmid 10$.

Vorlesung 11

I.9. Normal- und Kompositionsreihen

Ziel dieses Abschnittes ist es, Gruppen so zu unterteilen, bis man sie nicht mehr weiter zerlegen kann.

Beispiele I.9.1.

- Ist G eine einfache Gruppe wie zum Beispiel A_n für $n \geqslant 5$, dann gibt es keine normale Untergruppe zwischen $\{1_G\}$ und G.
- Für die Σ_4 gibt es dagegen

$$\{\mathrm{id}_{\mathbf{4}}\} \lhd \{\mathrm{id}_{\mathbf{4}}, (1,2)(3,4)\} \lhd K_4 \lhd A_4 \lhd \Sigma_4.$$

- Für die Σ_n mit $n \geqslant 5$ passt nur jeweils die A_n zwischen die triviale Untergruppe und Σ_n.

Definition I.9.2.

(a) Eine *Normalreihe* einer Gruppe G ist eine endliche Folge von Untergruppen

$$\mathcal{G} = (\{1_G\} = G_0 \lhd G_1 \lhd \ldots \lhd G_n = G). \tag{I.9.1}$$

(b) In einer Normalreihe wie in (I.9.1) heißen die G_i *Terme* und die Restklassengruppen G_{i+1}/G_i *Faktoren*.

Jede Gruppe G besitzt natürlich eine Normalreihe $\{1_G\} \lhd G$. Die bringt zwar nichts, existiert aber...

Definition I.9.3. Es seien $\mathcal{G}$ und $\mathcal{H}$ zwei Normalreihen einer Gruppe G.

(a) Die Normalreihe $\mathcal{H}$ heißt eine *Verfeinerung von* $\mathcal{G}$, falls jeder Term von $\mathcal{G}$ auch ein Term von $\mathcal{H}$ ist.
(b) Wir nennen $\mathcal{H}$ *äquivalent zu* $\mathcal{G}$, falls es eine Bijektion zwischen den Faktoren von $\mathcal{H}$ und denen von $\mathcal{G}$ gibt, so dass die zugeordneten Faktoren jeweils isomorph sind.

Beispiel I.9.4. Es sei

$$\mathcal{G} = (\{0\} \lhd 8\mathbb{Z}/16\mathbb{Z} \lhd 2\mathbb{Z}/16\mathbb{Z} \lhd \mathbb{Z}/16\mathbb{Z})$$

und

$$\mathcal{H} = (\{0\} \lhd 4\mathbb{Z}/16\mathbb{Z} \lhd 2\mathbb{Z}/16\mathbb{Z} \lhd \mathbb{Z}/16\mathbb{Z})$$

Dann hat $\mathcal{G}$ Faktoren, die isomorph sind zu

$$\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/4\mathbb{Z} \text{ und } \mathbb{Z}/2\mathbb{Z},$$

und $\mathcal{H}$ hat Faktoren, die isomorph sind zu

$$\mathbb{Z}/4\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \text{ und } \mathbb{Z}/2\mathbb{Z}.$$

Damit ist $\mathcal{H}$ äquivalent zu $\mathcal{G}$.

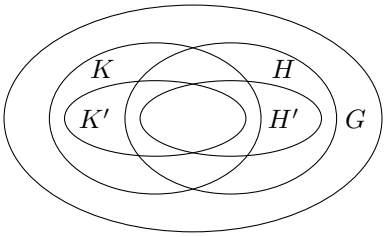
Das Folgende ist ein technisch wichtiges Hilfsresultat.

Lemma I.9.5 (Schmetterlingslemma)**.** *Sind H und K jeweils Untergruppen einer Gruppe G und sind $H' \lhd H$ und $K' \lhd K$ jeweils Normalteiler, dann gilt:*

(a)
$$H'(H \cap K') \lhd H'(H \cap K) \text{ und } K'(K \cap H') \lhd K'(K \cap H).$$

(b)
$$H'(H \cap K)/H'(H \cap K') \cong K'(K \cap H)/K'(K \cap H') \cong H \cap K/(H \cap K')(H' \cap K).$$

Beachten Sie, dass die letzte Isomorphie eine symmetrische Formel gibt, die sich in dem folgenden Bild widerspiegelt, welches Sie auch gerne zu einem Schmetterling morphen dürfen.



Beweis. Wir wissen, dass $H \cap K < H$ und $H' \lhd H$. Damit ist $H'(H \cap K)$ eine Untergruppe von H. Weil $H' \lhd H$ ist, gilt auch $H' \lhd H'(H \cap K)$. Aus Korollar I.4.21 folgt dann

$$H'(H \cap K)/H' \cong (H \cap K)/H' \cap H \cap K = (H \cap K)/H' \cap K.$$

Die Untergruppen $H \cap K'$ und $H' \cap K$ sind normal in $H \cap K$. Wiederum mit Korollar I.4.21 erhalten wir

$$(H \cap K)/(H \cap K')(H' \cap K) \cong (H \cap K)/(H' \cap K)/(H \cap K')(H' \cap K)/(H' \cap K),$$

so dass wir $(H \cap K)/(H \cap K')(H' \cap K)$ bis auf Isomorphie als eine Restklassengruppe von $H \cap K/H' \cap K$ auffassen können.

Wir erhalten also einen Epimorphismus

$$\varrho\colon H'(H \cap K)/H' \cong H \cap K/H' \cap K \to H \cap K/(H \cap K')(H' \cap K)$$

und der Kern von ϱ ist $H'(H \cap K')/H'$, so dass wir mit dem Isomorphiesatz den Isomorphismus

$$(H'(H \cap K)/H')/(H'(H \cap K')/H') \cong H \cap K/(H \cap K')(H' \cap K)$$

erhalten. Da

$$(H'(H \cap K)/H')/(H'(H \cap K')/H') \cong H'(H \cap K)/H'(H \cap K')$$

gilt, folgt eine Hälfte des Satzes. Wenn wir die Rollen von $H' \lhd H$ und $K' \lhd K$ vertauschen, erhalten wir die andere. □

Otto Schreier (1901–1929).

Satz I.9.6 (Satz von Schreier)**.** *Sind $\mathcal{G}$ und $\mathcal{H}$ zwei Normalreihen einer Gruppe G, so besitzen $\mathcal{G}$ und $\mathcal{H}$ äquivalente Verfeinerungen.*

Beweis. Es sei

$$\mathcal{G} = (\{1_G\} = G_0 \lhd G_1 \lhd \ldots \lhd G_n = G)$$

und

$$\mathcal{H} = (\{1_G\} = H_0 \lhd H_1 \lhd \ldots \lhd H_m = G).$$

Wir definieren

$$G_{ij} := G_i(G_{i+1} \cap H_j) \text{ und } H_{ij} := H_j(G_i \cap H_{j+1}).$$

Mit

$$H' = G_i, H = G_{i+1}, K' = H_j \text{ und } K = H_{j+1}$$

folgt mit dem Schmetterlingslemma, dass

$$G_{ij} \lhd G_{i,j+1} \text{ und } H_{ij} \lhd H_{i+1,j}.$$

Außerdem gilt für die Restklassengruppen

$$G_{i,j+1}/G_{ij} \cong H_{i+1,j}/H_{ij}.$$

Die Untergruppen H_{ij} und G_{ij} sind aneinandergekettet, weil nach Konstruktion gilt

$$\begin{aligned} G_{im} &= G_i(G_{i+1} \cap H_m) = G_i G_{i+1} = G_{i+1}, \\ G_{i+1,0} &= G_{i+1}(G_{i+2} \cap \{1_G\}) = G_{i+1} \end{aligned}$$

und ebenso

$$\begin{aligned} H_{nj} &= H_j(G_n \cap H_{j+1}) = H_j H_{j+1} = H_{j+1}, \\ H_{0,j+1} &= H_{j+1}(\{1_G\} \cap H_{j+2}) = H_{j+1}. \end{aligned}$$

Wir können diese Matrix von Untergruppen also zu zwei Normalreihen zusammenfädeln und erhalten:

$$\begin{aligned} \{1_G\} = G_{0,0} \lhd G_{0,1} \lhd \ldots \lhd G_{0,m} = G_{1,0} \lhd \ldots \lhd G_{nm} = G, \\ \{1_G\} = H_{0,0} \lhd H_{1,0} \lhd \ldots \lhd H_{n,0} = H_{0,1} \lhd \ldots \lhd H_{nm} = G. \end{aligned}$$

Dies sind äquivalente Normalreihen von G, die $\mathcal{G}$ und $\mathcal{H}$ verfeinern. □

Wir wollen Normalreihen erhalten, die so fein wie möglich sind:

Definition I.9.7. Eine Normalreihe wie in (I.9.1) heißt *Kompositionsreihe*, falls $G_i \neq G_{i+1}$ für alle $0 \leqslant i \leqslant n-1$ und falls sie keine echte Verfeinerung besitzt.

Beispiel I.9.8. Die Normalreihe, die wir für Σ_4 aufgestellt hatten

$$\{\mathrm{id}_{\mathbf{4}}\} \lhd \{\mathrm{id}_{\mathbf{4}}\}, (1,2)(3,4)\} \lhd K_4 \lhd A_4 \lhd \Sigma_4$$

ist eine Kompositionsreihe, weil alle Faktoren Primzahlordnung haben, so dass keine weitere Untergruppe dazwischenpasst.

Die Atome der Gruppentheorie sind die einfachen Gruppen:

Satz I.9.9. *Eine Normalreihe ist genau dann eine Kompositionsreihe, wenn alle Faktoren einfach sind.*

BEWEIS. Ist in

$$\mathcal{G} = (\{1_G\} = G_0 \lhd G_1 \lhd \ldots \lhd G_i \lhd G_{i+1} \lhd \ldots \lhd G_n = G)$$

ein Faktor G_{i+1}/G_i nicht einfach, so gibt es also einen nicht-trivialen Normalteiler $\{1_{G_{i+1}/G_i}\} \neq N \neq G_{i+1}/G_i$, $N \lhd G_{i+1}/G_i$. Dann ist N von der Form $N \cong N'/G_i$, so dass $N' \lhd G_{i+1}$ und $G_i \neq N' \neq G_{i+1}$. Somit ist

$$\mathcal{G}' = (\{1_G\} = G_0 \lhd G_1 \lhd \ldots \lhd G_i \lhd N' \lhd G_{i+1} \lhd \ldots \lhd G_n = G)$$

eine echte Verfeinerung von $\mathcal{G}$.

Umgekehrt, hat eine Normalreihe $\mathcal{G}$ wie oben eine echte Verfeinerung, dann gibt es ein $0 \leqslant i \leqslant n$ und ein N' mit $G_i \lhd N' \lhd G_{i+1}$ mit $G_i \neq N' \neq G_{i+1}$ und damit ist $N := N'/G_{i+1}$ ein echter Normalteiler des Faktors G_i/G_{i+1} und $\mathcal{G}$ war keine Kompositionsreihe. □

Als Konsequenz erhalten wir die folgende Eindeutigkeitsaussage für Kompositionsreihen.

Korollar I.9.10 (Satz von Jordan-Hölder)**.** *Hat G eine Kompositionsreihe $\mathcal{G}$, so ist jede Kompositionsreihe $\mathcal{H}$ von G äquivalent zu $\mathcal{G}$.*

Otto Ludwig Hölder (1859–1937), Marie Ennemond Camille Jordan (1838–1922).

Beispiele I.9.11.

- Für $n \geqslant 5$ ist
$$\{\mathrm{id}_{\mathbf{n}}\} \lhd A_n \lhd \Sigma_n$$
eine Kompositionsreihe von Σ_n.
- Für $n = 4$ hatten wir die Kompositionsreihe für Σ_4 schon gesehen. Für $n = 3$ ist A_3 auch einfach mit $A_3 \cong \mathbb{Z}/3\mathbb{Z}$. Also ist
$$\{\mathrm{id}_{\mathbf{3}}\} \lhd A_3 \cong \mathbb{Z}/3\mathbb{Z} \lhd \Sigma_3$$
eine Kompositionsreihe.
- Ist $G = \mathbb{Z}/n\mathbb{Z}$ mit $1 \neq n \in \mathbb{N}$, so hat n eine Primfaktorzerlegung $n = p_1 \cdot \ldots \cdot p_r$. Hierbei sind die p_i prim und können durchaus mehrfach auftreten. Dann ist
$$\{\bar{0}\} = p_1 \cdot \ldots \cdot p_r\mathbb{Z}/n\mathbb{Z} \lhd p_2 \cdot \ldots \cdot p_r\mathbb{Z}/n\mathbb{Z} \lhd \ldots \lhd p_r\mathbb{Z}/n\mathbb{Z} \lhd \mathbb{Z}/n\mathbb{Z}$$
eine Kompositionsreihe von $\mathbb{Z}/n\mathbb{Z}$, weil die Faktoren jeweils von der Form $\mathbb{Z}/p_i\mathbb{Z}$ sind und damit einfach. Insbesondere hat für jede Primzahl p die Gruppe $\mathbb{Z}/p^r\mathbb{Z}$ die Kompositionsreihe
$$\{\bar{0}\} = p^r\mathbb{Z}/p^r\mathbb{Z} \lhd p^{r-1}\mathbb{Z}/p^r\mathbb{Z} \lhd \ldots \lhd p\mathbb{Z}/p^r\mathbb{Z} \lhd \mathbb{Z}/p^r\mathbb{Z}.$$

Vorlesung 12

I.10. Auflösbare Gruppen

Definition I.10.1. Eine Gruppe G heißt *auflösbar*, falls sie eine Normalreihe mit abelschen Faktoren besitzt.

Beispiele I.10.2.

- Abelsche Gruppen sind natürlich auflösbar.
- Die Gruppen Σ_3 und Σ_4 sind auflösbar, während die Gruppen Σ_n und A_n für $n \geqslant 5$ nicht auflösbar sind.

Bemerkung I.10.3. Die Auflösbarkeit von Gruppen hängt in der Galoistheorie mit der Frage der Auflösbarkeit von Gleichungen zusammen. Sie können quadratische Gleichungen immer durch die pq-Formeln auflösen und die Lösungen sind explizite Ausdrücke, die durch die Koeffizienten der Gleichung und Quadratwurzeln gegeben sind. Ähnliche Lösungsformeln finden Sie für Gleichungen bis zum Grad 4. Es gibt Gleichungen vom Grad 5, die in dieser Form nicht auflösbar sind.

Satz I.10.4. *Die Klasse der auflösbaren Gruppen ist abgeschlossen unter der Bildung von Untergruppen und Bildern unter Homomorphismen.*

Beweis. Es sei

$$\mathcal{G} = (\{1_G\} = G_0 \lhd G_1 \lhd \ldots \lhd G_n = G)$$

eine Normalreihe von G mit abelschen Faktoren G_{i+1}/G_i und $H < G$ sei eine Untergruppe. Wir betrachten

$$\mathcal{G}_H = (\{1_G\} = G_0 \cap H < G_1 \cap H < \ldots < G_n \cap H = H).$$

Ist $g \in G_{i+1} \cap H$ und $h \in G_i \cap H$, dann ist ghg^{-1} wieder in $G_i \cap H$, weil G_i normal ist in G_{i+1} und weil H eine Untergruppe von G ist.

Die Kürzungsregel I.4.21 ergibt

$$G_{i+1} \cap H/G_i \cap H \cong (H \cap G_{i+1})G_i/G_i.$$

Dies ist eine Untergruppe der abelschen Gruppe G_{i+1}/G_i und damit abelsch. Also ist H auflösbar.

Ist $f\colon G \to G'$ ein Homomorphismus und ist G auflösbar, so betrachten wir $\mathrm{Bild}(f) < G'$. Wir betrachten

$$\{1_{G'}\} = f(G_0) < f(G_1) < \ldots < f(G_n) = \mathrm{Bild}(f),$$

wobei

$$\mathcal{G} = (\{1_G\} = G_0 \lhd G_1 \lhd \ldots \lhd G_n = G)$$

eine Normalreihe von G mit abelschen Faktoren ist.

Die Untergruppe $f(G_i)$ von $f(G_{i+1})$ ist jeweils normal, weil $G_i \lhd G_{i+1}$. Die Einschränkung von f auf G_{i+1} ist ein Epimorphismus

$$f|_{G_{i+1}}\colon G_{i+1} \to f(G_{i+1})$$

und daher ist die Verkettung mit der kanonischen Projektion $\pi\colon f(G_{i+1}) \to f(G_{i+1})/f(G_i)$ ebenfalls ein Epimorphismus

$$G_{i+1} \to f(G_{i+1})/f(G_i), \quad g \mapsto f(g)f(G_i).$$

Ist $g \in G_i$, so ist $f(g)f(G_i) = f(G_i)$, also ist $G_i \subset \ker(\pi \circ f|_{G_{i+1}}$. Wir erhalten damit einen Epimorphismus

$$G_{i+1}/G_i \to f(G_{i+1})/f(G_i).$$

Da G_{i+1}/G_i abelsch ist, ist $f(G_{i+1})/f(G_i)$ ebenfalls abelsch. □

Das folgende Konzept hatten Sie schon in einer Übungsaufgabe kennengelernt.

Definition I.10.5. Sind G_1, G_2, G_3 Gruppen und $f_1\colon G_1 \to G_2$, $f_2\colon G_2 \to G_3$ Homomorphismen, so heißt die Sequenz

$$G_1 \xrightarrow{f_1} G_2 \xrightarrow{f_2} G_3$$

exakt, falls gilt: $\mathrm{Bild}(f_1) = \ker(f_2)$.

Bemerkung I.10.6. Ist $f\colon G \to G'$ ein Monomorphismus, so ist die Sequenz

$$\{1_G\} \longrightarrow G \xrightarrow{f} G'$$

exakt. Ist dagegen f ein Epimorphismus, so ist die Sequenz

$$G \xrightarrow{f} G' \longrightarrow \{1_{G'}\}$$

exakt. Da es nur jeweils genau einen Homomorphismus aus der trivialen Gruppe beziehungsweise in die triviale Gruppe gibt, muss man an den Stellen keine Abbildung benennen.

Definition I.10.7. Die Folge

$$1 \longrightarrow G_1 \xrightarrow{f_1} G_2 \xrightarrow{f_2} G_3 \longrightarrow 1$$

heißt *kurze exakte Sequenz*, falls sie an jeder Stelle exakt ist, also

- f_1 ist ein Monomorphismus
- f_2 ist ein Epimorphismus und
- $\mathrm{Bild}(f_1) = \ker(f_2)$.

Hier steht 1 für eine triviale Gruppe. Die Mengenklammern läßt man weg.

Beispiel I.10.8. Ist G eine Gruppe und $N \lhd G$, so ist

$$1 \longrightarrow N \xrightarrow{i} G \xrightarrow{\pi} G/N \longrightarrow 1$$

eine kurze exakte Sequenz. Hierbei ist i die Inklusion von N nach G und π ist die kanonische Projektion mit $N = \ker(\pi)$.

Bemerkung I.10.9. Ist

$$1 \longrightarrow G_1 \xrightarrow{f_1} G_2 \xrightarrow{f_2} G_3 \longrightarrow 1$$

exakt, so ist $f_1(G_1) \lhd G_2$, weil $f_1(G_1) = \text{Bild}(f_1) = \ker(f_2)$. Die Gruppe G_3 ist dann isomorph zu $G_2/\text{Bild}(f_1)$.
Sind alle beteiligten Gruppen in einer exakten Sequenz abelsch, so schreibt man auch 0 statt 1 für die triviale Gruppe.

Definition I.10.10. Sind N und H Gruppen, so heißt eine kurze exakte Sequenz

$$1 \longrightarrow N \xrightarrow{f_1} G \xrightarrow{f_2} H \longrightarrow 1$$

eine *Gruppenerweiterung von H durch N*.

Beispiele I.10.11.

(a) Ist $G = G_1 \times G_2$, so ist sowohl

$$1 \longrightarrow G_1 \xrightarrow{i_1} G \xrightarrow{p_2} G_2 \longrightarrow 1$$

als auch

$$1 \longrightarrow G_2 \xrightarrow{i_2} G \xrightarrow{p_1} G_1 \longrightarrow 1$$

eine Gruppenerweiterung. Hierbei bezeichnet $i_j \colon G_j \to G$ die Inklusion und $p_j \colon G \to G_j$ die Projektion.

(b) Ist $G = N \rtimes H$ ein semidirektes Produkt, so ist

$$1 \longrightarrow N \xrightarrow{i} G \xrightarrow{p} H \longrightarrow 1$$

eine Gruppenerweiterung mit $i(n) = (n, 1_H)$ und $p(n, h) = h$.

(c)

$$0 \to \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \to 0$$

ist eine Gruppenerweiterung. Was sind die einzig möglichen Abbildungen?

Satz I.10.12. *Sind N und H auflösbare Gruppen und ist*

$$1 \longrightarrow N \xrightarrow{i} G \xrightarrow{\pi} H \longrightarrow 1$$

eine Gruppenerweiterung, so ist auch G auflösbar.

Beweis. Es sei

$$\{1\} = H_0 \lhd H_1 \lhd \ldots \lhd H_n = H$$

eine Normalreihe mit abelschen Faktoren H_{i+1}/H_i und

$$\{1\} = N_0 \lhd N_1 \lhd \ldots \lhd N_m = N$$

sei eine Normalreihe mit abelschen Faktoren N_{i+1}/N_i.

Wir definieren

$$G_j := \begin{cases} i(N_j), & 0 \leqslant j \leqslant m, \\ \pi^{-1}(H_{j-m}), & m+1 \leqslant j \leqslant m+n. \end{cases}$$

Es ist klar, dass $i(N_0) \lhd \ldots \lhd i(N_m)$ und dass $\pi^{-1}(H_1) \lhd \ldots \lhd \pi^{-1}(H_n)$.

Da $i(N_m) = i(N) \lhd G$ ist auch $i(N)$ normal in $G \cap \pi^{-1}(H_1) = \pi^{-1}(H_1)$. Damit ist

$$i(N_0) \lhd \ldots \lhd i(N_m) \lhd \pi^{-1}(H_1) \lhd \ldots \lhd \pi^{-1}(H_m) = G$$

eine Normalreihe von G. Die Faktoren sind

$$G_{i+1}/G_i \cong \begin{cases} N_{i+1}/N_i, & i < m \\ H_{i+1-m}/H_{i-m}, & i \geqslant m. \end{cases}$$

□

Korollar I.10.13.

(a) *Semidirekte Produkte auflösbarer Gruppen sind auflösbar.*

(b) *Für jede Primzahl p ist jede endliche p-Gruppe auflösbar.*

Beweis. Behauptung (a) ist klar. Für (b) machen wir Induktion über $|G|$. Für $|G| = p$ ist G abelsch. Ist $|G| > p$, so hat G ein nicht-triviales Zentrum, $Z(G)$, so dass $|G/Z(G)| < |G|$. Nach Induktion ist also $G/Z(G)$ auflösbar. Das Zentrum ist als abelsche Gruppe auflösbar und damit ist auch G als Gruppenerweiterung

$$1 \to Z(G) \to G \to G/Z(G) \to 1$$

auflösbar. □

Satz I.10.14. *Ist G eine endliche auflösbare Gruppe, so hat G eine Normalreihe*

$$\{1\} = G_0 \lhd G_1 \lhd \ldots \lhd G_n = G$$

mit zyklischen Gruppen G_{i+1}/G_i von Primzahlordnung.

Beweis. Nach Satz I.9.9 hat eine Kompositionsreihe von G einfache Faktoren. Eine solche Kompositionsreihe von G existiert, weil G endlich ist:

$$\mathcal{G} = (\{1\} = G_0 \lhd G_1 \lhd \ldots \lhd G_n = G)$$

Da G auflösbar ist, sind auch alle G_i auflösbar und damit auch alle Faktoren G_{i+1}/G_i als Bilder der kanonischen Projektionen.

Wir zeigen also das Folgende: Ist $\{1\} \neq H$ eine endliche, einfache, auflösbare Gruppe, so ist gibt es eine Primzahl p, so dass H zyklisch ist mit Ordnung p.

Nach Annahme ist $H \cong H/\{1\}$ abelsch. Sei $1 \neq h \in H$. Dann gilt, dass $\langle h\rangle < H$. Wäre $\langle h\rangle \neq H$, so wäre $\langle h\rangle$ eine echte normale Untergruppe von H im Widerspruch dazu, dass H einfach ist. Daher ist $H = \langle h\rangle$. Hätte die Ordnung von h, $\mathsf{ord}(h) = n$, einen echten Teiler d, so wäre $\langle h^{n/d}\rangle$ ein echter Normalteiler von H. Also ist n eine Primzahl. □

Wir entwickeln nun eine alternatives Kriterium für die Auflösbarkeit einer Gruppe.

Definition I.10.15. Es sei G eine beliebige Gruppe und $g, h \in G$.

(a) Das Element

$$[g, h] := ghg^{-1}h^{-1} \in G$$

heißt der *Kommutator von g und h.*

(b) Die *Kommutatoruntergruppe von G*, $[G, G]$, ist die kleinste Untergruppe von G, die alle Kommutatoren enthält.

Bemerkung I.10.16. Ist G eine Gruppe und $S \subset G$ eine beliebige Teilmenge, so sei $\langle S\rangle$ die von S erzeugte Untergruppe von G, also die kleinste Untergruppe von G, die alle Elemente von S enthält. Mit dieser Notation ist

$$[G, G] = \langle\{[g, h], g, h \in G\}\rangle.$$

Man kann $\langle S\rangle$ ausdrücken als

$$\langle S\rangle = \bigcap_{\substack{H<G \\ S\subset H}} H.$$

Oft ist es nicht einfach, solche Untergruppen explizit zu beschreiben.

Vorlesung 13

Beispiel I.10.17. Für alle $n \geqslant 5$ ist

$$[\Sigma_n, \Sigma_n] = A_n = [A_n, A_n].$$

Betrachten Sie dazu eine fünfelementige Teilmenge

$$\{a, b, c, d, e\} \subset \mathbf{n}$$

und die Elemente $g = (a, b, d)$ und $h = (a, c, e)$. Dann ist der Kommutator

$$ghg^{-1}h^{-1} = (a, b, d)(a, c, e)(a, d, b)(a, e, c) = (a, b, c).$$

Also ist jeder 3-Zykel in $[\Sigma_n, \Sigma_n]$ und in $[A_n, A_n]$. Damit folgt $A_n = [A_n, A_n]$ sofort, weil A_n von 3-Zykeln erzeugt wird. Da außerdem

$$A_n < [\Sigma_n, \Sigma_n] < \Sigma_n$$

gilt und $\Sigma_n/A_n \cong \{\pm 1\}$ gilt, muss $A_n = [\Sigma_n, \Sigma_n]$ gelten, weil $\Sigma_n \neq A_n[\Sigma_n, \Sigma_n]$, weil alle Elemente in $[\Sigma_n, \Sigma_n]$ Signum $= 1$ haben.

Lemma I.10.18. *Ist G eine beliebige Gruppe und $\varphi \in \mathsf{Aut}(G)$, so gilt*

$$\varphi[G, G] = [G, G].$$

Beweis. Für alle $g, h \in G$ gilt

$$\varphi[g, h] = \varphi(ghg^{-1}h^{-1}) = \varphi(g)\varphi(h)\varphi(g)^{-1}\varphi(h)^{-1} = [\varphi(g), \varphi(h)]$$

und somit ist $\varphi[g, h] \in [G, G]$ und $\varphi[G, G] \subset [G, G]$. Da φ bijektiv ist, muss die Gleichheit gelten. □

Speziell für innere Automorphismen $\varphi = c_{\tilde{g}}$ erhalten wir:

Korollar I.10.19. *Für jede Gruppe G gilt $[G, G] \lhd G$.*

Definition I.10.20. Wir definieren iterativ:

$$G^0 := G, G' = G^1 := [G, G] \text{ und } G^n = (G^{n-1})' = [G^{n-1}, G^{n-1}].$$

Jede Gruppe besitzt die sogenannte *abgeleitete Reihe*

$$G \rhd [G, G] = G' \rhd G^2 \rhd \dots$$

Als Übungsaufgabe beweisen Sie die folgende Hilfsaussage.

Lemma I.10.21. *Es sei G eine beliebige Gruppe und $N \lhd G$. Die Restklassengruppe G/N ist genau dann abelsch, wenn $G' < N$.*

Hier kommt das versprochene alternative Kriterium für Auflösbarkeit mittels der abgeleiteten Reihe.

Satz I.10.22. *Eine Gruppe G ist genau dann auflösbar, wenn es ein $m \in \mathbb{N}$ gibt mit $G^m = \{1\}$.*

Beweis. Ist $G^m = \{1\}$ für ein m, dann ist

$$G^m = \{1\} \lhd G^{m-1} \lhd \dots \lhd G^1 \lhd G$$

eine Normalreihe von G mit abelschen Faktoren und damit ist G auslösbar.

Es sei umgekehrt G auflösbar und

$$\{1\} = G_0 \lhd G_1 \lhd \dots \lhd G_n = G$$

sei eine Normalreihe mit abelschen Faktoren G_{i+1}/G_i. Nach Lemma I.10.21 gilt dann $[G_{i+1}, G_{i+1}] \lhd G_i$ für alle i.

Wir behaupten induktiv, dass $G^i < G_{n-i}$ für alle $i \leqslant n$. Für $i = 0$ ist $G^0 = G = G_n$. Für den Schluss von i auf $i + 1$ benutzen wir $G^{i+1} = [G^i, G^i]$ und nach Induktionsannahme ist dies eine Untergruppe von $[G_{n-i}, G_{n-i}]$. Mit Lemma I.10.21 erhalten wir wiederum, dass gilt

$$[G_{n-i}, G_{n-i}] < G_{n-i-1} = G_{n-(i+1)},$$

was zu zeigen war. Insbesondere gilt dann $G^n < G_0 = \{1\}$. □

Zum Abschluss gebe ich Ihnen noch zwei wichtige Resultate an, die ich hier aber nicht beweise.

- Theorem von Burnside [1904] (William Burnside (1852–1927))
  Alle Gruppen der Ordnung $p^a q^b$ mit p, q prim und $a, b \in \mathbb{N}$ sind auflösbar.
- Theorem von Feit-Thompson [1963]
  Alle endlichen Gruppen G mit $|G|$ ungerade sind auflösbar.

Walter Feit (1930–2004), John Griggs Thompson (*1932).

Der Beweis des Satzes von Burnside benutzt Darstellungstheorie, der Beweis des Satzes von Feit-Thompson ist über 250 Seiten lang und benutzt Techniken, wie sie zur Klassifikation der endlichen einfachen Gruppen gebraucht werden. Beides geht weit über eine Bachelor-Algebra Vorlesung hinaus.

I.11. Abelsche Gruppen

Das Ziel dieses Abschnitts ist die Klassifikation der endlich-erzeugten abelschen Gruppen. Wir möchten jede solche Gruppe zerlegen als Produkt von Bausteinen der Form $\mathbb{Z}$ oder $\mathbb{Z}/p^\ell\mathbb{Z}$ mit p prim.

Beispiel I.11.1. Die Kleinsche Vierergruppe K_4 ist isomorph zu $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ und sie ist nicht isomorph zu $\mathbb{Z}/4\mathbb{Z}$.

Definition I.11.2. Eine Gruppe G heißt *endlich erzeugt*, falls es $s_1, \ldots, s_n \in G$ gibt, so dass $\langle s_1, \ldots, s_n \rangle = G$.

Beispiele I.11.3.
- Jede zyklische Gruppe $G = \langle g \rangle$ ist endlich erzeugt.
- Ist $G = G_1 \times G_2$ und sind G_1, G_2 endlich erzeugt, dann ist auch G endlich erzeugt. Warum?
- Die Gruppe $SL_2(\mathbb{Z})$ ist endlich erzeugt und zwar ist

$$SL_2(\mathbb{Z}) = \langle S, T \rangle \text{ mit } S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Wir schreiben abelsche Gruppen meistens additiv.

Definition I.11.4. Ist $(G_i)_{i \in I}$ eine beliebige Familie abelscher Gruppen G_i, so ist die *direkte Summe der* G_i die Menge aller $(g_i)_{i \in I}$ mit $g_i = 0$ für fast alle $i \in I$ und wir notieren diese als

$$\bigoplus_{i \in I} G_i.$$

Bemerkung I.11.5.
- Es gilt immer
$$\bigoplus_{i \in I} G_i < \prod_{i \in I} G_i$$
und so ist auch die Gruppenstruktur auf $\bigoplus_{i \in I} G_i$ definiert: komponentenweise.
- Ist I eine endliche Menge, so ist
$$\bigoplus_{i \in I} G_i = \prod_{i \in I} G_i.$$
Ist I unendlich und sind unendlich viele G_i nicht-trivial, so ist die direkte Summe eine echte Untergruppe des Produkts.
- Wir schreiben Elemente $(g_i)_{i \in I} \in \bigoplus_{i \in I} G_i$ auch manchmal als Summe $\sum_{i \in I} g_i$. Ist $\alpha_i \in \mathbb{Z}$, so ist $\alpha_i g_i \in G_i$, so dass auch $\sum_{i \in I} \alpha_i g_i$ vorkommen wird.

Definition I.11.6. Eine abelsche Gruppe G heißt *frei abelsch*, falls G isomorph ist zu einer direkten Summe unendlicher zyklischer Gruppen.

Beispiele I.11.7.
- $\prod_{i=1}^n \mathbb{Z}$ ist frei abelsch für jedes endliche $n \in \mathbb{N}$, weil $\bigoplus_{i=1}^n \mathbb{Z} = \prod_{i=1}^n \mathbb{Z}$. Dagegen ist $\prod_{n \in \mathbb{N}} \mathbb{Z}$ nicht frei abelsch. Dieses Resultat heißt auch Baers Theorem.
- Ist $\varphi \in (0, 1)$ irrational, so ist $\langle e^{2\pi i \varphi} \rangle$ unendlich zyklisch, also frei abelsch.

Definition I.11.8. Ist G frei abelsch und ist $X \subset G$ eine Teilmenge, so dass jedes $x \in X$ unendliche Ordnung hat und ist

$$G \cong \bigoplus_{x \in X} \langle x \rangle.$$

Dann heißt X eine *Basis von* G.

Diametral entgegengesetzt zu freien abelschen Gruppen sind Torsionsgruppen.

Definition I.11.9. Es sei G eine abelsche Gruppe.

(a) Dann heißt G eine *Torsionsgruppe*, falls jedes $g \in G$ endliche Ordnung hat.
(b) Die Gruppe G heißt *torsionsfrei*, falls alle $0 \neq g$ unendliche Ordnung haben.
(c) Wir setzen
$$G_{\mathsf{tor}} := \{g \in G, \mathsf{ord}(g) < \infty\}$$
und nennen G_{tor} die *Torsionsuntergruppe von* G.
(d) Alle Elemente $g \in G$ mit $\mathsf{ord}(g) < \infty$ heißen *Torsionselemente* in G.

Beispiele I.11.10.

- In $(\mathbb{C} \setminus \{0\}, \cdot) =: G$ besteht G_{tor} aus den Einheitswurzeln
$$G_{\mathsf{tor}} = \{z \in \mathbb{C}, \exists n \in \mathbb{N}, z^n = 1\}.$$
- In $(\mathbb{R} \setminus \{0\}, \cdot)$ gibt es nur die Torsionselemente ± 1.
- Es sei $\mathrm{diag}_n < GL_n(\mathbb{C})$ die Untergruppe der Diagonalmatrizen in $GL_n(\mathbb{C})$. Dann ist $(\mathrm{diag}_n)_{\mathsf{tor}}$ die Untergruppe aller Diagonalmatrizen, die als Diagonalelemente Einheitswurzeln haben.

In der linearen Algebra haben Sie oft ausgenutzt, dass lineare Abbildungen auf der Basis eines Vektorraums festgelegt sind. Für freie abelsche Gruppen gilt ein analoges Resultat:

Satz I.11.11. *Ist G frei abelsch mit Basis X und ist G' eine beliebige abelsche Gruppe, so gibt es für jede Abbildung von Mengen $f\colon X \to G'$ genau einen Homomorphismus $\psi_f\colon G \to G'$ mit $\psi_f|_X = f$.*

Beweis. Wir wissen, dass $G \cong \bigoplus_{x \in X} \langle x \rangle$. Somit ist jedes $g \in G$ von der Form $\sum_{x \in X} \alpha_x x$ mit $\alpha_x \in \mathbb{Z}$ und $\alpha_x = 0$ für fast alle x. Wir setzen $\psi_f(g) := \sum_{x \in X} \alpha_x f(x)$. Damit ist ψ_f durch f eindeutig festgelegt, es gilt $\psi_f(x) = f(x)$ für alle $x \in X$ und nach Konstruktion ist ψ_f ein Homomorphismus. □

Korollar I.11.12. *Jede abelsche Gruppe ist die Restklassengruppe einer frei abelschen Gruppe.*

Beweis. Es sei G eine abelsche Gruppe. Setze

$$F := \bigoplus_{g \in G} \mathbb{Z}.$$

Wir wissen, dass jedes $\mathbb{Z}$ unendlich zyklisch ist: $\mathbb{Z} = \langle 1 \rangle$. Wir schreiben das $\mathbb{Z}$ in Komponente $g \in G$ als $\mathbb{Z} \cong \langle x_g \rangle$ und setzen

$$X := \{x_g, g \in G\}.$$

Dann ist X eine Basis von F. Es sei $f\colon X \to G$ definiert als

$$f(x_g) := g.$$

Damit ist f eine Abbildung von Mengen und nach Satz I.11.11 gibt es einen eindeutigen Homomorphismus $\psi_f\colon F \to G$ mit $\psi_f(x_g) = g$. Nach Konstruktion ist ψ_f ein Epimorphismus, also erhalten wir

$$G \cong F/\ker(\psi_f).$$

□

Satz I.11.13. *Es seien F_1, F_2 zwei frei abelsche Gruppen mit Basis X_1 beziehungsweise X_2. Dann ist F_1 genau dann zu F_2 isomorph, wenn es eine Bijektion zwischen X_1 und X_2 gibt.*

BEWEIS. Es sei $f\colon X_1 \to X_2$ eine Bijektion mit Umkehrabbildung $f^{-1}\colon X_2 \to X_1$. Da $X_1 \subset F_1$ und $X_2 \subset F_2$ können wir f und f^{-1} auffassen als Abbildungen von Mengen $f\colon X_1 \to F_2$ und $f^{-1}\colon X_2 \to F_1$. Dann gibt es eindeutige Homomorphismen

$$\psi_f\colon F_1 \to F_2 \text{ und } \psi_{f^{-1}}\colon F_2 \to F_1 \text{ mit } \psi_f|_{X_1} = f, \psi_{f^{-1}}|_{X_2} = f^{-1}.$$

Für $\psi_f \circ \psi_{f^{-1}}$ gilt

$$\psi_f \circ \psi_{f^{-1}}|_{X_2} = \mathrm{id}_{F_2}|_{X_2}.$$

Genauso gilt

$$\psi_{f^{-1}} \circ \psi_f|_{X_1} = \mathrm{id}_{F_1}|_{X_1}.$$

Da diese Abbildungen auf den Basen festgelegt sind, folgt somit

$$\psi_{f^{-1}} \circ \psi_f = \mathrm{id}_{F_1} \text{ und } \psi_f \circ \psi_{f^{-1}} = \mathrm{id}_{F_2}$$

und $F_1 \cong F_2$.

Für die Rückrichtung betrachten wir eine frei abelsche Gruppe F mit Basis X. Die Menge $2F = \{2g, g \in F\}$ ist eine Untergruppe von F. Ein Element $\sum_{x\in X} \alpha_x x \in F$ ist genau dann in $2F$, wenn alle α_x gerade sind. Jede Nebenklasse von $2F$ hat also einen Repräsentanten der Form

$$\sum_{x\in X} \mu_x x \text{ mit } \mu_x \in \{0,1\}, \mu_x = 0 \text{ für fast alle } x.$$

Wir betrachten die Restklassengruppe $F/2F$. Diese ist ein $\mathbb{F}_2$-Vektorraum mit Basis X.

Sind jetzt F_1, F_2 zwei frei abelsche Gruppen und ist $F_1 \cong F_2$, so sind auch die $\mathbb{F}_2$-Vektorräume $F_1/2F_1$ und $F_2/2F_2$ isomorph. Dann müssen aber auch die Basen X_1 und X_2 in Bijektion stehen. □

Damit ist die folgende Zahl wohldefiniert:

Definition I.11.14. Ist F eine frei abelsche Gruppe mit Basis X, so heißt $|X|$ der *Rang von F*.

Vorlesung 14

Satz I.11.15. *Es sei G eine abelsche Gruppe und $H < G$, also $H \lhd G$. Ist G/H frei abelsch, so ist H ein direkter Summand von G, also $G \cong H \oplus Q$ und $Q \cong G/H$.*

BEWEIS. Wir betrachten die kanonische Projektion $\pi\colon G \to G/H$. Es sei X eine Basis von G/H. Wir definieren eine Abbildung von Mengen

$$f\colon X \to G, f(x) = g, \text{ für ein gewähltes } g \text{ mit } \pi(g) = x.$$

Wir erhalten einen eindeutigen Homomorphismus $\psi_f\colon G/H \to G$ mit $\psi_f(x) = f(x)$. Es gilt

$$\pi \circ \psi_f(\sum_{x\in X} \alpha_x x) = \pi(\sum_{x\in X} \alpha_x f(x)) = \sum_{x\in X} \alpha_x x,$$

weil $\pi(f(x)) = x$. Damit gilt

$$\pi \circ \psi_f = \mathrm{id}_{G/H}$$

und ψ_f ist injektiv.

Es sei $g \in \ker(\pi) \cap \mathrm{Bild}(\psi_f)$. Da $g \in \mathrm{Bild}(\psi_f)$, gibt es ein $y \in G/H$ mit $\psi_f(y) = g$. Da aber gleichzeitig gilt, dass $g \in \ker(\pi)$, folgt

$$0 = \pi(g) = \pi(\psi_f(y)) = y.$$

Also ist $y = 0$ und damit auch $g = \psi_f(y)$.

Für alle $g \in G$ ist $g - \psi_f(\pi(g))$ im Kern von π:

$$\pi(g - \psi_f(\pi(g))) = \pi(g) - \pi(\psi_f(\pi(g)) = \pi(g) - \pi(g) = 0.$$

Also können wir jedes $g \in G$ schreiben als

$$g = g - \psi_f(\pi(g)) + \psi_f(\pi(g))$$

mit $g - \psi_f(\pi(g)) \in \ker(\pi)$ und $\psi_f(\pi(g)) \in \mathrm{Bild}(\psi_f)$.

Es ist $\ker(\pi) = H$, und wir haben gezeigt, dass

$$G = H \times \mathrm{Bild}(\psi_f) \cong H \oplus \mathrm{Bild}(\psi_f).$$

Da ψ_f ein Monomorphismus ist, ist $\text{Bild}(\psi_f) \cong G/H$. □

Satz I.11.16. *Ist F frei abelsch mit endlichem Rang und ist $H < F$, so ist H ebenfalls frei abelsch und der Rang von H ist kleiner gleich dem Rang von F.*

Bemerkung I.11.17. Dieser Satz klingt selbstverständlich; er ist aber falsch, wenn man „abelsch“oder „frei“als Voraussetzung weglässt: Untergruppen freier Gruppen sind zwar frei, können aber größeren Rang haben als die ursprüngliche Gruppe. Untergruppen endlich erzeugter Gruppen müssen nicht endlich erzeugt sein.

Satz I.11.16 gilt leicht allgemeiner: Untergruppen beliebiger frei abelscher Gruppen sind frei abelsch.

Beweis. Wir machen Induktion über den Rang von F. Ist dieser gleich 1, so gilt $F \cong \mathbb{Z}$ und hier sind alle Untergruppen von der Form $m\mathbb{Z}$ für ein $m \in \mathbb{N}_0$. Diese Gruppen sind frei abelsch: $m\mathbb{Z} = \langle m \rangle$ für $m \neq 0$ und $0 = \bigoplus_{\varnothing} \mathbb{Z}$.

Für den Schritt von $n-1$ auf n betrachten wir ein F mit Basis $X = \{x_1, \ldots, x_n\}$ und $H < F$. Wir betrachten den Homomorphismus

$$h \colon H \to \mathbb{Z}, \quad h(\sum_{i=1}^{n} \alpha_i x_i) = \alpha_n.$$

Dann gilt $\ker(h) < F' \cap H < F'$ mit F' frei abelsch mit Basis $X' = \{x_1, \ldots, x_{n-1}\}$. Nach Induktionsannahme ist $\ker(h)$ frei abelsch mit einem Rang kleiner gleich $n-1$. Das Bild von h ist eine Untergruppe von $\mathbb{Z}$, ist also

$$\text{Bild}(h) \cong \begin{cases} \mathbb{Z}, & \text{oder} \\ 0. \end{cases}$$

Also gilt ebenfalls

$$H/\ker(h) \cong \begin{cases} \mathbb{Z}, & \text{oder} \\ 0. \end{cases}$$

Nehmen wir an, dass $H/\ker(h) = 0$, so ist $\ker(h) \cong H$, also ist H frei abelsch mit einem Rang kleiner gleich $n-1$.

Ist $H/\ker(h) \cong \mathbb{Z}$, so gibt es nach Satz I.11.15 ein $H' < H$, so dass $H \cong \ker(h) \oplus H'$ und $H' \cong H/\ker(h) \cong \mathbb{Z}$. Damit ist H frei abelsch und

$$\text{Rang}(H) = \text{Rang}(\ker(h)) + 1 \leqslant n - 1 + 1 = n.$$

□

Frei abelsche Gruppen sind nach Definition torsionsfrei. Es gilt eine partielle Umkehrung:

Satz I.11.18. *Eine endlich erzeugte abelsche torsionsfreie Gruppe ist frei abelsch.*

Beweis. Es sei G eine solche Gruppe und $S = \{s_1, \ldots, s_n\}$ sei eine endliche erzeugende Menge. Es sei $T = \{t_1, \ldots, t_k\}$ eine Teilmenge von S, die maximal ist mit der Eigenschaft, dass aus

$$\alpha_1 t_1 + \ldots + \alpha_k t_k = 0$$

schon folgt, dass $\alpha_1 = \ldots = \alpha_k = 0$.

Für alle $s \in S \setminus T$ gibt es also Zahlen $\beta, \beta_1, \ldots, \beta_k \in \mathbb{Z}$ mit

$$\alpha s = \beta_1 t_1 + \ldots + \beta_k t_k.$$

Da $S \setminus T$ endlich ist, gibt es ein $a \in \mathbb{Z}$, so dass $as \in \langle T \rangle$ gilt für alle $s \in S \setminus T$. Wir definieren

$$f \colon G \to G, \quad g \mapsto ag.$$

Damit ist f ein Homomorphimus $f \colon G \to \langle T \rangle$. Ist $f(g) = 0$, so ist $ag = 0$, aber G ist torsionsfrei. Somit muss g schon 0 gewesen sein. Also ist f ein Monomorphimus und G ist isomorph zu einer Untergruppe von $\langle T \rangle$. Da $\langle T \rangle$ frei abelsch ist, ist G somit auch frei abelsch nach Satz I.11.16. □

Damit erhalten wir eine Vorstufe des Klassifikationssatzes für endlich erzeugte abelsche Gruppen:

Korollar I.11.19. *Eine endlich erzeugte abelsche Gruppe G ist isomorph zu einer direkten Summe aus einer frei abelschen Gruppe von endlichem Rang und einer endlichen Gruppe.*

Beweis. Wir betrachten die Torsionsuntergruppe G_{tor} von G. Damit ist G/G_{tor} eine torsionsfreien endlich erzeugte Gruppe, also frei abelsch. Mit Satz I.11.15 ist G_{tor} ein direkter Summand von G und es gibt ein $F < G$ mit

$$G \cong G_{\mathsf{tor}} \oplus F.$$

Hierbei ist $F \cong G/G_{\mathsf{tor}}$, also frei abelsch.

Wir wissen, dass G_{tor} endlich erzeugt ist, also zum Beispiel

$$G_{\mathsf{tor}} = \{s_1, \ldots, s_n\}.$$

Jedes Elemente in G_{tor}, also insbesondere die s_i sind Torsionselemente. Es gibt also für jedes $1 \leqslant i \leqslant n$ ein $N(i)$ mit $N(i)s_i = 0$. Damit ist aber G_{tor} eine endliche Gruppe. □

Wir wollen G_{tor} feiner zerlegen.

Definition I.11.20. Es sei G eine endliche abelsche Gruppe und p sei eine Primzahl. Dann heißt

$$G_p := \{g \in G, \exists n \in \mathbb{N}_0, p^n g = 0\}$$

die *p-primäre Komponente von G.*

Satz I.11.21. *Es sei G abelsch und $|G| = p^k$ für eine Primzahl p und ein $k \in \mathbb{N}$. Ist $g \in G$ ein Element maximaler Ordnung in G. Dann ist $\langle g\rangle$ ein direkter Summand von G.*

Beweis. Es sei p^n die maximal vorkommende Ordnung eines Elementes in G. Dann gilt für alle $h \in G$, dass $p^n h = 0$ und $\mathsf{ord}(h) \mid p^n$.

Ist $g \in G$ mit $\mathsf{ord}(g) = p^n$ und $G = \langle g\rangle$, dann ist nichts zu zeigen.

Wir nehmen also an, dass $\langle g\rangle \neq G$ und $h \in G \setminus \langle g\rangle$. Es sei p^m die Ordnung von $h + \langle g\rangle$ in $G/\langle g\rangle$. Dann muss $m > 0$ sein, weil sonst $h \in \langle g\rangle$ wäre. Weiterhin muss es ein $a \in \mathbb{Z}$ geben, mit $p^m h = ag$, weil $p^m h \in \langle g\rangle$.

Daher gilt

$$0 = p^n h = p^{n-m} ag$$

und deshalb muss p a teilen. Es gibt also ein $b \in \mathbb{Z}$ mit $pb = a$.

Wir setzen

$$x := p^{m-1}h - bg.$$

Dann gilt $px = p^m h - pbg = 0$. Andererseits ist $x \notin \langle g\rangle$, denn sonst wäre auch $p^{m-1}h \in \langle g\rangle$. Also ist $\mathsf{ord}(x) = p$ und $\langle x\rangle \cap \langle g\rangle = \{0\}$.

Wir betrachten die kanonische Projektion

$$\pi\colon G \to G/\langle x\rangle.$$

Dann hat $\pi(g)$ maximale Ordnung in $G/\langle x\rangle$ und $|G/\langle x\rangle| = p^{k-1}$.

Per Induktion können wir also annehmen, dass $\langle \pi(g)\rangle$ ein direkter Summand von $G/\langle x\rangle$ ist, also gibt es ein $V < G/\langle x\rangle$ mit

$$G/\langle x\rangle \cong V \oplus \langle \pi(g)\rangle.$$

Wir betrachten das Urbild $U := \pi^{-1}(V) < G$.

Da $V \cap \langle \pi(g)\rangle = \{0\}$, muss $U \cap \langle g\rangle \subset \langle x\rangle$ gelten. Aber $\langle x\rangle \cap \langle g\rangle = \{0\}$, so dass $U \cap \langle g\rangle = \{0\}$ ist.

Es gilt weiterhin, dass $\langle U, g\rangle = G$, weil $G = \pi^{-1}(G/\langle x\rangle)$.

Insgesamt erhalten wir also

$$G = U \times \langle g\rangle = U \oplus \langle g\rangle.$$

□

Wir können die G_ps weiter aufdröseln:

Lemma I.11.22. *Es sei G eine endliche abelsche p-Gruppe für eine Primzahl p. Ist $|G| = p^n$, so gibt es eindeutige Zahlen $d_i \in \mathbb{N}$ mit*

$$d_1 \geqslant d_2 \geqslant \ldots \geqslant d_k > 0, \quad \sum_{i=1}^{k} d_i = n$$

und zyklische Untergruppen H_i von G mit $|H_i| = p^{d_i}$, so dass

$$G \cong H_1 \oplus \ldots \oplus H_k.$$

Beweis. Es sei g_1 ein Element maximaler Ordnung in G. Dann gilt mit Satz I.11.21, dass $G \cong \langle g_1 \rangle \oplus \tilde{G}$. Wir setzen $H_1 = \langle g_1 \rangle$ und machen weiter mit $\tilde{G}$. Wir erhalten iterativ $G \cong H_1 \oplus \ldots \oplus H_k$.

Zu zeigen ist die Eindeutigkeit der d_i: Wir machen dazu wiederum Induktion. Es sei

$$G^{(1)} := \{g \in G, pg = 0\} \text{ und } H_i^{(1)} := \{h \in H_i, ph = 0\}.$$

Aus $G = H_1 \oplus \ldots \oplus H_k$ folgt

$$G^{(1)} = H_1^{(1)} \oplus \ldots \oplus H_k^{(1)}.$$

Es gilt für alle i, dass $|H_i^{(1)}| = p$. Damit ist $|G^{(1)}| = p^k$. Also ist k eindeutig bestimmt. Außerdem ist

$$G/G^{(1)} \cong H_1/H_1^{(1)} \oplus \ldots \oplus H_k/H_k^{(1)}$$

und die $H_i/H_i^{(1)}$ sind zyklisch der Ordnung p^{d_i-1}. Mit Induktion über $|G|$ erhalten wir also, dass die $d_i - 1$ eindeutig sind für alle $d_i > 1$. Da wir k kennen und alle d_i mit $d_i > 1$, wissen wir auch, wie viele $d_i = 1$ vorkommen. □

Beispiel I.11.23. Für eine abelsche Gruppe G mit $|G| = p^2$ kommen als Möglichkeiten entweder $G \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ (also $d_1 = d_2 = 1$) oder $G \cong \mathbb{Z}/p^2\mathbb{Z}$ (also $d_1 = 2$) in Betracht.

Satz I.11.24 (Klassifikationssatz für endlich erzeugte abelsche Gruppen)**.** *Es sei G eine endlich erzeugte abelsche Gruppe. Dann gibt es ein $r \in \mathbb{N}_0$ und eindeutig bestimmte Primzahlpotenzen q_j, $1 \leqslant j \leqslant k$ mit $k \in \mathbb{N}_0$, so dass G/G_{tor} frei abelsch ist vom Rang r und*

$$G_{\mathsf{tor}} \cong \mathbb{Z}/q_1\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}/q_k\mathbb{Z}.$$

Beweis. Wir müssen zeigen, dass $G_{\mathsf{tor}} \cong G_{p_1} \oplus \ldots \oplus G_{p_k}$ wenn die p_i die Primteiler von $|G_{\mathsf{tor}}| = p_1^{\ell_1} \cdot \ldots \cdot p_k^{\ell_k}$ sind.

Die G_{p_i} sind jeweils normale Untergruppen von G_{tor} und sie sind p_i-Gruppen, die alle Untergruppen $H < G_{\mathsf{tor}}$ mit $|H| = p^a$ enthalten. Damit sind sie die p_i-Sylowuntergruppen von G_{tor}.

Ist $p_i \neq p_j$, so ist $G_{p_i} \cap G_{p_j} = \{0\}$, weil jedes Element g im Schnitt sowohl $p_i^n g = 0$ als auch $p_j^m g = 0$ erfüllen muss und das geht nur für $g = 0$.

Das innere Produkt der G_{p_1} bis G_{p_k} ist eine Untergruppe von G_{tor} und hat die gleiche Mächtigkeit wie $|G_{\mathsf{tor}}|$. Damit gilt

$$G_{\mathsf{tor}} = G_{p_1} \times \ldots \times G_{p_k} = G_{p_1} \oplus \ldots \oplus G_{p_k}.$$

Jedes G_{p_i} hat eine Zerlegung wie in Lemma I.11.22. □

KAPITEL II

Elementare Ringtheorie

Vorlesung 15

Ringtheorie ist ein weitreichendes Gebiet der Algebra, welches wir hier nur kurz anreissen. Mehr dazu finden Sie in [**1, 3, 4**].

II.1. Definitionen und Beispiele

Die folgende Definition kennen Sie aus der linearen Algebra.

Definition II.1.1.

(a) Eine Menge R mit zwei Verknüpfungen

$$+ : R \times R \to R \text{ und}$$
$$\cdot : R \times R \to R$$

heißt ein *Ring*, falls gilt:

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

(2) $\cdot$ ist assoziativ, das heißt, dass für alle $a, b, c \in R$ gilt

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c.$$

(3) Es gelten die Distributivgesetze. Für alle $a, b, c \in R$:

$$a \cdot (b + c) = a \cdot b + a \cdot c,$$
$$(a + b) \cdot c = a \cdot c + b \cdot c.$$

(a) Es gibt ein Einselement $1 \in R$, so dass für alle $a \in R$ gilt:

$$a \cdot 1 = a = 1 \cdot a.$$

(b) Ein Ring heißt *kommutativ*, falls für alle $a, b \in R$ gilt

$$a \cdot b = b \cdot a.$$

Bemerkung II.1.2.

- Es gibt den *Nullring* $R = \{0\}$, der nur aus dem Element 0 besteht mit $0 + 0 = 0$ und $0 \cdot 0 = 0$. Hier ist das Einselement gleich 0. Vorsicht: Viele allgemeine Eigenschaften von Ringen gelten für den Nullring nicht und wir werden ihn oft aus unseren Betrachtungen ausschließen.
- Wir benutzen „Punkt- vor Strichrechnung“ in Ringen.
- Ist 0 das neutrale Element in $(R, +)$, so gilt:

$$0 \cdot a = (0 + 0) \cdot a = 0 \cdot a + 0 \cdot a$$

und damit ist $0 \cdot a = 0$. Analog zeigen Sie, dass auch $a \cdot 0 = 0$ gilt.

- Es gelten viele weitere Rechenregeln, zum Beispiel

$$(-a)b = -(ab) = a(-b),$$

weil $(-a)b + ab = (-a + a)b = 0b = 0$

Definition II.1.3.

(a) Ist R ein Ring, so heißt ein $x \in R$ eine *Einheit*, falls es ein $y \in R$ gibt mit $xy = 1 = yx$.

(b) Die Menge der Einheiten in R bezeichnet man mit $R^\times$.

(c) Ist $R^\times = R \setminus \{0\}$ für einen Ring $R \neq 0$, so heißt R ein *Schiefkörper*.

(d) Ein kommutativer Schiefkörper heißt *Körper*.

Beispiele II.1.4.

- $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ und $\mathbb{C}$ sind kommutative Ringe und $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ sind Körper.
- Ist K ein Körper, so bilden die $n \times n$-Matrizen über K, $M(n \times n, K)$ einen Ring, den wir in dieser Vorlesung mit $M_n(K)$ bezeichnen.
- Ist $(R_i)_{i \in I}$ eine beliebige Familie von Ringen, so ist $\prod_{i \in I} R_i$ wieder ein Ring mit der komponentenweisen Addition und Multiplikation.
- Ist A eine abelsche Gruppe, so ist die Menge aller Endomorphismen von A, $\mathsf{End}(A)$, ein Ring: Für $f, g \in \mathsf{End}(A)$ und $a \in A$ sei
$$(f+g)(a) := f(a) + g(a) \quad (fg)(a) := f(g(a)).$$
- Ist $U \subset \mathbb{R}^n$ offen, so ist
$$C^k(U) := \{f \colon U \to \mathbb{R}, f \text{ } k\text{-mal stetig differenzierbar}\}$$
ein kommutativer Ring mit
$$(f+g)(x) := f(x) + g(x) \quad \text{und } (fg)(x) = f(x)g(x) \text{ für alle } f, g \in C^k(U), x \in U.$$
- Ist $(M, \cdot)$ ein Monoid, so ist $\mathbb{Z}[M]$ der *Monoidring* zu M: Elemente in $\mathbb{Z}[M]$ sind von der Form $\sum_{m \in M} a_m m$, wobei nur endlich viele $a_m \in \mathbb{Z}$ ungleich 0 sind. Die Addition ist definiert durch
$$\sum_{m \in M} a_m m + \sum_{m \in M} b_m m = \sum_{m \in M} (a_m + b_m) m$$
und die Multiplikation ist
$$\Big(\sum_{m \in M} a_m m\Big) \cdot \Big(\sum_{m \in M} b_m m\Big) = \sum_{m \in M} c_m m,$$
mit $c_\ell = \sum_{mn = \ell} a_m b_n$. Wichtig sind vor allem Gruppenringe, also $\mathbb{Z}[G]$, bei denen G eine Gruppe ist.
- Endliche Schiefkörper sind nach einem Satz von Wedderburn immer Körper (Joseph Henry Maclagan Wedderburn (1882–1948)).

Definition II.1.5.

- Sind R und R' Ringe und ist $f \colon R \to R'$ eine Abbildung, so heißt f ein *Ringhomomorphismus*, falls für alle $a, b \in R$ gilt:
  (a) $f(a+b) = f(a) + f(b)$,
  (b) $f(ab) = f(a)f(b)$ und
  (c) $f(1_R) = 1_{R'}$.
- Für einen Ringhomomorphismus $f \colon R \to R'$ ist der *Kern von* f
$$\ker(f) := \{r \in R, f(r) = 0_{R'}\}.$$

Bemerkung II.1.6. Begriffe wie Epi-, Mono- und Isomorphismen werden wie üblich benutzt. Ein Ringhomomorphismus ist genau dann ein Monomorphismus, wenn sein Kern nur aus der Null besteht.

Wir betrachten mehrere Sorten von Unterobjekten:

Definition II.1.7. Es sei R ein Ring.

(a) Eine Teilmenge $R' \subset R$ heißt ein *Unterring von* R, falls R' mit den Verknüpfungen aus R ein Ring ist mit $1_R = 1_{R'}$.
(b) Eine Teilmenge $I \subset R$ heißt ein *Linksideal* (beziehungsweise *Rechtsideal*) in R, falls $(I, +)$ eine Untergruppe von $(R, +)$ ist und wenn für alle $r \in R$ und $y \in I$ gilt: $ry \in I$ (beziehungsweise $yr \in I$).
(c) Ein *Ideal* in R ist eine Teilmenge $I \subset R$, die sowohl Rechts- als auch Linksideal ist. Möchte man das betonen, sagt man auch manchmal *beidseitiges Ideal*.

Beispiele II.1.8.

- In einem kommutativen Ring sind alle Linksideale auch Rechtsideale und umgekehrt.
- In jedem Ring R sind sowohl $\{0\}$ als auch R Ideale.
- Ist R kommutativ und $y \in R$, so ist die Teilmenge
$$yR := \{yr, r \in R\}$$
ein Ideal. Ideale dieser Form heißen *Hauptideale* und werden mit (y) abgekürzt.
- In $R = \mathbb{Z}$ ist für ein Ideal I insbesondere $(I, +) < (\mathbb{Z}, +)$, also ist I von der Form $n\mathbb{Z}$ mit $n \in \mathbb{N}_0$. Jede dieser Teilmengen $n\mathbb{Z}$ ist ein Ideal.
- Ist $R = M_2(K)$ für einen Körper K. Dann ist
$$I = \left\{ \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix}, a, b \in K \right\}$$
ein Linksideal in R und
$$J = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}, a, b \in K \right\}$$
ein Rechtsideal, aber beides sind keine beidseitigen Ideale. Zum Beispiel ist
$$\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \begin{pmatrix} x & y \\ z & w \end{pmatrix} = \begin{pmatrix} ax & ay \\ bx & by \end{pmatrix} \notin I.$$

Satz II.1.9. *Ist I ein beidseitiges Ideal eines Ringes R, so ist die Gruppe $(R, +)/(I, +)$ definiert. Sie erhält eine Multiplikation durch*
$$(r + I)(s + I) := rs + I$$
und wird damit zu einem Ring, dem Restklassenring, *R/I.*

Beweis. Wir zeigen, dass die obige Multiplikation wohldefiniert ist. Es sei also $r' = r + x$ und $s' = s + y$ mit $x, y \in I$. Dann ist nach Definition
$$(r' + I)(s' + I) = (r's') + I = (r + x)(s + y) + I = rs + ry + xs + xy + I.$$
Da aber $ry + xs + xy \in I$ sind, ist dies gleich $rs + I$.

Das Element $1_R + I$ ist das Einselement von R/I. Die Assoziativität und die Distributivgesetze vererben sich von R auf R/I.

□

Bemerkung II.1.10.

- Die kanonische Projektion $\pi\colon R \to R/I$ ist ein Ringhomomorphismus und surjektiv.
- Ist I ein beidseitiges Ideal in R, so gibt es eine Bijektion zwischen der Menge der Ideale $J \subset R$ mit $I \subset J$ und den Idealen $\bar{J} \subset R/I$, wobei J gerade $\pi^{-1}(\bar{J})$ ist. (Vergleiche Blatt 2, Aufgabe 3)
- Ist $f\colon R \to R'$ ein Ringhomomorphismus und ist $J \subset R'$ ein Ideal in R', so ist $f^{-1}(J)$ immer ein Ideal in R: Es ist klar, dass $(f^{-1}(J), +) < (R, +)$. Ist $x \in f^{-1}(J)$ und $r \in R$, so ist $rx \in f^{-1}(J)$, weil $f(rx) = f(r)f(x) \in J$. Genauso folgt $xr \in f^{-1}(J)$.
- Insbesondere ist $f^{-1}(\{0_{R'}\}) = \ker(f)$ immer ein beidseitiges Ideal in R für alle Ringhomomorphismen f.

Vorlesung 16

II.2. Ideale, Nullteiler und Charakteristik

Das Wort *Ideal* steht für *ideale Zahl*. Ideale wurden als Verallgemeinerungen von Zahlen eingeführt. Wie für Zahlen definieren wie einige Rechenoperationen auf Idealen:

Definition II.2.1. Es sei R ein Ring und I, J und I_γ für $\gamma \in \Gamma$ seien Ideale von R.

(a) $I + J := \{i + j, i \in I, j \in J\}$ ist ein Ideal von R.
(b) $\bigcap_{\gamma \in \Gamma} I_\gamma$ ist ein Ideal von R.

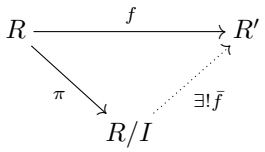
(c)
$$IJ = I \cdot J = \{\sum_{k=1}^{n} i_k j_k, i_k \in I, j_k \in J, n \in \mathbb{N}_0\}$$
ist ein Ideal von R.

(d) Speziell für $I = J$ ist $I^2 = I \cdot I$ definiert und wir setzen induktiv $I^n := I \cdot I^{n-1}$ für $n \in \mathbb{N}$ und $I^0 := R$.

Bemerkung II.2.2. Es gilt immer, dass $I \cdot J \subset I \cap J$ gilt, weil jedes $i_k j_k$ mit $i_k \in I$ und $j_k \in J$ in $I \cap J$ liegt und damit auch jede endliche Summe solcher Elemente.

Beispiel II.2.3. Ist $R = \mathbb{Z}$ und $I = n\mathbb{Z}$, $J = m\mathbb{Z}$, so ist $IJ = (n\mathbb{Z})(m\mathbb{Z}) = (nm)\mathbb{Z}$ aber
$$I \cap J = n\mathbb{Z} \cap m\mathbb{Z} = \{x \in \mathbb{Z}, n \mid x \text{ und } m \mid x\} = \mathsf{kgV}(n, m)\mathbb{Z}.$$
Insbesondere müssen IJ und $I \cap J$ nicht gleich sein. Zum Beispiel ist $(2\mathbb{Z})(6\mathbb{Z}) = 12\mathbb{Z}$, aber $2\mathbb{Z} \cap 6\mathbb{Z} = 6\mathbb{Z}$.

Satz II.2.4 (Isomorphiesatz für Ringe)**.** *Ist $f\colon R \to R'$ ein Ringhomomorphismus und ist $I \subset R$ ein Ideal mit $I \subset \ker(f)$, so gibt es genau einen Ringhomomorphismus $\bar{f}\colon R/I \to R'$ mit $\bar{f} \circ \pi = f$.*



Speziell für $I = \ker(f)$ erhalten wir einen Isomorphismus
$$\bar{f}\colon R/\ker(f) \to \mathrm{Bild}(f).$$

Beweis. Der Beweis ist völlig analog zu dem Beweis im Kontext von Gruppen.

Die Forderung $\bar{f} \circ \pi = f$ zwingt uns, $\bar{f}(r + I) = f(r)$ zu setzen. Damit ist $\bar{f}$ eindeutig festgelegt, wohldefiniert und eine Ringhomomorphismus; das rechnen Sie nach.

Für $I = \ker(f)$ ist $\bar{f}$ dann injektiv, weil aus
$$\bar{f}(r + I) = f(r) = 0_{R'}$$
folgt, dass $f \in \ker(f)$ ist. Damit ist $\bar{f}$ ein Isomorphismus auf $\mathrm{Bild}(f)$. □

Das folgende Phänomen kennen Sie schon aus dem Ring der quadratischen Matrizen:

Definition II.2.5. Es sei R ein Ring.

(a) Ein $a \in R$ heißt ein *Linksnullteiler* (beziehungsweise *Rechtsnullteiler*), falls es ein $x \in R \setminus \{0\}$ gibt mit $ax = 0_R$ (beziehungsweise $xa = 0$).

(b) Ein *Nullteiler* ist ein Links- oder Rechtsnullteiler.

Lemma II.2.6. *Ist $a \in R$ kein Linksnullteiler, so folgt aus $ax = ay$ schon, dass $x = y$ ist. Ist $b \in R$ kein Rechtsnullteiler, so folgt aus $xb = yb$, dass $x = y$ ist.*

Beweis. Ist $ax = ay$, so erhalten wir $a(x - y) = 0_R$ und da a kein Linksnullteiler ist, impliziert dies $x - y = 0$, also $x = y$. Der andere Fall geht analog. □

Definition II.2.7.

(a) Ist $R \neq 0$ ein kommutativer Ring und hat R keine Nullteiler $\neq 0_R$, so heißt R ein *Integritätsbereich*.

(b) Ein Integritätsbereich, in dem jedes Ideal ein Hauptideal ist, heißt ein *Hauptidealring*.

Beispiele II.2.8.

- Ist R ein Körper, so ist R ein Integritätsbereich.
- Wir wissen schon, dass $\mathbb{Z}$ ein Hauptidealring ist.

- Sind R_1, R_2 (kommutative) Ringe, so hat $R_1 \times R_2$ immer Nullteiler, weil für alle $r_1 \in R_1$ und $r_2 \in R_2$ gilt
$$(r_1, 0_{R_2})(0_{R_1}, r_2) = (0_{R_1}, 0_{R_2}) = 0_{R_1 \times R_2}.$$
Produkte von Ringen sind also niemals Integritätsbereiche.
- Der Ring $\mathbb{Z}/n\mathbb{Z}$ hat nicht-triviale Nullteiler, wenn n nicht prim ist. Ist $n = ab$, $a, b \neq 1, n$, so ist $\bar{a} \neq \bar{0} \neq \bar{b}$, aber $\bar{0} = \bar{n} = \bar{a}\bar{b} = \bar{a}\bar{b}$.

Lemma II.2.9. *Für jeden beliebigen Ring R gibt es genau einen Ringhomomorphismus von $\mathbb{Z}$ nach R.*

Beweis. Da $(R, +)$ eine abelsche Gruppe ist, ist für alle $n \in \mathbb{Z}$ und alle $r \in R$ das Element $nr \in R$ definiert. Ist $f\colon \mathbb{Z} \to R$ ein Ringhomomorphismus, so muss $f(1) = 1_R$ gelten. Damit ist für alle $n \in \mathbb{Z}$
$$f(n) = f(n \cdot 1) = n \cdot 1_R.$$
Dadurch ist f aber schon festgelegt und existiert für alle R. □

Definition II.2.10. Wir bezeichnen den eindeutigen Ringhomomorphismus von $\mathbb{Z}$ nach R mit χ_R.

Das eindeutig bestimmte $n \in \mathbb{N}_0$ mit $n\mathbb{Z} = \ker(\chi)$ heißt die *Charakteristik von R* und wird mit $\mathsf{Char}(R)$ notiert.

Beispiele II.2.11.
- Es gilt $\mathsf{Char}(\mathbb{Z}) = 0$, weil $\chi_{\mathbb{Z}} = \mathrm{id}_{\mathbb{Z}}$.
- für $1 \neq n \in \mathbb{N}$ ist $\mathsf{Char}(\mathbb{Z}/n\mathbb{Z}) = n$, weil
$$\chi_{\mathbb{Z}/n\mathbb{Z}} = \pi\colon \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$$
und weil $\ker(\pi) = n\mathbb{Z}$.
- Für $\mathbb{Q}$ gilt $\mathsf{Char}(\mathbb{Q}) = 0$, weil $\chi_{\mathbb{Q}}(x) = x \neq 0$ für alle $x \neq 0$.
- Allgemeiner gilt: Ist R ein Integritätsbereich, so ist $\mathsf{Char}(R) = 0$ oder $\mathsf{Char}(R) = p$ für eine Primzahl p. Wäre $\mathsf{Char}(R) = n = ab$ und $1 \neq a, b \in \mathbb{N}$, so wäre
$$0_R = n \cdot 1_R = (ab) \cdot 1_R = (a \cdot 1_R)(b \cdot 1_R)$$
aber $a, b < n$.
- Sie wissen schon, dass $\mathbb{Z}/p\mathbb{Z}$ ein Körper ist für jede Primzahl p und $\mathsf{Char}(\mathbb{Z}/p\mathbb{Z}) = p$.

II.3. Primideale und maximale Ideale

In diesem Abschnitt betrachten wir ausschließlich kommutative Ringe.

Definition II.3.1.
(a) Ein Ideal $\mathfrak{p} \subset R$ heißt *Primideal*, falls $\mathfrak{p} \neq R$ und falls gilt: Ist $ab \in \mathfrak{p}$, so ist $a \in \mathfrak{p}$ oder $b \in \mathfrak{p}$.
(b) Ein Ideal $\mathfrak{m} \subset R$ heißt *maximal*, falls $\mathfrak{m} \neq R$ und falls es kein Ideal $I \subset R$ gibt mit
$$\mathfrak{m} \subsetneq I \subsetneq R.$$

Primideale und maximale Ideale geben hochwertige Restklassenringe:

Lemma II.3.2. *Es seien $\mathfrak{p}$ und $\mathfrak{m}$ Ideale in R. Dann gilt*
(a) *Das Ideal $\mathfrak{m}$ ist genau dann maximal, wenn $R/\mathfrak{m}$ ein Körper ist.*
(b) *Das Ideal $\mathfrak{p}$ ist genau dann ein Primideal, wenn $R/\mathfrak{p}$ ein Integritätsbereich ist.*

Beweis. Für (a) wissen wir, dass $R/\mathfrak{m}$ keine echten Ideale hat, falls $R/\mathfrak{m}$ ein Körper ist. Damit gibt es dann keine Ideale zwischen $\mathfrak{m}$ und R.

Ist $\mathfrak{m}$ umgekehrt maximal und ist $x \in R \setminus \mathfrak{m}$, so ist $xR \neq \mathfrak{m}$. Damit ist $\mathfrak{m}$ eine echte Teilmenge von $\mathfrak{m} + xR$ und $\mathfrak{m} + xR$ ist ein Ideal in R. Wegen der Maximalität von $\mathfrak{m}$ muss dann $\mathfrak{m} + xR = R$ sein. Insbesondere gibt es ein $y \in R$ und ein z in $\mathfrak{m}$, so dass $1_R = z + xy$ gilt. Damit ist $x + \mathfrak{m}$ aber eine Einheit in $R/\mathfrak{m}$ und somit ist
$$(R/\mathfrak{m})^\times = (R/\mathfrak{m}) \setminus \{0_{R/\mathfrak{m}}\}.$$

Zu (b): Ist $R/\mathfrak{p}$ ein Integritätsbereich, so ist dies äquivalent dazu, dass aus
$$(a + \mathfrak{p})(b + \mathfrak{p}) = \mathfrak{p}$$
folgt, dass a oder b aus $\mathfrak{p}$ ist und das ist genau die Eigenschaft von $\mathfrak{p}$ prim zu sein. □

Bemerkung II.3.3. Lemma II.3.2 besagt auch, dass jedes maximale Ideal ein Primideal ist. Die Umkehrung gilt nicht: Für $R = \mathbb{Z}$ sind die Ideale der Form $p\mathbb{Z}$ für p prim Primideale und auch maximal, weil $Z/p\mathbb{Z}$ ein Körper ist. Da $\mathbb{Z}$ Integritätsbereich ist, ist $(0) = 0\mathbb{Z}$ ein Primideal, aber es ist nicht maximal.

Die Ideale der Form $n\mathbb{Z}$ für n weder 0 noch prim sind keine Primideale. Wir wissen schon, dass $\mathbb{Z}/n\mathbb{Z}$ dann entweder der Nullring ist (für $n = 1$) oder echte Nullteiler hat.

Für das folgende Resultat nehmen wir an, dass das Lemma von Zorn oder äquivalent dazu das Auswahlaxiom gilt.

Satz II.3.4.

(a) *Jeder kommutative Ring $R \neq 0$ besitzt ein maximales Ideal.*
(b) *Ist $\{0_R\} \neq I \subsetneq R$ ein Ideal, so gibt es ein maximales Ideal $\mathfrak{m}$ mit $I \subset \mathfrak{m}$.*

Beweis. Die Behauptung (b) folgt aus (a), indem wir den Ring R/I betrachten. Wir zeigen also (a). Wir setzen

$$S := \{I \subset R, I \text{ Ideal}, I \neq R\}.$$

Dann ist S nicht leer, weil $(0) \in S$.

Wir definieren eine partielle Ordnung auf S, indem wir sagen, dass $I \leqslant J$ ist, wenn $I \subset J$.

Es sei T eine total geordnete Teilmenge von S. Wir setzen

$$\mathfrak{J}_T := \bigcup_{I \in T} I$$

und behaupten, dass $\mathfrak{J}_T$ eine obere Schranke für T ist.

- Für alle $I \in T$ gilt $I \leqslant \mathfrak{J}_T$, weil nach Konstruktion $I \subset \mathfrak{J}_T$.
- Es gilt $\mathfrak{J}_T \in S$: Sind $a, b \in \mathfrak{J}_T$, so gibt es $I, J \in T$, mit $a \in I$, $b \in J$. Da T total geordnet ist, gilt $I \subset J$ oder $J \subset I$. Ohne Beschränkung der Allgemeinheit nehmen wir an, dass $I \subset J$. Dann sind $a + b \in J \subset \mathfrak{J}_T$ und $xa \in J \subset \mathfrak{J}_T$ für alle $x \in R$. Damit ist $\mathfrak{J}_T$ ein Ideal in R.
- Wäre $\mathfrak{J}_T = R$, so wäre insbesondere $1_R \in \mathfrak{J}_T$. Dann gibt es ein $I \in T$ mit $1_R \in I$, aber dann ist $I = R$ im Widerspruch zu $I \in S$.

Das Lemma von Zorn gibt nun, dass S ein maximales Element hat. Dies ist ein maximales Ideal in R. □

II.4. Teilerfremdheit und Teilbarkeit

Definition II.4.1. Zwei Ideale I, J in einem kommutativen Ring R heißen *teilerfremd*, falls $I + J = R$ gilt.

Bemerkung II.4.2. Damit sind I und J genau dann teilerfremd, wenn es ein $x \in I$ und ein $y \in J$ gibt mit $x + y = 1_R$.

Sind I und J teilerfremd, so gilt auch

$$IJ = I \cap J :$$

Ist $a \in I \cap J$ und sind $x \in I$, $y \in J$ mit $x + y = 1_R$ gegeben, so ist

$$a = a \cdot 1_R = a(x + y) = ax + ay \in IJ + IJ = IJ.$$

Im Kontext von Gruppen hatten wir analoge Resultate zu dem Folgenden:

Satz II.4.3. *Ist $0 \neq R$ ein kommutativer Ring und sind $I_1, \ldots, I_n$ Ideale in R, die paarweise teilerfremd sind. Dann gilt:*

(a) *I_i ist teilerfremd zu $I_1 \cdot \ldots \cdot I_{i-1} \cdot I_{i+1} \cdot \ldots \cdot I_n$ für $1 \leqslant i \leqslant n$.*
(b) *$I_1 \cdot \ldots \cdot I_n = \bigcap_{i=1}^n I_i$.*
(c) *Die Projektion $\varphi\colon R \to \prod_{i=1}^n R/I_i$ induziert einen Isomorphismus*

$$R/I_1 \cdot \ldots \cdot I_n \cong \prod_{i=1}^n R/I_i.$$

Vorlesung 17

BEWEIS. Wir zeigen (a). Die restlichen Beweise laufen analog zu denen für Gruppen. Für ein festes i gilt wegen der paarweisen Teilerfremdheit der Ideale für alle $j \neq i$, dass es ein $x_j \in I_i$ und ein $y_j \in I_j$ gibt mit $x_j + y_j = 1_R$. Damit können wir die 1_R schreiben als

$$1_R = \prod_{j \neq i}(x_j + y_j) = y_1 \cdot \ldots \cdot y_{i-1} \cdot y_{i+1} \cdot \ldots \cdot y_n + \text{ Restterme.}$$

Da die Restterme alle ein $x_j \in I_i$ erhalten, gilt

$$1_R = s + r$$

mit $s \in I_1 \cdot \ldots \cdot I_{i-1} \cdot I_{i+1} \cdot \ldots \cdot I_n$ und $r \in I_i$. Das zeigt (a). □

Definition II.4.4. Es sei R ein Integritätsbereich und $a, b \in R$.

(a) Wir sagen a *teilt* b ($a \mid b$), falls es ein $c \in R$ gibt mit $ac = b$.
(b) Wir nennen a *assoziiert zu* b, falls $a \mid b$ und $b \mid a$.
(c) Ein $p \in R$ heißt *Primelement* oder *prim*, falls $p \neq 0$ und falls $(p) = pR$ ein Primideal ist.
(d) Ein $u \in R$ heißt *irreduzibel* oder *unzerlegbar*, falls $u \neq 0$, $u \notin R^\times$, und wenn aus $u = ab$ mit $a, b \in R$ folgt, dass a oder b eine Einheit ist.

Beispiel II.4.5. Ein $p \in \mathbb{Z}$ ist genau dann ein Primelement in $\mathbb{Z}$, wenn p eine Primzahl ist.

Im Ring der Gaußschen Zahlen $\mathbb{Z}[i]$ ist $1 + i$ ein Primelement. Eine Primzahl $p \in \mathbb{Z}$ ist nicht unbedingt ein Primelement in $\mathbb{Z}[i]$.

Lemma II.4.6. *Ein $u \in R$ ist genau dann irreduzibel, falls $R \neq (u) \neq (0)$ und falls für alle $a \in R$ gilt:*

$$(u) \subset (a) \Rightarrow (a) = (u) \text{ oder } (a) = R.$$

BEWEIS. Ist $(u) \subset (a)$, dann ist a ein Teiler von u, also gibt es ein $b \in R$ mit $ab = u$. Da u irreduzibel ist, ist $a \in R^\times$ oder $b \in R^\times$. Im ersten Fall ist $(a) = R$. Im zweiten Fall ist $(u) = (a)$.

Für die Rückrichtung schreiben wir $u = ab$, also $(u) \subset (a)$. Damit folgt nach Annahme, dass $(a) = (u)$ ist oder $(a) = R$. Im ersten Fall muss $b \in R^\times$ sein, im zweiten ist $a \in R^\times$.

□

Satz II.4.7. *Es sei R ein Integritätsbereich.*

(a) *Ist $p \in R$ prim, so ist p irreduzibel.*
(b) *Ist R ein Hauptidealring, so gilt*

$$p \text{ ist prim } \Leftrightarrow p \text{ ist irreduzibel.}$$

Außerdem gilt: Ist $0 \neq \mathfrak{p}$ ein Primideal in R, so ist $\mathfrak{p}$ auch maximal.

BEWEIS. Für (a) schreiben wir $p = ab$ und p sei prim. Dann gilt, $p \mid a$ oder $p \mid b$. Wir nehmen ohne Beschränkung der Allgemeinheit an, dass $p \mid a$. Aber a und b teilen beide p. Damit folgt, dass p assoziiert ist zu a. Schreiben wir a explizit als $a = cp$, so folgt

$$p = ab = bcp \Rightarrow (1 - bc)p = 0 \Rightarrow 1 - bc = 0 \Rightarrow b \in R^\times.$$

Also ist p auch irreduzibel.

Für (b) nehmen wir an, dass p irreduzibel ist. Dann gibt es keine echten Ideale oberhalb von (p), also ist $R/(p)$ ein Körper und (p) ist ein maximales Ideal. Damit ist (p) auch ein Primideal und p ist prim.

Ist $0 \neq \mathfrak{p}$ ein Primideal und R ist ein Hauptidealring, so ist $\mathfrak{p} = (p)$ für ein Primelement p. Damit ist $\mathfrak{p}$ dann aber auch maximal mit dem gleichen Argument wie oben. □

Definition II.4.8. Es sei $0 \neq R$ ein kommutativer Ring. Zu $a, b \in R$ heißt $d \in R$ ein *größter gemeinsamer Teiler von a und b* ($d = \mathsf{ggT}(a, b)$), falls gilt:

$$d \mid a, d \mid b \text{ und für alle } x \in R \text{ mit } x \mid a, x \mid b \text{ gilt } x \mid d.$$

Analog heißt ein $v \in R$ ein *kleinstes gemeinsames Vielfaches von a und b* ($v = \mathsf{kgV}(a, b)$), falls gilt: $a \mid v$ und $b \mid v$ und für alle $x \in R$ mit $a \mid x$ und $b \mid x$ gilt $v \mid x$.

Es ist überhaupt nicht klar, dass solche Objekte existieren. Was sollte zum Beispiel der kgV von $2+10\mathbb{Z}$ und $5+10\mathbb{Z}$ in $\mathbb{Z}/10\mathbb{Z}$ sein?

Ist der ggT und der kgV jeweils eindeutig, falls er existiert?

Satz II.4.9. *Ist R ein Hauptidealring, so gibt es zu je zwei $a, b \in R$ ein $\mathsf{ggT}(a,b)$ und ein $\mathsf{kgV}(a,b)$.*

Beweis. Zu $a, b \in R$ ist $(a)+(b)$ wiederum ein Ideal in R, also von der Form $(a)+(b)=(d)$ für ein $d \in R$. Da $(a) \subset (d)$ und $(b) \subset (d)$ gilt, dass $d \mid a$ und $d \mid b$. Ist $x \in R$ mit $x \mid a$ und $x \mid b$ gegeben, so gilt

$$(d) = (a)+(b) \subset (x),$$

also $x \mid d$ und $d = \mathsf{ggT}(a,b)$.

Analog ist $(a) \cap (b)$ wieder ein Ideal in R, also

$$(a) \cap (b) = (v) \text{ für ein } v \in R.$$

Dann ist $(v) \subset (a)$ und $(v) \subset (b)$, also $a \mid v$ und $b \mid v$. Ist $x \in R$ gegeben mit $a \mid x$ und $b \mid x$, so ist

$$(x) \subset (a) \cap (b) = (v)$$

also $v \mid x$ und $v = \mathsf{kgV}(a,b)$. □

Definition II.4.10. Ist R ein Integritätsbereich, so heißen $a, b \in R$ *teilerfremd*, falls $1_R = \mathsf{ggT}(a,b)$.

Aus dem, was wir bereits gezeigt haben, erhalten wir sofort die folgenden Äquivalenzen:

Korollar II.4.11. *Ist R ein Hauptidealring und $a, b \in R$, dann sind äquivalent:*

(a) *a und b sind teilerfremd,*
(b) *(a) und (b) sind teilerfremd,*
(c) *es gibt $x, y \in R$: $ax + by = 1_R$.*

II.5. Faktorielle und noethersche Ringe

Wir schreiben $a \sim b$, falls a und b zueinander assoziiert sind.

Satz II.5.1. *Für einen Integritätsbereich sind äquivalent:*

(a) *Jedes $0 \neq a \in R$, $a \notin R^\times$ lässt sich als endliches Produkt $a = u_1 \cdot \ldots \cdot u_n$ schreiben, wobei die u_i unzerlegbar sind. Gilt*

$$a = u_1 \cdot \ldots \cdot u_n = v_1 \cdot \ldots \cdot v_m$$

mit v_i unzerlegbar, so ist $n = m$ und es gibt ein $\sigma \in \Sigma_n$ mit $u_i \sim v_{\sigma(i)}$ für alle $1 \leqslant i \leqslant n$.

(b) *Jedes $0 \neq a \in R$, $a \notin R^\times$ lässt sich als endliches Produkt $a = u_1 \cdot \ldots \cdot u_n$ schreiben, wobei die u_i unzerlegbar sind und jedes unzerlegbare Element $u \in R$ ist auch prim.*

Beweis. Für (a) ⇒ (b) nehmen wir an, dass $u \in R$ unzerlegbar ist und a, b seien aus R mit $u \mid ab$. Dann gibt es also ein $d \in R$ mit $ud = ab$.

Ist $a = 0$ (oder $b = 0$), so teilt u a (oder b).

Ist $a \in R^\times$ (oder $b \in R^\times$), so ist $ua^{-1}d = b$ (oder $ub^{-1}d = a$), so dass $u \mid b$ (oder $u \mid a$).

Wir können also annehmen, dass $0 \neq a, b$ und $a, b \notin R^\times$. Damit ist dann auch $0 \neq d$ und $d \notin R^\times$. Wir schreiben $a = p_1 \cdot \ldots \cdot p_n$, $b = q_1 \cdot \ldots \cdot q_m$ und $d = v_1 \cdot \ldots \cdot v_k$ mit unzerlegbaren p_i, q_j und v_ℓ. Damit ist dann auch

$$ud = uv_1 \cdot \ldots \cdot v_k = p_1 \cdot \ldots \cdot p_n q_1 \cdot \ldots \cdot q_m$$

und nach Voraussetzung ist dann $k+1 = n+m$ und es gibt ein p_i mit $u \sim p_i$ oder es gibt ein q_j mit $q_j \sim u$. Dann teilt u aber a oder b.

Für (b) ⇒ (a) Nehmen wir an, dass

$$a = u_1 \cdot \ldots \cdot u_n = v_1 \cdot \ldots \cdot v_m$$

mit u_i, v_j unzerlegbar, also auch prim. Wir machen Induktion nach $n+m$.

Ist $n+m = 2$, so ist $a = u_1 = v_1$.

Ist $n+m>2$, so gilt $u_1 \mid v_1 \cdot \ldots \cdot v_m$. Da u_1 prim ist, gibt es ein j, so dass $u_1 \mid v_j$. Da beide Elemente unzerlegbar sind, gibt es ein $\lambda \in R^\times$ mit $\lambda u_1 = v_j$ und somit ist

$$u_1 \cdot \ldots \cdot u_n = \lambda v_1 \cdot \ldots \cdot v_{j-1} \cdot u_1 \cdot v_{j+1} \cdot \cdot v_m$$

und kürzen ergibt

$$u_2 \cdot \ldots \cdot u_n = \lambda v_1 \cdot \ldots \cdot v_{j-1} \cdot v_{j+1} \cdot \ldots \cdot v_m.$$

Nach Induktionsannahme ist dann $n-1 = m-1$ und u_i ist jeweils assoziiert zu einem v_ℓ für $1 \leqslant \ell \neq j \leqslant m$. Da $u_1 \sim v_j$, folgt die Behauptung. □

Definition II.5.2. Ein Integritätsbereich, der die Eigenschaften aus Satz II.5.1 hat, heißt *faktorieller Ring.*

Beispiele II.5.3.

- Der Ring $\mathbb{Z}[\sqrt{-5}]$ ist *nicht* faktoriell. Wir betrachten dazu die Normabbildung

  $$N\colon \mathbb{Z}[\sqrt{-5}] \to \mathbb{Z}, \quad x + y\sqrt{-5} \mapsto x^2 + 5y^2.$$

  Für $u \in \{3, 2+\sqrt{-5}, 2-\sqrt{-5}\}$ ist $N(u) = 9$. Nehmen wir an, dass $u = ab$. Dann ist $N(u) = 9 = N(a)N(b)$, weil die Norm multiplikativ ist. Die Werte $N(a) = 3$ oder $N(b) = 3$ können aber nicht angenommen werden. Damit ist $N(a) = 1$ oder $1 = N(b)$ und somit müssen a und b Einheiten sein. Die Elemente sind also $3, 2+\sqrt{-5}, 2-\sqrt{-5}$ alle unzerlegbar, aber

  $$9 = 3 \cdot 3 = (2+\sqrt{-5})(2-\sqrt{-5}),$$

  so dass die Zerlegung nicht eindeutig ist.
- Der Ring der Gaußschen Zahlen $\mathbb{Z}[i]$ ist faktoriell.

In faktoriellen Ringen können Sie mit ggTs und kgVs rechnen wie in $\mathbb{Z}$:

Korollar II.5.4. *Es sei R ein faktorieller Ring. Sind $0 \neq a, b \in R$ mit*

$$a = s p_1^{\ell_1} \cdot \ldots \cdot p_n^{\ell_n}, \quad b = t p_1^{k_1} \cdot \ldots \cdot p_n^{k_n}$$

mit $s, t \in R^\times$, $\ell_i, k_i \in \mathbb{N}$ und $p_1, \ldots, p_n$ eine Menge von paarweise nicht assoziierten unzerlegbaren Elementen in R, so gilt:

(a)
$$a \mid b \Leftrightarrow \ell_i \leqslant k_i \text{ für alle } 1 \leqslant i \leqslant n.$$

(b) *Ist $m_i = \min(\ell_i, k_i)$ und $M_i = \max(\ell_i, k_i)$, so ist*

$$\prod_{i=1}^n p_i^{m_i} = \mathsf{ggT}(a,b) \text{ und } \prod_{i=1}^n p_i^{M_i} = \mathsf{kgV}(a,b).$$

(c) *Für alle $c \in R$ gilt: Teilt a das Produkt bc und ist $1 = \mathsf{ggT}(a,b)$ so gilt $a \mid c$.*

□

Korollar II.5.5. *Ist R ein faktorieller Ring, so gibt es zu einem festen $0 \neq a \in R$ nur endlich viele verschiedene Hauptideale (b) mit $(a) \subset (b)$.*

Beweis. Ist $a \in R^\times$, so ist $(a) = R$ und die Behauptung gilt trivialerweise. Es sei also a keine Einheit. Dann schreiben wir a als

$$a = u_1 \cdot \ldots \cdot u_n$$

mit unzerlegbaren u_i. Ist $(a) \subset (b)$, so gibt es ein $d \in R$ mit $a = db$. Dann muss b assoziiert sein zu $u_{i_1} \cdot \ldots \cdot u_{i_k}$ für $1 \leqslant i_1 < \ldots < i_k \leqslant n$ und $(b) = (u_{i_1} \cdot \ldots \cdot u_{i_k})$. □

Satz II.5.6. *Ein Integritätsbereich ist genau dann faktoriell, wenn jedes unzerlegbare Element prim ist und jede aufsteigende Kette von Hauptidealen*

$$(a_0) \subset (a_1) \subset \ldots$$

stationär wird, das heißt, es gibt ein $n_0 \in \mathbb{N}$ mit $(a_m) = (a_{n_0})$ für alle $m \geqslant n_0$.

Vorlesung 18

BEWEIS. Die Richtung $\Rightarrow$ folgt direkt mit Korollar II.5.5. Für die Rückrichtung definieren wir

$$H := \{(a) \subset R, 0 \neq a \notin R^\times, a \text{ ist kein Produkt von unzerlegbaren Elementen}\}.$$

Annahme, $H \neq \varnothing$. Hat H kein maximales Element, so gilt sofort, dass es eine aufsteigende Kette von Hauptidealen gibt, die nicht abbricht.

Hat H ein maximales Element (a), so ist a selbst nicht unzerlegbar. Es gibt also $b, c \in R$, $b, c \notin R^\times$ mit $a = bc$. Dann ist

$$(a) \subsetneq (b) \text{ und } (a) \subsetneq (c)$$

und da (a) maximal ist, können (b) und (c) nicht in H liegen. Damit können wir b und c als Produkt von Unzerlegbaren schreiben, aber dann auch a, was im Widerspruch zu $a \in H$ steht. Also ist $H = \varnothing$. □

Definition II.5.7. Es sei R ein kommutativer Ring. Dann heißt R *noethersch*, falls jede aufsteigende Kette von Idealen

$$I_0 \subset I_1 \subset \dots$$

stationär wird.

Amalie („Emmy“) Noether (1882–1935). Der Begriff der noetherschen Ringe ist grundlegend für die gesamte Ringtheorie. Körper sind natürlich noethersche Ringe, aber auch $\mathbb{Z}$ und $K[X]$, falls K ein Körper ist. Ist R noethersch, so auch R/I für alle Ideale $I \subset R$. Der Hilbertsche Basissatz besagt, dass für jeden noetherschen Ring R auch $R[X]$ noethersch ist.

Satz II.5.8. *Für einen kommutativen Ring R sind äquivalent:*

(a) *R ist noethersch,*
(b) *In jeder nicht-leeren Menge von Idealen in R gibt es ein maximales Element bezüglich der Inklusion,*
(c) *Jedes Ideal $I \subset R$ ist endlich erzeugt; es gibt also $a_1, \dots, a_n \in R$, so dass*

$$I = (a_1, \dots, a_n) = (a_1) + \dots + (a_n).$$

BEWEIS. Für (a) $\Rightarrow$ (b) zeigen wir $\neg$ (b) $\Rightarrow \neg$(a). Es sei also $\mathfrak{M}$ eine solche Menge von Idealen in R ohne maximales Element. Es gibt also für jedes $I_1 \in \mathfrak{M}$ ein $I_2 \in \mathfrak{M}$ mit $I_1 \subsetneq I_2$. Wir können damit eine aufsteigende Folge von Idealen konstruieren, die nicht stationär wird.

Für (b) $\Rightarrow$ (c) betrachten wir ein Ideal $I \subset R$ und wir setzen

$$\mathfrak{N} := \{J \subset R \text{ Ideal }, J \text{ endlich erzeugt und } J \subset I\}.$$

Dann ist $\mathfrak{N} \neq \varnothing$, weil für jedes $x \in I$ gilt, dass $(x) \subset I$. Es sei $m \in \mathfrak{N}$ ein maximales Element und $x \in I$. Ist $I = 0$, so ist nichts zu zeigen. Wir können also annehmen, dass $x \neq 0$. Das Ideal $(x) + m$ ist endlich erzeugt und $(x) + m \subset I$. Damit ist $(x) + m$ aber in $\mathfrak{N}$ und die Maximalität von m besagt $(x) + m = m$. Dann ist $x \in m$ und somit ist jedes Element von I in m, so dass $I \subset m$. Es gilt nach Annahme $m \subset I$, also insgesamt $m = I$. Damit ist I endlich erzeugt.

Für (c) $\Rightarrow$ (a) betrachten wir eine aufsteigende Kette von Idealen $I_0 \subset I_1 \subset \dots$. Dann ist auch

$$\mathfrak{I} = \bigcup_{i \in \mathbb{N}_0} I_i$$

ein Ideal in R. Nach Annahme ist $\mathfrak{I} = (a_1, \dots, a_n)$ für $a_i \in R$. Es gibt also für jedes $1 \leqslant i \leqslant n$ ein $N(i)$ mit $a_i \in I_{N(i)}$. Wir setzen $N := \max\{N(i), 1 \leqslant i \leqslant n\}$. Damit ist $\mathfrak{I} = I_N$ und die Kette wird stationär. □

Korollar II.5.9. *Ist R ein Hauptidealring, so ist R faktoriell und noethersch.*

BEWEIS. Ist $I \subset R$ ein Ideal, so ist $I = (a)$, also insbesondere endlich erzeugt. Damit ist R noethersch. Wir wissen schon, dass jedes unzerlegbare Element auch prim ist. Ist $a \in R$, so gibt es ein maximales Ideal $\mathfrak{m}$ mit $(a) \subset \mathfrak{m}$. Aber $m = (p)$ für ein Primelement p. Also gilt $(a) \subset (p)$ und somit $a = pb$ für ein b. Die Iteration dieses Arguments gibt die Zerlegung von a in Primelemente, also in Unzerlegbare. □

Sie kennen euklidische Ringe aus der linearen Algebra. Sie wissen, dass diese Hauptidealringe sind, also gilt:

Korollar II.5.10. *Euklidische Ringe sind faktoriell und noethersch.*

Als Beispiele haben wir $\mathbb{Z}$, $K[X]$ für einen Körper K, $\mathbb{Z}[i]$, $\mathbb{Z}[\sqrt{2}]$ und viele mehr. Wir haben aber auch schon gesehen, dass $\mathbb{Z}[\sqrt{-5}]$ nicht faktoriell ist.

II.6. Lokalisierungen und Quotientenkörper

In diesem Abschnitt betrachten wir ausschließlich kommutative Ringe. Wir wollen aus einem Ring R Ringe konstruieren, die R enthalten, die aber mehr Einheiten besitzen als R. Im besten Fall möchten wir Ringe in Körper einbetten.

Definition II.6.1. Eine Teilmenge $S \subset R$ eines kommutativen Ringes R heißt *multiplikativ abgeschlossen*, falls gilt:

(a) $1_R \in S$,
(b) Mit $s, t \in S$ ist auch $st \in S$.

Beispiele II.6.2.

- In jedem kommutativen Ring sind $S = \{1_R\}$ und $S = R$ multiplikativ abgeschlossen.
- Ist R ein Integritätsbereich, so ist $S = R \setminus \{0_R\}$ multiplikativ abgeschlossen.
- In $\mathbb{Z}$ ist $S = \{p^r, r \in \mathbb{N}_0\}$ multiplikativ abgeschlossen für jede Primzahl p.
- In $\mathbb{Z}$ ist auch die Menge $S = \mathbb{Z} \setminus (p)$ multiplikativ abgeschlossen für jede Primzahl p.

Sie wissen, wie Sie $\mathbb{Q}$ aus $\mathbb{Z}$ konstruieren. Die allgemeine Form dieser Konstruktion ist die folgende:

Definition II.6.3. Es sei R ein kommutativer Ring und $S \subset R$ sei multiplikativ abgeschlossen. Die *Lokalisierung von R an S* ist ein Ring $R[S^{-1}]$.

Als Menge ist $R[S^{-1}] = R \times S/\sim$, wobei

$$(a, s) \sim (b, t) \Leftrightarrow \exists u \in S : (at - bs)u = 0.$$

Hierbei definiert $\sim$ eine Äquivalenzrelation auf $R \times S$ und wir bezeichnen die Äquivalenzklasse von (a, s) mit $[a, s]$.

Wir definieren

$$[a, s][b, t] := [ab, st] \text{ und } [a, s] + [b, t] := [at + sb, st].$$

Bemerkung II.6.4.

- Es gilt $(a, s) \sim (a, s)$, weil mit $u = 1$ gilt: $(as - sa)1_R = 0$. Gibt es $u, v \in S$ mit $(at - bs)u = 0$ und $(br - ct)v = 0$, also $(a, s) \sim (b, t)$ und $(b, t) \sim (c, r)$, so ist auch

  $$(ar - cs)tusvr = 0$$

  und $\sim$ ist transitiv. Die Relation ist sichtbar symmetrisch.
- Sie rechnen nach, dass die Multiplikation und die Addition auf $R[S^{-1}]$ wohldefiniert sind.
- Damit ist $R[S^{-1}]$ immer ein kommutativer Ring.
- Es kann aber vorkommen, dass $R[S^{-1}]$ der Nullring ist!

  $$(a, s) \sim (0, 1) \Leftrightarrow \exists t \in S : at = 0.$$

  Ist $0 \in S$, dann ist also insbesondere $R[S^{-1}] = 0$.
- Wir wollen R mit $R[S^{-1}]$ verbinden. Es sei $\varphi_S \colon R \to R[S^{-1}]$ der Ringhomomorphismus mit $\varphi(r) = [r, 1]$. Dann ist für alle $s \in S$

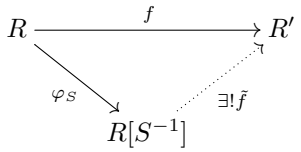
  $$[s, 1][1, s] = [s, s] \sim [1, 1] = 1_{R[S^{-1}]},$$

  also ist $\varphi_S(S) \subset R[S^{-1}]^\times$.
- Der Kern von φ_S ist

  $$\begin{aligned} \ker(\varphi_S) &= \{r \in R, [r, 1] = [0, 1]\} \\ &= \{r \in R, \exists s \in S : rs = 0\}. \end{aligned}$$

Satz II.6.5 (Universelle Eigenschaft von φ_S)**.** *Ist $f\colon R \to R'$ ein Ringhomomorphismus mit $f(s) \in (R')^\times$ für alle $s \in S$, so gibt es genau einen Ringhomomorphismus*

$$\tilde{f}\colon R[S^{-1}] \to R' \text{ mit } \tilde{f} \circ \varphi_S = f.$$



Beweis. Ist $\tilde{f} \circ \varphi_S = f$ ein Ringhomomorphismus, so ist für alle $r \in R$ und $s \in S$

$$\tilde{f}[r,1] = \tilde{f}(\varphi_S(r)) = f(r) \text{ und } \tilde{f}[1,s] = \tilde{f}([s,1]^{-1}) = \tilde{f}([s,1])^{-1} = f(s)^{-1}.$$

Dadurch ist $\tilde{f}$ auf beliebigen Elementen $[r,s] \in R[S^{-1}]$ festgelegt, weil $[r,s] = [r,1][1,s]$, also

$$\tilde{f}[r,s] = f(r)f(s)^{-1}.$$

Wir müssen also nur zeigen, dass dieses $\tilde{f}$ wohldefiniert ist. Ist also $(r,s) \sim (a,t)$, so gibt es ein $u \in S$ mit $(rt - as)u = 0$. Damit ist auch

$$0 = (f(r)f(t) - f(a)f(s))f(u).$$

Aber $f(u) \in (R')^\times$, so dass auch gilt

$$0 = f(r)f(t) - f(a)f(s) \Leftrightarrow f(r)f(t) = f(a)f(s) \Leftrightarrow f(r)f(s)^{-1} = f(a)f(t)^{-1}$$

und das ist gerade die Gleichung $\tilde{f}[r,s] = \tilde{f}[a,t]$. □

Definition II.6.6. Ist R ein Integritätsbereich, so heißt $R[(R\setminus\{0_R\})^{-1}]$ der *Quotientenkörper von R*, $\mathsf{Quot}(R)$.

Beispiel II.6.7. Für $R = \mathbb{Z}$ ist $\mathsf{Quot}(\mathbb{Z}) \cong \mathbb{Q}$, wobei $[r,s] \in \mathsf{Quot}(\mathbb{Z})$ dem Element $\frac{r}{s} \in \mathbb{Q}$ entspricht.

In Quotientenkörpern verwenden wir die Notation $\frac{r}{s}$ für $[r,s]$.

Definition II.6.8. Ist $\mathfrak{p} \subset R$ ein Primideal, so heißt $R[(R \setminus \mathfrak{p})^{-1}]$ die *Lokalisierung bezüglich* $\mathfrak{p}$.

Oft finden Sie auch *Lokalisierung an* $\mathfrak{p}$ oder *Lokalisierung weg von* $\mathfrak{p}$. Man benutzt die Notation $R_\mathfrak{p}$, also zum Beispiel $\mathbb{Z}_{(p)}$ für eine Primzahl p. Diese Ringe sind in der Zahlentheorie und der algebraischen Geometrie sehr wichtig und sie kommen häufig in der algebraischen Topologie vor.

Satz II.6.9. *Für ein Primideal $\mathfrak{p}$ eines kommutativen Ringes $R \neq 0$ hat $R_\mathfrak{p}$ ein einziges maximales Ideal*

$$\mathfrak{m}_\mathfrak{p} = \{[a,s] \in R_\mathfrak{p}, a \in \mathfrak{p}\}.$$

Beweis. Sie rechnen nach, dass $\mathfrak{m}_\mathfrak{p}$ ein Ideal ist.
Ist $x \in R_\mathfrak{p} \setminus \mathfrak{m}_\mathfrak{p}$ so ist $x = [a,s]$ mit $a \notin \mathfrak{p}$. Damit hat aber x das Inverse $[s,a]$ und somit sind alle Elemente außerhalb von $\mathfrak{m}_\mathfrak{p}$ invertierbar. Damit ist $\mathfrak{m}_\mathfrak{p}$ ein maximales Ideal und eindeutig. □

Bemerkung II.6.10.

- Für $\mathfrak{m}_\mathfrak{p}$ schreibt man auch oft $\mathfrak{p}R_\mathfrak{p}$.
- Kommutative Ringe mit nur einem einzigen maximalen Ideal heißen *lokale Ringe*.
- Es gibt Varianten der Lokalisierung für nicht-kommutative Ringe. Die sind aber komplizierter.

Vorlesung 19

II.7. Polynomringe

Vieles in diesem Abschnitt kennen Sie schon aus der linearen Algebra. Alle in diesem Abschnitt betrachteten Ringe sind wieder kommutativ.

Definition II.7.1. Für einen kommutativen Ring R sei der *Polynomring in einer Unbestimmten X*, $R[X]$, die Menge aller Abbildungen $f\colon \mathbb{N}_0 \to R$ mit der Eigenschaft, dass $f(n) = 0$ ist für fast alle $n \in \mathbb{N}_0$.

Das Nullpolynom ist die Funktion $0(n) = 0_R$ für alle $n \in \mathbb{N}_0$ und das Einselement ist

$$1(n) = \begin{cases} 1, & n = 0, \\ 0, & n \neq 0. \end{cases}$$

Für $f, g \in R[X]$ sei

$$(f+g)(n) = f(n) + g(n) \text{ und } (fg)(n) = \sum_{j=0}^{n} f(j)g(n-j) \text{ für } n \in \mathbb{N}_0.$$

Bemerkung II.7.2.

- $R[X]$ ist ein kommutativer Ring.
- Wie üblich identifizieren wir $f \in R[X]$ mit
$$\sum_{n\in\mathbb{N}_0} f(n)X^n.$$
- R ist ein Unterring von $R[X]$ vermittels der Abbildung $i\colon R \to R[X]$, die ein $r \in R$ auf $i_r(0) = r$ und $i_r(n) = 0$ für $n \neq 0$ schickt. In der alternativen Schreibweise entspricht dies dem konstanten Polynom mit konstantem Term r.
- $f(n) \in R$ heißt der $n$te Koeffizient des Polynoms f.

Sie kennen auch schon den Grad eines Polynoms:

Definition II.7.3.

(a) Ist $0 \neq f \in R[X]$ so heißt das größte $n \in \mathbb{N}_0$ mit $f(n) \neq 0$ der *Grad von f*, $\mathrm{Grad}(f)$ und $f(n)$ heißt dann der *Höchstkoeffizient von f*.
(b) Wir setzen $\mathrm{Grad}(0) = -\infty$.
(c) Ein $f \in R[X]$ heißt *normiert*, falls sein Höchstkoeffizient gleich 1_R ist.

Satz II.7.4. *Für den Grad gelten die Rechenregeln*

(a) $\mathrm{Grad}(f+g) \leqslant \max(\mathrm{Grad}(f), \mathrm{Grad}(g))$,
(b) $\mathrm{Grad}(fg) \leqslant \mathrm{Grad}(f) + \mathrm{Grad}(g)$.
(c) *Ist R ein Integritätsbereich, so gilt* $\mathrm{Grad}(fg) = \mathrm{Grad}(f) + \mathrm{Grad}(g)$.

Beweis. Für (a) rechnen Sie das direkt nach. Wir betrachten $n = \mathrm{Grad}(f)$ und $m = \mathrm{Grad}(g)$. Ohne Einschränkung sind $f, g \neq 0$, weil sonst die Behauptung in (b) sichtbar wahr ist. Dann ist

$$fg = \sum_{h\in\mathbb{N}_0} c_h X^h, \quad c_h = 0 \text{ für alle } h > n+m.$$

Ist $f = \sum_{i=0}^{n} a_i X^i$ und $g = \sum_{j=0}^{m} b_j X^j$ mit $a_n \neq 0 \neq b_m$, so ist $c_{n+m} = a_n b_m$. Das zeigt (b). Ist R ein Integritätsbereich, so ist auch $c_{n+m} \neq 0$, also gilt (c). □

Korollar II.7.5.

(a) *Der kommutative Ring R ist genau dann ein Integritätsbereich, wenn $R[X]$ es ist.*
(b) *In diesem Fall gilt $R[X]^\times = R^\times$.*

Beweis. Behauptung (a) folgt direkt daraus, wie R ein Unterring von $R[X]$ ist. Für (b) nehmen wir an, dass $fg = 1_{R[X]}$ gilt. Wir erhalten die Gleichung für den Grad

$$\mathrm{Grad}(fg) = \mathrm{Grad}(f) + \mathrm{Grad}(g) = \mathrm{Grad}(1_{R[X]}) = 0.$$

Dies geht nur, wenn $\mathrm{Grad}(f) = \mathrm{Grad}(g) = 0$ ist, und damit liegen f, g im Unterring $R \subset R[X]$ und sind dort invertierbar. □

Lemma II.7.6. *Ist $\varphi\colon R \to R'$ ein Ringhomomorphismus zwischen kommutativen Ringen und ist $a \in R'$. Dann gibt es genau einen Ringhomomorphismus*

$$\varphi_a\colon R[X] \to R' \text{ mit } \varphi_a(X) = a \text{ und } \varphi_a|_R = \varphi.$$

Beweis. Die Bedingungen legen φ_a eindeutig fest, so dass

$$\varphi_a\Big(\sum_{n\in\mathbb{N}_0} b_n X^n\Big) = \sum_{n\in\mathbb{N}_0} \varphi(b_n) a^n$$

mit $a^0 = 1$.. □

Ist $\varphi = \mathrm{id}_R$, so gibt es also für alle $a \in R$ die Abbildung $\varphi_a\colon R[X] \to R$, die ein Polynom $f \in R[X]$ auf die Auswertung des Polynoms an a, $f(a)$ abbildet.

Definition II.7.7. Ist $0 \neq f \in R[X]$ ein Polynom, so heißt ein $b \in R$ eine *Nullstelle von f*, falls $f(b) = 0_R$ ist.

Definition II.7.8. Es sei $R \subset R'$ ein Unterring, $i\colon R \to R'$ sei die Inklusion und $a \in R'$ sei fest gewählt. Dann gibt es nach Lemma II.7.6 einen Ringhomomorphismus $i_a\colon R[X] \to R'$ mit $i_a(X) = a$ und $i_a|_R = i$.

(a) Ist i_a injektiv, so heißt a *transzendent über R*.
(b) Ist $\ker(i_a) \neq \{0\}$, so heißt a *algebraisch über R*.

Bemerkung II.7.9.

- Das Bild von i_a besteht aus allen Elementen der Form
$$\sum_{n\in\mathbb{N}_0} b_n a^n \text{ mit } b_n = 0 \text{ für fast alle } n$$
und $\mathrm{Bild}(i_a)$ ist ein Unterring von R', der mit $R[a]$ bezeichnet wird.
- Ist i_a injektiv, so gilt $R[X] \cong R[a]$ und damit erfüllt das Element a keine algebraische Relation.
- Ist der Kern von i_a nicht-trivial, so gibt es $b_n \in R$ mit
$$\sum_{i=0}^{n} b_i a^i = 0$$
und somit ist a eine Nullstelle des zugehörigen Polynoms.

Den folgenden Satz kennen Sie aus der linearen Algebra. Wer sich noch gut daran erinnert, kann diesen Satz gerne überspringen.

Satz II.7.10. *Ist R ein Integritätsbereich, $0 \neq g \in R[X]$ und der Höchstkoeffizient von g sei invertierbar in R. Dann gibt es für alle $f \in R[X]$ eindeutige Polynome $q, r \in R[X]$ mit*

$$f = gq + r \text{ und } \mathrm{Grad}(r) < \mathrm{Grad}(g).$$

Beweis. Wir betrachten zunächst den Fall, dass $f = 0$ ist oder dass $f \neq 0$ aber $\mathrm{Grad}(f) < \mathrm{Grad}(g)$ ist. In diesem Fall setzen wir $q = 0$ und $r = f$.

Es sei also $f \neq 0$ und $M := \mathrm{Grad}(f) \geqslant \mathrm{Grad}(g) =: N$. Wir beweisen die Behauptung durch absteigende Induktion nach M. Für $M = N$ korrigiert q den Höchstkoeffizienten und r sammelt die abweichenden Anteile niedrigeren Grades auf.

Es sei also $M > N$ und wir schreiben $f = \sum_{i=0}^{M} a_i X^i$ und $g = \sum_{j=0}^{N} b_j X^j$ mit $a_M \neq 0 \neq b_N$. Nach Voraussetzung ist b_N invertierbar in R.

Wir definieren

$$h := f - a_M b_N^{-1} X^{M-N} g.$$

Nach Konstruktion ist der Koeffizient bei X^M für h gerade $a_M - a_M b_N^{-1} b_N = 0$ und damit ist der Grad von h echt kleiner als M. Nach Induktionsvoraussetzung gibt es also $q_0, r \in R[X]$ mit $\mathrm{Grad}(r) < N$ und $h = q_0 g + r$. Damit können wir auch f zerlegen:

$$f = h + a_M b_N^{-1} X^{M-N} g = (q_0 + a_M b_N^{-1} X^{M-N}) g + r$$

und wir setzen $q = q_0 + a_M b_N^{-1} X^{M-N}$. Das zeigt die Existenz der Zerlegung.

Zur Eindeutigkeit: Ist $f = qg + r = pg + s$, so dass $\mathrm{Grad}(r), \mathrm{Grad}(s) < \mathrm{Grad}(g)$ gilt, so ist

$$(q - p)g = s - r.$$

Es gilt aber $\mathrm{Grad}((q-p)g) = \mathrm{Grad}(q-p) + \mathrm{Grad}(g)$, während $\mathrm{Grad}(s-r) < \mathrm{Grad}(g)$ ist. Das geht nur, wenn $q - p = 0$ ist und damit ist auch $s - r = 0$, also sind $q = p$ und $r = s$. □

Korollar II.7.11. *Ist R ein Integritätsbereich und ist $0 \neq f \in R[X]$. Dann ist genau dann $b \in R$ eine Nullstelle von f, wenn $(X - b)$ ein Teiler von f ist.*

Beweis. Es ist $\mathrm{Grad}(X - b) = 1$ und der Höchstkoeffizient ist 1_R. Damit gibt es eindeutige $q, r \in R[X]$ mit $f = q(X - b) + r$ und $\mathrm{Grad}(r) < 1$. Da $f(b) = 0$ ist, ist auch $r(b) = 0$, somit muss $r = 0$ sein. □

Teilt $(X - b)^n$ ein Polynom f, aber $(X - b)^{n+1}$ teilt f nicht, dann heißt b auch eine *n-fache Nullstelle von f*.

Die Polynomdivision mit Rest wie in Satz II.7.10 ergibt, dass $K[X]$ ein eukidischer Ring ist, falls K ein Körper ist. Also erhalten wir:

Korollar II.7.12. *Ist K ein Körper, so ist $K[X]$ ein Hauptidealring und damit faktoriell und noethersch.*

Es gilt auch eine Umkehrung:

Satz II.7.13. *Ist $R[X]$ ein Hauptidealring, so ist R ein Körper.*

Beweis. Der Ring R ist ein Unterring von $R[X]$ und somit ein Integritätsbereich. Wir betrachten den Ringhomomorphismus

$$f_0 \colon R[X] \to R,\ f_0(X) = 0,\ f_0|_R = \mathrm{id},$$

das heißt f_0 wertet Polynome $g \in R[X]$ auf null aus:

$$f_0(g) = g(0).$$

Der Kern von f_0 ist ein Ideal in $R[X]$ und da R ein Integritätsbereich ist, ist $\ker(f_0)$ ein nichttriviales Primideal, also maximal. Damit ist $R[X]/\ker(f_0) \cong \mathrm{Bild}(f_0)$ ein Körper. Da f_0 surjektiv ist, ist also R ein Körper. □

Den folgenden Satz kennen Sie auch schon aus der linearen Algebra:

Satz II.7.14. *Ist R ein Integritätsbereich, so besitzt jedes $0 \neq f \in R[X]$ höchstens $\mathrm{Grad}(f)$ viele Nullstellen.*

Beweis. Wir beweisen die Behauptung durch Induktion über den Grad von f. Ist $\mathrm{Grad}(f) = 0$, so hat f gar keine Nullstellen.

Ist $\lambda \in R$ eine Nullstelle, so zerlegen wir f wie eben als $f = (X - \lambda)g$ mit $\mathrm{Grad}(g) = \mathrm{Grad}(f) - 1$. Nach Induktionsvoraussetzung hat g dann höchstens $\mathrm{Grad}(f) - 1$ viele Nullstellen und daher hat f höchstens $\mathrm{Grad}(f)$ viele Nullstellen. □

Es gilt das folgende wichtige Resultat:

Satz II.7.15 (Kleiner Fermat)**.** *Es sei p eine Primzahl. Für alle $a \in \mathbb{Z}$ gilt $\bar{a}^p = \bar{a} \in \mathbb{F}_p$.*

Beweis. Für $a = 0$ gilt natürlich $\bar{0}^p = \bar{0} \in \mathbb{F}_p$. Ist $\bar{a} \neq 0$, so ist $\bar{a} \in \mathbb{F}_p^\times$ und dies ist eine Gruppe der Ordnung $p - 1$. Also gilt $\bar{a}^{p-1} = \bar{1}$ und $\bar{a}^p = \bar{a} \in \mathbb{F}_p$. □

Vorlesung 20

Der Kleine Fermat besagt auch, dass das Polynom $f = \prod_{\bar{a} \in \mathbb{F}_p} (X - \bar{a})$ gleich dem Polynom $X^p - X$ ist. Beide haben jedes $\bar{a} \in \mathbb{F}_p$ als Nullstelle, aber $X^p - X$ hat Grad p, somit kann es nicht mehr Nullstellen haben und ist gleich f.

Wir erhalten damit das folgende wichtige Resultat:

Satz II.7.16. *Ist K ein Körper und ist $G < K \setminus \{0\}$ eine endliche Gruppe, so ist G zyklisch.*

Beweis. Die Gruppe G ist nach Voraussetzung abelsch und endlich. Es seien $p_1, \ldots, p_r$ die Primzahlen, die $|G|$ teilen und $S(p_i)$ sei die p_i-Sylowuntergruppe von G. (Es gibt jeweils eine eindeutige, weil G abelsch ist.) Ähnlich wie im Beweis des Klassifikationssatzes endlich erzeugter abelscher Gruppen (Satz I.11.24) folgern wir, dass G das direkte Produkt ihrer Sylowuntergruppen ist:

$$G = S(p_1) \times \ldots \times S(p_r).$$

Die $S(p_i)$ sind normal, weil G abelsch ist und es gilt $S(p_i) \cap S(p_j) = \{1_K\}$.

Nehmen wir an, es gibt ein i, so dass $S(p_i)$ nicht zyklisch ist. Damit gilt für alle $g \in S(p_i)$, dass die Ordnung von g, $\mathsf{ord}(g)$, echt kleiner ist als $|S(p_i)|$. Damit muss es eine p_i-Potenz q geben mit $q < |S(p_i)|$ und $g^q = 1_K$ für alle $g \in S(p_i)$. Aber das Polynom $X^q - 1$ hat höchstens q Nullstellen.

Damit sind alle Sylowuntergruppen von G zyklisch und

$$G = S(p_1) \times \ldots \times S(p_r) \cong \mathbb{Z}/p_1^{\ell_1}\mathbb{Z} \times \ldots \times \mathbb{Z}/p_r^{\ell_r}$$

und da die p_i paarweise teilerfremd sind, ist dies isomorph zur zyklischen Gruppe $\mathbb{Z}/(p_1^{\ell_1} \cdot \ldots \cdot p_r^{\ell_r})\mathbb{Z} = \mathbb{Z}/|G|\mathbb{Z}$. □

Bemerkung II.7.17. Wir können induktiv Polynomringe in mehreren Unbestimmten als

$$R[X_1, X_2] := (R[X_1])[X_2], \ldots, R[X_1, \ldots, X_n] := R[X_1, \ldots, X_{n-1}][X_n]$$

definieren. Elemente in $R[X_1, \ldots, X_n]$ können Sie schreiben als

$$\sum_{k_1,\ldots,k_n \geqslant 0} a_{k_1,\ldots,k_n} X_1^{k_1} \cdot \ldots \cdot X_n^{k_n},$$

wobei wiederum $a_{k_1,\ldots,k_n} \in R$ und $a_{k_1,\ldots,k_n} = 0$ für fast alle $k_1, \ldots, k_n$ gilt.

II.8. Irreduzible Polynome

Wir untersuchen, wann Polynomringe $R[X]$ faktoriell sind und behandeln ein Kriterium für die Irreduzibilität von Polynomen. Beachten Sie bitte, dass faktorielle Ringe immer Integritätbereiche sind.

Lemma II.8.1. *Es sei R ein Integritätsbereich und $a \in R$.*

(a) *Die kanonische Surjektion $\pi\colon R \to R/(a)$ induziert eine Surjektion*

$$\pi_*\colon R[X] \to (R/(a))[X]$$

und

$$R[X]/(a) \cong (R/(a))[X].$$

(b) *Ein $a \in R$ ist genau dann prim in R, wenn a prim in $R[X]$ ist.*

Beweis. Im Kern der Surjektion $R[X] \to (R/(a))[X]$ liegen die Polynome, deren Koeffizienten alle Vielfache von a sind. Sie bilden aber gerade das von a erzeugte Hauptideal in $R[X]$. Das zeigt (a).

Ein $a \in R$ ist genau dann in R prim, wenn $R/(a)$ ein Integritätbereich ist. Aber genau dann ist auch der Ring $(R/a)[X]$ ein Integritätsbereich, der nach (a) isomorph ist zu $R[X]/(a)$. Dies ist aber äquivalent dazu, dass a prim in $R[X]$ ist. □

Satz II.8.2. *Es sei $R \neq 0$ ein kommutativer Ring. Ist $R[X]$ faktoriell, so auch R.*

Beweis. Es sei $a \in R$, $a \neq 0$ und $a \notin R^\times$. Als Element im faktoriellen Ring $R[X]$ hat a eine eindeutige Zerlegung

$$a = \varepsilon p_1(X) \cdot \ldots \cdot p_r(X)$$

mit $\varepsilon \in R[X]^\times = R^\times$ und irreduziblen Polynomen $p_i \in R[X]$, die im faktoriellen Ring $R[X]$ auch prim sind. Diese Polynome haben dann alle Grad 0, also $p_i(X) = \pi_i \in R$.

Nach Lemma II.8.1 sind die π_i auch prim in R. Somit besitzt jedes $a \neq 0$ $a \in R$ eine Darstellung

$$a = \varepsilon \pi_1 \cdot \ldots \cdot \pi_r$$

mit $\varepsilon \in R^\times$ und Primelementen $\pi_i \in R$. Für jedes irreduzible Element a ist diese Zerlegung von der Form $a = \varepsilon\pi_1$. Mit π_1 ist dann aber auch a prim. Also ist R faktoriell. □

Um die Umkehrung zu zeigen, brauchen wir einige Vorbereitungen.

Definition II.8.3. Es sei R ein faktorieller Ring und $\pi \in R$ irreduzibel. Wir betrachten die Abbildung

$$\omega_\pi \colon R \to \mathbb{N}_0 \cup \{\infty\},$$

die definiert ist durch $\omega_\pi(0) = \infty$ und für $a \neq 0$ von der Form $a = \pi^e a'$ mit $\pi \nmid a'$ durch $\omega_\pi(a) = e$. Wir setzen sie auf $K = \mathsf{Quot}(R)$ fort durch

$$\omega_\pi \colon K \to \mathbb{Z} \cup \{\infty\}, \quad \frac{a}{b} \mapsto \omega_\pi(a) - \omega_\pi(b).$$

Die Abbildung ω_π heißt die *zum Primelement π gehörige Exponentialbewertung von K*.

Bemerkung II.8.4. Rechnen Sie bitte nach, dass für alle $x, y \in K$ gilt

$$\omega_\pi(xy) = \omega_\pi(x) + \omega_\pi(y),$$
$$\omega_\pi(x+y) \geqslant \min\left(\omega_\pi(x), \omega_\pi(y)\right).$$

Wir können ω_π auf den Polynomring $K[X]$ fortsetzen, indem wir definieren

$$\omega_\pi \colon K[X] \to \mathbb{Z} \cup \{\infty\}, \quad \omega_\pi\left(\sum_i a_i X^i\right) = \min_i\{\omega_\pi(a_i)\}.$$

Es gilt

$$\omega_\pi(cf) = \omega_\pi(c) + \omega_\pi(f) \tag{II.8.1}$$

für alle $c \in K$, $f \in K[X]$.

Lemma II.8.5. *Es sei R ein faktorieller Ring und $\pi \in R$ prim. Für je zwei Polynome $f, g \in K[X]$ gilt:*

$$\omega_\pi(gf) = \omega_\pi(g) + \omega_\pi(f).$$

Beweis. Indem wir einen Hauptnenner für die Koeffizienten des Polynoms bilden, finden wir für jedes $f \in K[X]$ ein $c \in R$, so dass $cf \in R[X]$. Wegen (II.8.1) reicht es daher aus, die Behauptung für $f, g \in R[X]$ zu zeigen.

Es sei nun $g = \pi^{\omega_\pi(g)} g_1$ und $f = \pi^{\omega_\pi(f)} f_1$ mit $\omega_\pi(g_1) = \omega_\pi(f_1) = 0$. Damit ist auch

$$gf = \pi^{\omega_\pi(g)} \pi^{\omega_\pi(f)} g_1 f_1 = \pi^{\omega_\pi(g)+\omega_\pi(f)} g_1 f_1$$

und

$$\omega_\pi(gf) = \omega_\pi(g) + \omega_\pi(f) + \omega_\pi(g_1 f_1).$$

Es bleibt somit zu zeigen, dass

$$\omega_\pi(g_1 f_1) = 0.$$

Wäre $\omega_\pi(g_1 f_1) > 0$, so teilt π $g_1 f_1$. Nach Lemma II.8.1 ist π auch prim im Polynomring, also müsste π f_1 oder g_1 teilen, so dass $\omega_\pi(g_1) > 0$ oder $\omega_\pi(f_1) > 0$ gelten müsste. □

Definition II.8.6.

(a) Es sei $f \in R[X]$, $f(X) = \sum_{i=0}^n a_i X^i$ mit $\mathrm{Grad}(f) \geqslant 1$. Dann heißt f *primitiv*, falls die Koeffizienten von f keinen echten gemeinsamen Teiler haben, also $\mathsf{ggT}(a_0, \ldots, a_n) = 1$.

(b) Es sei R faktoriell, $f \in R[X]$, $\mathrm{Grad}(f) \geqslant 1$. Dann gibt es eine Darstellung von f

$$f = ag, \text{ mit } a \in R \setminus \{0\}, g \in R[X] \text{ primitiv},$$

wobei a der ggT der Koeffizienten ist und damit bis auf Einheiten eindeutig. Das Hauptideal (a) heißt *Inhalt von f*.

Aus Lemma II.8.5 können Sie folgern, dass gilt

$$\mathsf{Inhalt}(gf) = \mathsf{Inhalt}(g) \cdot \mathsf{Inhalt}(f).$$

Lemma II.8.7. *Es sei R faktoriell, $K := \mathsf{Quot}(R)$ und $g \in R[X]$ mit $\mathrm{Grad}(g) \geqslant 1$. Ist g primitiv, so gilt: Ist g irreduzibel in $K[X]$, so auch in $R[X]$*

BEWEIS. Es sei $g \in R[X]$ irreduzibel in $K[X]$. Wir nehmen an, dass wir g schreiben können als $g = ab$ mit $a, b \in R[X] \subset K[X]$. Da g irreduzibel in $K[X]$ ist, ist einer der Faktoren, etwa a eine Einheit, $a \in K[X]^\times = K^\times$. Also liegt a in $K^\times \cap R[X] = R \setminus \{0\}$. Damit ist g genau dann in $R[X]$ irreduzibel, wenn man aus den Koeffizienten keinen gemeinsamen Faktor in R herausziehen kann, also wenn g primitiv ist. □

Beispiel II.8.8. Das Polynom $g(X) = 2X + 4$ ist irreduzibel in $\mathbb{Q}[X]$, nicht in aber in $\mathbb{Z}[X]$, da $g = 2(X+2)$ und 2 zwar eine Einheit in $\mathbb{Q}$, aber nicht in $\mathbb{Z}$ ist. Das Polynom ist allerdings auch nicht primitiv.

Satz II.8.9 (Satz von Gauß)**.** *Ist R faktoriell, so auch $R[X]$. Genauer gilt: Sei R faktoriell mit $\mathsf{Quot}(R) = K$ und ist $\mathfrak{P}_1$ (beziehungsweise $\mathfrak{P}_2$) ein Repräsentantensystem für die Klassen assoziierter Primelemente von R (beziehungsweise von $K[X]$, bestehend aus primitiven Polynomen in $R[X]$).*

Dann ist $R[X]$ faktoriell und $\mathfrak{P}_1 \cup \mathfrak{P}_2$ ist ein Repräsentantensystem der Klassen assoziierter Primelemente von $R[X]$.

BEWEIS. Der Ring $K[X]$ ist ein Hauptidealring und daher faktoriell. Jedes Primelement in $K[X]$ ist assoziiert zu einem primitiven Polynom in $R[X]$. Daher existieren die geforderten Repräsentantensysteme.

Wir wollen zeigen, dass ein beliebiges Element $g \in R[X]$ eindeutig als Produkt von Elementen in $\mathfrak{P}_1 \cup \mathfrak{P}_2$ und einer Einheit geschrieben werden kann. Dazu fassen wir g zunächst als Element des faktoriellen Rings $K[X]$ auf. Dort finden wir eine Zerlegung

$$g = a \prod_{f \in \mathfrak{P}_2} f^{e_f}$$

mit $a \in K^\times$ und $e_f \geqslant 0$, so dass fast alle e_f gleich 0 sind. Diese Zerlegung ist eindeutig in $K[X]$, weil dieser Ring faktoriell ist.

Für jedes $\pi \in \mathfrak{P}_1$ gilt nach Lemma II.8.5

$$0 \leqslant \omega_\pi(g) = \omega_\pi(a) + \sum_{f \in \mathfrak{P}_2} e_f \omega_\pi(f) = \omega_\pi(a),$$

weil alle f primitive Polynome in $R[X]$ sind.

Da somit $\omega_\pi(a) \geqslant 0$ für alle $\pi \in \mathfrak{P}_1$ ist, ist $a \in R$. Es sei also $a = \varepsilon \prod_{\pi \in \mathfrak{P}_1} \pi^{e_\pi}$ die Primfaktorzerlegung von a im faktoriellen Ring R mit $\varepsilon \in R^\times$, so dass die e_π fast alle 0 sind. Auch diese Zerlegung ist eindeutig. Insgesamt erhalten wir eine Zerlegung in irreduzible Faktoren

$$g = \varepsilon \prod_{\pi \in \mathfrak{P}_1} \pi^{e_\pi} \prod_{f \in \mathfrak{P}_2} f^{e_f}$$

in $R[X]$, weil π auch in $R[X]$ prim ist und f auch in $R[X]$ irreduzibel ist. Diese Zerlegung ist eindeutig, so dass $R[X]$ faktoriell ist. □

Korollar II.8.10. *Es sei R faktoriell, $K := \mathsf{Quot}(R)$ und $g \in R[X]$ mit $\mathrm{Grad}(g) \geq 1$. Ist g irreduzibel in $R[X]$, so ist es irreduzibel in $K[X]$.*

BEWEIS. Es sei g irreduzibel in $R[X]$. Nach dem Satz von Gauß schreibt sich $g = \varepsilon f$ mit $\varepsilon \in R^\times$ und $f \in \mathfrak{P}_2$. Damit ist aber g auch irreduzibel in $K[X]$. □

Vorlesung 21

Satz II.8.11 (Lemma von Gauß)**.** *Es sei R faktoriell, $K = \mathsf{Quot}(R)$ und $f \in R[X]$. Lässt sich f als Produkt von normierten Polynomen $g, h \in K[X]$ schreiben, $f = gh$, so liegen deren Koeffizienten schon in R, also $g, h \in R[X]$.*

BEWEIS. Der Beweis benutzt Bewertungen im faktoriellen Ring $R[X]$. Es sei $\pi \in R$ prim. Da $f \in R[X]$ liegt, ist $\omega_\pi(f) \geqslant 0$. Da g, h normierte Polynome sind, ist

$$\omega_\pi(g) \leqslant \omega_\pi(1) = 0,$$
$$\omega_\pi(h) \leqslant \omega_\pi(1) = 0.$$

Aus Lemma II.8.5 folgt $\omega_\pi(f) = \omega_\pi(g) + \omega_\pi(h)$. Damit ist aber $\omega_\pi(g) = \omega_\pi(h) = 0$ und $g, h \in R[X]$. □

Korollar II.8.12. *Es sei R faktoriell und $K = \mathsf{Quot}(R)$. Es sei $f = X^n + a_{n-1}X^{n-1} + \ldots + a_1X + a_0 \in R[X]$ ein normiertes Polynom und $\alpha \in K$ sei eine Nullstelle von f. Dann liegt $\alpha \in R$ und α teilt $a_0 = f(0)$.*

Beweis. Nach den Annahmen existiert in $K[X]$ die Zerlegung $f(X) = (X - \alpha)g(X)$ mit einem normierten Polynom $g(X) \in K[X]$. Nach dem Lemma von Gauß ist dann $X - \alpha \in R[X]$ und $g \in R[X]$. Damit liegt aber $\alpha \in R$. Ferner gilt $a_0 = f(0) = -\alpha g(0)$, also teilt α a_0. □

Dieser Satz besagt insbesondere, dass die Nullstellen normierter Polynome mit ganzen Koeffizienten entweder ganze Zahlen sind oder irrational. Sind sie ganz, so kommen auch nur die Teiler des Absolutkoeffizienten a_0 in Frage. Betrachtet man zum Beispiel das Polynom $f(X) = X^n - 2$ mit $n \geqslant 2$, so sieht man, dass alle n-ten Wurzeln aus 2 irrational sein müssen.

Wir wollen nun noch ein wichtiges Kriterium herleiten, mit dem wir irreduzible Polynome erkennen können. Dies ist zentral für die Galoistheorie. Zur Vorbereitung beweisen wir den folgenden Satz:

Satz II.8.13. *Es sei R ein Integritätsbereich und $\mathfrak{p} \subset R$ ein Primideal. Wir setzen die kanonische Projektion $R \to R/\mathfrak{p}$ zu einer Surjektion*

$$R[X] \to R/\mathfrak{p}[X]$$

fort. Es sei $f(X) = a_nX^n + \cdots + a_0 \in R[X]$ primitiv mit $\bar{a}_n \neq 0$ in $R/\mathfrak{p}$. Ist dann $\bar{f}$ irreduzibel in $R/\mathfrak{p}[X]$, so ist f auch irreduzibel in $R[X]$.

Bemerkung II.8.14. Die Umkehrung gilt nicht! Wir werden sehen, dass für jede Primzahl p $f(X) = X^2 - p \in \mathbb{Z}[X]$ irreduzibel ist, aber $\bar{f}(X) = X^2 = X \cdot X$ ist in $\mathbb{Z}/p\mathbb{Z}[X]$ reduzibel.

Beweis. Angenommen, wir finden eine Darstellung $f = gh$ mit $g, h \in R[X]$. Da f primitiv ist, kann man keinen Faktor in R aus f herausziehen. Also haben g und h Grad größer gleich 1.

Aus der Darstellung $\bar{f} = \bar{g}\bar{h}$ und der Tatsache, dass $\bar{a}_n \neq 0$ ist, folgt, dass

$$\mathrm{Grad}(\bar{g}) = \mathrm{Grad}(g) \geqslant 1 \text{ und } \mathrm{Grad}(\bar{h}) = \mathrm{Grad}(h) \geqslant 1.$$

Da $\mathfrak{p}$ prim ist, ist $R/\mathfrak{p}$ ein Integritätsbereich, also sind alle Einheiten Polynome vom Grad 0, also $R/\mathfrak{p}[X]^\times = R/\mathfrak{p}^\times$. Man hat somit einen Widerspruch zur Irreduzibilität von $\bar{f}$ in $R/\mathfrak{p}[X]$. □

Satz II.8.15 (Irreduzibilitätskriterium von Eisenstein)**.** *Es sei R ein Integritätsbereich und $f(X) = a_nX^n + \ldots + a_1X^1 + a_0 \in R[X]$ primitiv. Es sei $\pi \in R$ prim und es gelte*

(a) $\pi \nmid a_n$,
(b) $\pi \mid a_i$ *für* $0 \leqslant i \leqslant n-1$,
(c) $\pi^2 \nmid a_0$.

Dann ist f irreduzibel in $R[X]$. Ist R faktoriell, so ist f nach Korollar II.8.10 auch irreduzibel in $\mathsf{Quot}(R)[X]$.

Ein primitives Polynom mit den obigen Eigenschaften heißt *Eisensteinpolynom bezüglich $\pi \in R$.*

Beweis. Da π prim ist, ist $R/(\pi)$ ein Integritätsbereich. Wäre f reduzibel, so hätte man $f = gh$ mit $r = \mathrm{Grad}(g) \geqslant 1$ und $s = \mathrm{Grad}(h) \geqslant 1$, weil f primitiv ist. Dies hätte eine entsprechende Zerlegung in $R/(\pi)[X]$ der Form

$$\bar{f} = \bar{g}\bar{h}$$

zur Folge. Aus Bedingung (a) folgt $\mathrm{Grad}(\bar{g}) = r$ und $\mathrm{Grad}(\bar{h}) = s$ und aus Bedingung (b) können wir $\bar{f}$ berechnen als

$$\bar{f} = \bar{a}_nX^n.$$

Da $R/(\pi)$ Integritätsbereich ist, existiert der Quotientenkörper $K = \mathsf{Quot}(R/(\pi))$. Wir fassen $\bar{f}$ als Element des Rings $K[X]$ auf, der als Hauptidealring faktoriell ist. In diesem Ring sind die einzig möglichen Zerlegungen von $\bar{f}$ als $\bar{f} = \bar{g}\bar{h}$ von der Form

$$\bar{g} = \beta X^r, \quad \bar{h} = \gamma X^s \text{ mit } \beta, \gamma \in K, \text{ so dass } \beta\gamma = \bar{a}_n.$$

Da $r, s \geqslant 1$, ist $\bar{g}(0) = \bar{h}(0) = 0$.

Also teilt π sowohl $g(0)$ also auch $h(0)$, so dass π^2 das Produkt $g(0)h(0) = a_0$ teilt im Widerspruch zu Bedingung (c). □

Beispiel II.8.16. Es sei $a \in \mathbb{Z} \setminus \{\pm 1\}$ quadratfrei, das heißt für alle $p \in \mathbb{Z}$ prim gilt $p^2 \nmid a$. Dann ist $X^n - a \in \mathbb{Z}[X]$ nach dem Eisenstein-Kriterium irreduzibel.

Bemerkung II.8.17. Wir werden das Eisenstein-Kriterium vor allem auf normierte Polynome anwenden. Diese sind immer primitiv.

KAPITEL III

Galoistheorie

Vorlesung 22

Galoistheorie hat vielfältige Anwendungen, die von der Behandlung algebraischer Gleichungen bis hin zu geometrischen Problemen reichen. So kann man zum Beispiel mit der Hilfe der Galoistheorie zeigen, dass man nicht zu jedem Winkel Θ mit Zirkel und Lineal den Winkel $\Theta/3$ konstruieren kann (s. [**5**, F14, Seite 62]). In dieser Vorlesung behandeln wir nur einen kleinen Ausschnitt der Galoistheorie. Wer das vertiefen möchte, kann das zum Beispiel mit [**1, 4, 5, 6, 7**] tun.

III.1. Körpererweiterungen

Definition III.1.1.

(a) Es sei K ein Körper. Ein Körper L mit $K \subset L$ heißt eine *Körpererweiterung von* K.
(b) Ein Körper K' mit $K \subset K' \subset L$ heißt ein *Zwischenkörper von* K *und* L.
(c) Ist L eine Körpererweiterung von K, so ist L insbesondere ein K-Vektorraum. Die Dimension $\dim_K L$ heißt der *Grad der Körpererweiterung* und wird mit $[L : K]$ notiert.
(d) Ist $[L : K] < \infty$, so heißt $K \subset L$ *endlich*.

Beispiele III.1.2. Die Körpererweiterung $\mathbb{R} \subset \mathbb{C}$ hat $[\mathbb{C} : \mathbb{R}] = 2$, weil zum Beispiel $(1, i)$ eine geordnete Basis von $\mathbb{C}$ als $\mathbb{R}$-Vektorraum ist. Dagegen hat die Körpererweiterung $\mathbb{Q} \subset \mathbb{R}$ Grad $[\mathbb{R} : \mathbb{Q}] = \infty$.

Satz III.1.3. *Für Körpererweiterungen $K \subset K' \subset L$ gilt*

$$[L : K'][K' : K] = [L : K].$$

Beweis. Ist eine der beteiligten Körpererweiterungen unendlich-dimensional über K, so gilt die Gleichheit. Also sei

$$[L : K'] = n \text{ und } [K' : K] = m, \quad n, m < \infty.$$

Es sei $e_1, \ldots, e_n$ eine Basis von L über K' und $f_1, \ldots, f_m$ sei eine Basis von K' über K. Wir behaupten, dass dann

$$\mathcal{B} = (e_1 f_1, \ldots, e_1 f_m, e_2 f_1, \ldots, e_2 f_m, \ldots, e_n f_1, \ldots, e_n f_m)$$

eine Basis von L über K ist.

Ist $x \in L$ so können wir x schreiben als

$$x = \sum_{i=1}^{n} \lambda_i e_i \text{ mit } \lambda_i \in K'$$

und ebenso können wir jedes λ_i schreiben als $\lambda_i = \mu_{i1} f_1 + \ldots + \mu_{im} f_m$ mit $\mu_{ij} \in K$. Somit ist

$$x = \sum_{i,j} \mu_{ij} f_j e_i$$

und $\mathcal{B}$ ist ein Erzeugendensystem von L über K.

Ist $\sum_{i,j} \mu_{ij} f_j e_i = 0$, so muss $\sum_j \mu_{ij} f_j = 0$ gelten, weil $e_1, \ldots, e_n$ eine Basis ist. Dann ist aber auch jedes $\mu_{ij} = 0$, weil $f_1, \ldots, f_m$ eine Basis ist. Also ist $\mathcal{B}$ auch linear unabhängig. □

Definition III.1.4. Ist $K \subset L$ eine Körpererweiterung und ist $S \subset L$ eine Teilmenge, so setzen wir

$$K(S) := \bigcap_{\substack{K \subset K' \subset L \\ S \subset K'}} K'$$

und nennen $K(S)$ den *von S über K erzeugte Zwischenkörper*.

Ein Zwischenkörper $K \subset L' \subset L$ heißt *endlich erzeugt*, falls $L' = K(S)$ mit $|S| < \infty$.

Bemerkung III.1.5. Ist $S = \{s_1, \ldots, s_n\}$, so schreiben wir $K(s_1, \ldots, s_n)$ für $K(\{s_1, \ldots, s_n\})$.

Der Körper $K(S)$ ist wirklich ein Zwischenkörper von K und L und er ist der kleinste solche Zwischenkörper, der S enthält.

Wie sieht $K(S)$ aus? Ist $S = \{s_1, \ldots, s_n\}$, so enthält $K(S)$ alle polynomialen Ausdrücke

$$K[S] := \{f(s_1, \ldots, s_n), f \in K[X_1, \ldots, X_n]\}.$$

Aber $K(S)$ ist ein Körper, so dass alle nicht-trivialen Elemente $f(s_1, \ldots, s_n)$ invertierbar sind. Er ist der Quotientenkörper von $K[S]$:

$$K(S) = \mathsf{Quot}(K[S]).$$

Er besteht also aus allen

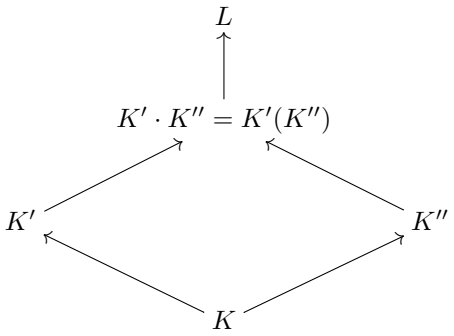
$$\frac{f(s_1, \ldots, s_n)}{g(s_1, \ldots, s_n)}$$

mit $f, g \in K[X_1, \ldots, X_n]$, $g(s_1, \ldots, s_n) \neq 0$.

Beispiel III.1.6. Es sei $S \subset \mathbb{R}$ die Menge $S = \{\sqrt{2}\}$. Dann ist $\mathbb{Q}(\sqrt{2})$ der kleinste Zwischenkörper $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{R}$ der $\sqrt{2}$ enthält. Da $\sqrt{2}^2 = 2 \in \mathbb{Q}$, aber $\sqrt{2} \notin \mathbb{Q}$, hat $\mathbb{Q}(\sqrt{2})$ die Basis $(1, \sqrt{2})$ über $\mathbb{Q}$ und es gilt

$$[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2.$$

Definition III.1.7. Sind K' und K'' Zwischenkörper von K und L, so sei $K' \cdot K'' := K'(K'')$. Dies heißt das *Kompositum von K' und K''*.



Bemerkung III.1.8. Überlegen Sie sich, dass gilt

$$K'(K'') = K''(K').$$

Statt nach Körpererweiterungen zu fragen, können wir umgekehrt fragen, welche Körper in einem gegebenen Körper enthalten sind. Was ist der kleinste Körper, der in einem Körper enthalten ist?

Definition III.1.9. Der kleinste Körper, der in einem Körper K enthalten ist, heißt *Primkörper von K*.

Ist K ein Körper, so haben wir die charakteristische Abbildung $\chi_K \colon \mathbb{Z} \to K$ mit $\chi_K(1) = 1_K$, also $\chi_K(n) = n \cdot 1_K$. Der Kern von χ_K ist ein Ideal in $\mathbb{Z}$, aber damit ist $\ker(\chi_K) = (n)$ für ein $n \in \mathbb{N}_0$, weil $\mathbb{Z}$ ein Hauptidealring ist. Wir wissen nach Beispiel II.2.11, dass $n = 0$ oder $n = p$ für eine Primzahl p sein muss.

Ist $n = p$ eine Primzahl, so gilt $\mathbb{Z}/p\mathbb{Z} \cong \text{Bild}(\chi_K) \subset K$, also ist $\mathbb{F}_p \subset K$.

Ist $n = 0$, so ist χ_K injektiv und $\mathbb{Z}$ ist ein Unterring von K. Damit ist aber $\mathbb{Q} = \mathsf{Quot}(\mathbb{Z})$ ein Teilkörper von K.

Definition III.1.10. Ist $K \subset L$ eine Körpererweiterung und ist $a \in L$, so heißt $K \subset K(a)$ eine *einfache Körpererweiterung von K*.

Wir hatten in Definition II.7.8 die Definition algebraischer und transzendenter Elemente kennengelernt. Zur Erinnerung sei $i\colon K \to L$ die Inklusion und $a \in L$. Dann gibt es genau einen Ringhomomorphismus $i_a\colon K[X] \to L$ mit $i_a|_K = i$ und $i_a(X) = a$. Ist i_a injektiv, so war a transzendent, andernfalls ist es algebraisch.

Ist i_a injektiv, so erhalten wir einen Isomorphismus $i_a\colon K[X] \to K[a] = K[\{a\}]$ und $K(a)$ ist isomorph zum Quotientenkörper

$$K(X) = \mathsf{Quot}(K[X]).$$

Damit gilt

$$[K(a) : K] = \infty,$$

weil die Elemente $a^n, n \in \mathbb{Z}$ linear unabhängig sind.

In $\mathbb{R}$ sind e und π transzendent über $\mathbb{Q}$. Die Beweise dafür sind aufwendig. Einen Beweis für die Transzendenz von π finden Sie zum Beispiel in [**5**, §17].

Ist dagegen a algebraisch, so gilt

$$0 \neq \ker(i_a) \subset K[X]$$

und damit ist $\ker(i_a) = (f)$ für ein $0 \neq f \in K[X]$. Wir können ohne Einschränkung annehmen, dass f normiert ist. Da $\ker(i_a)$ ein Primideal sein muss, ist f ein Primelement und daher irreduzibel in $K[X]$. Somit ist f das Polynom kleinsten Grades mit $f(a) = 0$ und den Eigenschaften normiert und nichttrivial zu sein.

Definition III.1.11. Ein solches f heißt das *Minimalpolynom von a über K* und wird mit $m_{a,K}$ notiert.

Wie kann man $m_{a,K}$ zu einem Minimalpolynom der linearen Algebra in Beziehung setzen?

Im Beweis des folgenden Satzes ist enthalten, wie man $K(a)$ durch $m_{a,K}$ beschreiben kann.

Satz III.1.12. *Ist a algebraisch über K und $[K(a) : K] = n$, dann bilden die Elemente $1, a, \dots, a^{n-1}$ eine Basis von $K(a)$ über K.*

Beweis. Der Ring $K[X]/(m_{a,K})$ ist ein Körper, weil $m_{a,K}$ nicht trivial und prim ist, so dass $(m_{a,K})$ maximal ist. Eine Basis als K-Vektorraum von $K[X]/(m_{a,K})$ besteht aus den Restklassen von $1, X, \dots, X^{n-1}$.

Wir wissen, dass $i_a\colon K[X] \to K[a]$ ein Epimorphismus mit $\ker(i_a) = (m_{a,K})$, so dass

$$\bar{i}_a\colon K[X]/(m_{a,K}) \cong K[a]$$

gilt. Damit ist aber $K[a] = K(a)$ und $\bar{i}_a(1) = 1, \bar{i}_a(X) = a, \dots, \bar{i}_a(X^{n-1}) = a^{n-1}$ eine Basis von $K(a)$. □

Definition III.1.13. Eine Körpererweiterung $K \subset L$ heißt *algebraisch*, falls jedes $a \in L$ algebraisch ist über K.

Satz III.1.14. *Jede endliche Körpererweiterung ist algebraisch.*

Beweis. Es sei $K \subset L$ endlich und $a \in L$. Dann ist $K \subset K(a)$ ebenfalls endlich, weil

$$[L : K(a)][K(a) : K] = [L : K].$$

Damit ist a nicht transzendent, weil sonst $[K(a) : K] = \infty$ wäre. □

Beispiel III.1.15. Ist $d \neq 1$, $d \in \mathbb{Z}$ eine quadratfreie Zahl, so ist $\mathbb{Q}(\sqrt{d})$ eine algebraische Erweiterung von $\mathbb{Q}$ und $[\mathbb{Q}(\sqrt{d}) : \mathbb{Q}] = 2$: Das Element $\sqrt{d}$ erfüllt die algebraische Gleichung $\sqrt{d}^2 = d \in \mathbb{Q}$, daher ist es algebraisch und $(1, \sqrt{d})$ ist eine Basis über $\mathbb{Q}$.

Satz III.1.16.

(a) *Ist eine Körpererweiterung $K \subset L$ algebraisch und endlich erzeugt, so ist $K \subset L$ endlich.*

(b) *Sind $K \subset L$ und $L \subset L'$ algebraisch, so auch $K \subset L'$.*

Beweis. Für (a) sei $L = K(a_1, \dots, a_n)$. Nach Annahme sind die a_i algebraisch über K, also ist $K(a_1)$ algebraisch über K, $K(a_1, a_2)$ ist algebraisch über $K(a_1)$ und schließlich ist $K(a_1, \dots, a_n)$ algebraisch über $K(a_1, \dots, a_{n-1})$. Für den Körpergrad gilt:

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

Da jeder Faktor endlich ist, ist es auch das Produkt.

Für (b) sei $a \in L'$ beliebig. Nach Voraussetzung ist a algebraisch über L, so dass es ein $0 \neq f \in L[X]$ gibt, also $f = a_0 + a_1 X + \ldots + a_n X^n$, und dass gilt $f(a) = 0$. Damit ist a algebraisch über $\tilde{L} = K(a_0, \ldots, a_n)$. Da die $a_i \in L$ sind, gilt $\tilde{L} \subset L$. Nach Konstruktion ist $\tilde{L}$ endlich erzeugt über K und mit (a) folgt dann dass $\tilde{L}$ endlich ist über K. Für den Körpergrad gilt

$$[\tilde{L}(a) : \tilde{L}][\tilde{L} : K] = [\tilde{L}(a) : K]$$

und daher ist $[\tilde{L}(a) : K]$ endlich, so dass a algebraisch ist über K. □

Vorlesung 23

Beispiele III.1.17.

- Ist $p \in \mathbb{N}$ prim, so ist $\sqrt[n]{p}$ irrational für alle $n \geqslant 2$ und $f = X^n - p$ ist irreduzibel in $\mathbb{Q}[X]$ nach Satz II.8.15. Also ist $m_{\sqrt[n]{p},\mathbb{Q}} = X^n - p$ und $[\mathbb{Q}(\sqrt[n]{p}) : \mathbb{Q}] = n$.
- Ist K ein Körper, so ist $K(X) = \mathsf{Quot}(K[X])$ eine Körpererweiterung von K. Diese ist endlich erzeugt aber nicht endlich, weil $X^n, n \in \mathbb{Z}$ linear unabhängig ist.

III.2. Algebraischer Abschluss

Das Folgende wissen wir schon. Ist K ein Körper und $f = \sum_{i=0}^{n} a_i X^i \in K[X]$ irreduzibel, dann gibt es einen Körper L, der algebraisch ist über K, so dass $[L : K] = \mathrm{Grad}(f)$ und so dass f in L eine Nullstelle hat. Sie setzen einfach $L = K[X]/(f)$ und

$$\alpha \colon K \to L = K[X]/(f), \quad \alpha(y) = y + (f).$$

Mit der kanonische Projektion $\pi \colon K[X] \to L = K[X]/(f)$ bekommen wir dann, dass $a = \pi(X)$ eine Nullstelle von f in L ist:

$$f(\pi(X)) = \sum_{i=0}^{n} a_i \pi(X)^i = \sum_{i=0}^{n} a_i (X + (f))^i \equiv \sum_{i=0}^{n} a_i X^i + (f) = f + (f) = 0 \in K[X]/(f).$$

Können wir einen Körper finden, so dass wir nicht jedes f einzeln behandeln müssen?

Definition III.2.1. Ein Körper K heißt *algebraisch abgeschlossen*, falls jedes $f \in K[X]$ mit $\mathrm{Grad}(f) > 0$ eine Nullstelle in K besitzt.

Sie wissen aus der linearen Algebra, dass $K = \mathbb{C}$ algebraisch abgeschlossen ist. Das war der *Fundamentalsatz der Algebra*, den wir allerdings nicht bewiesen haben.

Lemma III.2.2. *Die folgenden Aussagen sind äquivalent:*

(a) *Der Körper K ist algebraisch abgeschlossen.*
(b) *Jedes $f \in K[X]$ mit $\mathrm{Grad}(f) > 0$ ist Produkt von Polynomen in $K[X]$ vom Grad 1.*
(c) *Die normierten irreduziblen Polynome in $K[X]$ sind die Polynome $X - a$ für $a \in K$.*
(d) *Ist $K \subset L$ eine algebraische Körpererweiterung, so ist $K = L$.*

Beweis. Das sind einfache Umformulierungen. □

Satz III.2.3. *Ist K ein Körper, so gibt es einen algebraisch abgeschlossenen Körper L mit $K \subset L$.*

Beweis. Wir konstruieren zunächst eine Körpererweiterung $K \subset L_1$, so dass jedes $f \in K[X]$ mit $\mathrm{Grad}(f) \geqslant 1$ ein Nullstelle in L_1 hat. Dazu setzen wir

$$\mathcal{R} := K[X_f, f \in K[X] \setminus K].$$

Das ist ein Polynomring in unendlich vielen Variablen. In $\mathcal{R}$ betrachten wir das Ideal, welches von allen $f(X_f)$ erzeugt wird:

$$I := \langle f(X_f), f \in K[X] \setminus K \rangle.$$

Wir zeigen zunächst, dass $I \subsetneq \mathcal{R}$: Nehmen wir an, dass $I = \mathcal{R}$ ist, dann gibt es $f_i \in I$ und $g_i \in \mathcal{R}$ mit

$$1_{\mathcal{R}} = \sum_{i=1}^{n} g_i f_i(X_{f_i}).$$

Es sei h_i jeweils ein irreduzibler Faktor von f_i. Wir bilden

$$K[X]/(h_1) \subset (K[X]/(h_1))[X_2]/(h_2) \subset \ldots \subset L = K[X, X_2, \ldots, X_n]/(h_1, \ldots, h_n) =: L.$$

Jedes f_i hat nach Konstruktion eine Nullstelle $a_i \in L$.

Es sei $\varphi\colon \mathcal{R} \to L[X_f, f \in K[X] \setminus K]$ der Ringhomomorphismus, der festgelegt ist durch

$$\varphi|_K = \mathrm{id}_K, \varphi(X_{f_i}) = a_i, 1 \leqslant i \leqslant n, \varphi(X_f) = f \quad \forall \quad f \notin \{f_1, \ldots, f_n\}.$$

Dann gilt

$$\varphi(f_i(X_{f_i})) = f_i(\varphi(X_{f_i})) = f_i(a_i) = 0$$

und somit folgt

$$1 = \varphi(1_{\mathcal{R}}) = \varphi(\sum_{i=1}^{n} g_i f_i(X_{f_i})) = 0.$$

Wegen dieses Widerspruchs wissen wir jetzt, dass $\mathcal{R} \neq I$.

Zu $I \subsetneq \mathcal{R}$ gibt es ein maximales Ideal $\mathfrak{m}$ nach Satz II.3.4 mit $I \subset \mathfrak{m} \subset \mathcal{R}$. Wir setzen $L_1 = \mathcal{R}/\mathfrak{m}$. Die Verkettung von Abbildungen

$$K \longrightarrow K[X_f, f \in K[X] \setminus K] = \mathcal{R} \xrightarrow{\pi} \mathcal{R}/\mathfrak{m}$$

ist injektiv. Ist $f \in K[X] \setminus K$, $f = \sum_{i=1}^{N} \lambda_i X^i$ so gilt

$$f(\pi(X_f)) = \sum_{i=1}^{N} \lambda_i \pi(X_f)^i = \pi(\sum_{i=1}^{N} \lambda_i X_f^i) = \pi(f(X_f)) = 0,$$

weil $f(X_f) \in I \subset \mathfrak{m}$ und f hat also eine Nullstelle in L_1.

Wir konstruieren iterativ eine Kette von Körpererweiterungen

$$K = L_0 \subset L_1 \subset \ldots,$$

so dass jedes $g \in L_n[X] \setminus L_n$ eine Nullstelle in L_{n+1}.

Dann ist $L = \bigcup_{i \in \mathbb{N}_0} L_i$ ein Körper (rechnen Sie das bitte nach) und $K \subset L$. Nach Konstruktion ist jedes $g \in L[X] \setminus L$ ein Polynom in einem $L_n[X]$ und hat daher eine Nullstelle in $L_{n+1} \subset L$. Damit ist L algebraisch abgeschlossen. □

Definition III.2.4. Ist K ein Körper und ist $K \subset \overline{K}$ eine algebraische Körpererweiterung, so dass $\overline{K}$ algebraisch abgeschlossen ist, so heißt $\overline{K}$ der *algebraische Abschluss von K*.

Bemerkung III.2.5.

- Auch wenn man *der* algebraische Abschluss sagt, ist $\overline{K}$ nicht eindeutig. Manchmal sind wir vorsichtig und sagen daher *ein* algebraischer Abschluss.
- Ist L algebraisch über K, dann ist $\overline{L}$ auch ein algebraischer Abschluss von K. Zum Beispiel ist $\overline{\mathbb{Q}(i)}$ ein algebraischer Abschluss von $\mathbb{Q}$.

Beispiele III.2.6. Der Körper $\mathbb{C}$ ist ein algebraischer Abschluss von $\mathbb{R}$: $\mathbb{C}$ ist algebraisch über $\mathbb{R}$, weil $\mathbb{C} = \mathbb{R}(i)$ und $\mathbb{C}$ ist algebraisch abgeschlossen.

Vorsicht: Es ist $\mathbb{Q} \subset \overline{\mathbb{Q}} \subsetneq \mathbb{C}$, weil ja zum Beispiel $e, \pi \in \mathbb{R} \subset \mathbb{C}$ sind, aber beide Elemente sind nicht algebraisch über $\mathbb{Q}$.

Was ist $\overline{\mathbb{F}_p}$? Mit etwas mehr Hintergrund kann man diesen Körper sehr gut beschreiben.

III.3. Körperhomomorphismen

Wir betrachten jetzt passende Abbildungen zwischen Körpererweiterungen.

Definition III.3.1.

(a) Sind $K \subset L_1$ und $K \subset L_2$ Körpererweiterungen von K, so heißt ein Ringhomomorphismus $\varphi\colon L_1 \to L_2$ ein *K-Homomorphismus*, falls $\varphi(\lambda) = \lambda$ gilt für alle $\lambda \in K$.

(b) Ist φ zusätzlich bijektiv, so heißt φ ein K-Isomorphismus.

(c) Ist $L_1 = L_2 =: L$ und ist φ ein K-Isomorphismus, so heißt φ ein *K-Automorphismus von L* und wir notieren die Gruppe aller K-Automorphismus von L mit $\mathsf{Aut}_K(L)$.

Beispiel III.3.2. Die komplexe Konjugation $\varphi\colon \mathbb{C} \to \mathbb{C}$, $z \mapsto \overline{z}$ ist ein $\mathbb{R}$-Automorphismus von $\mathbb{C}$.

Bemerkung III.3.3.

(a) Ist $\varphi\colon L_1 \to L_2$ ein K-Homomorphismus, so ist φ insbesondere eine K-lineare Abbildung: Sind $\lambda, \mu \in K$ und $x, y \in L_1$, so gilt

$$\varphi(\lambda x + \mu y) = \varphi(\lambda)\varphi(x) + \varphi(\mu)\varphi(y)$$

und weil $\varphi(\lambda) = \lambda$ und $\varphi(\mu) = \mu$ gilt, ist dies gleich

$$\lambda\varphi(x) + \mu\varphi(y).$$

Damit haben wir den gesamten Apparat der linearen Algebra zur Verfügung.

(b) Nehmen wir an, dass $\varphi(x) = 0$ ist für ein $0 \neq x \in L_1$. Dann ist x invertierbar und wir erhalten den Widerspruch

$$0 = \varphi(x)\varphi(x)^{-1} = \varphi(1) = 1.$$

Also sind K-Homomorphismen immer injektiv.

(c) Ist $[L_1 : K] = [L_2 : K] < \infty$, so muss daher φ auch surjektiv sein.

Lemma III.3.4. *Es sei $\varphi\colon L_1 \to L_2$ ein K-Homomorphismus.*

(a) *Ein $a \in L_1$ ist genau dann eine Nullstelle von $f \in K[X]$, wenn $\varphi(a)$ eine Nullstelle von f ist.*

(b) *Ist a algebraisch über K, so auch $\varphi(a)$.*

(c) *Für das Minimalpolynom gilt: $m_{a,K} = m_{\varphi(a),K}$.*

Beweis. Ist $f = \sum_{i=0}^{n} a_i X^i \in K[X]$, so ist

$$f(\varphi(a)) = \sum_{i=0}^{n} a_i \varphi(a)^i = \varphi(\sum_{i=0}^{n} a_i a^i).$$

Damit folgt (a) und (a) impliziert (b). Für (c) erinnern wir uns daran, dass

$$(m_{a,K}) = \ker(i_a).$$

Wir rechnen nach:

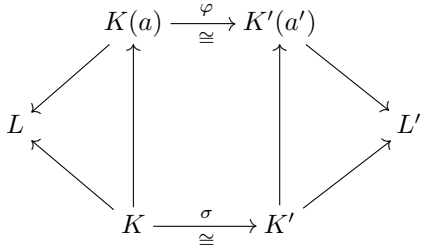
$$\begin{aligned} i_a(f) = 0 &\Leftrightarrow \sum_{i=0}^{n} a_i a^i = 0 \\ &\Leftrightarrow \sum_{i=0}^{n} a_i \varphi(a)^i = 0 \qquad \text{wegen (a)} \\ &\Leftrightarrow i_{\varphi(a)}(f) = 0 \end{aligned}$$

und dies zeigt die Behauptung. □

Satz III.3.5. *Es seien K und K' Körper und $\sigma\colon K \to K'$ sei ein Isomorphismus. Es sei $\sigma_*\colon K[X] \to K'[X]$ der von σ induzierte Isomorphismus gegeben durch $\sigma_*(\sum_{i=0}^{n} a_i X^i) = \sum_{i=0}^{n} \sigma(a_i) X^i$. Es seien $K \subset L$ und $K' \subset L'$ Körpererweiterungen. Dann gilt:*

(a) *Ist $a \in L$ und $a' \in L'$ mit $m_{a',K'} = \sigma_*(m_{a,K})$, so gibt es einen eindeutigen Isomorphismus $\varphi\colon K(a) \to K'(a')$ mit*

$$\varphi|_K = \sigma \text{ und } \varphi(a) = a'.$$



(b) *Für alle $a \in L$ ist die Anzahl der Homomorphismen $\varphi\colon K(a) \to L'$ mit $\varphi|_K = \sigma$ gleich der Anzahl der Nullstellen von $\sigma_*(m_{a,K})$ in L'.*

Beweis. Wir wissen, dass es Isomorphismen gibt

$$\xi\colon K[X]/(m_{a,K}) \to K(a), X + (m_{a,K}) \mapsto a$$

und

$$\xi'\colon K'[X]/(m_{a',K'}) \to K'(a'), X + (m_{a',K'}) \mapsto a'$$

und $m_{a',K'} = \sigma_*(m_{a,K})$ nach Voraussetzung. Daher induziert die Abbildung σ_* einen Isomorphismus

$$\overline{\sigma}_*\colon K[X]/(m_{a,K}) \to K'[X]/(m_{a',K'}) \text{ mit } \overline{\sigma}_*|_K = \sigma.$$

Wir setzen

$$\varphi := \xi' \circ \overline{\sigma}_* \circ \xi^{-1}.$$

$$\begin{array}{ccc} K[X]/(m_{a,K}) & \xrightarrow{\xi} & K(a) \\ \downarrow{\scriptstyle \overline{\sigma}_*} & & \vdots{\scriptstyle \varphi} \\ K'[X]/(m_{a',K'}) & \xrightarrow{\xi'} & K'(a') \end{array}$$

Dann ist die Einschränkung von φ auf K gleich σ und

$$\varphi(a) = \xi' \circ \overline{\sigma}_*(X + (m_{a,K})) = \xi'(X + (\sigma_*(m_{a,K}))) = \xi'(X + (m_{a',K'})) = a'.$$

Die Abbildung φ ist durch diese beiden Eigenschaften eindeutig festgelegt.

Für (b) ist mit (a) klar, dass für jede Nullstelle a' von $\sigma_*(m_{a,K})$ ein eindeutiges $\varphi\colon K(a) \to K'(a') \subset L'$ mit den gewünschten Eigenschaften gibt. Zu zeigen ist, dass jeder K-Homomorphismus $\varphi\colon K(a) \to L'$ mit $\varphi|_K = \sigma$ von dieser Form ist.

Ist $m_{a,K} = \sum_{i=0}^n \lambda_i X^i$, so gilt

$$\begin{aligned} \sigma_*(m_{a,K})(\varphi(a)) &= \sum_{i=0}^n \sigma(\lambda_i)\varphi(a)^i \\ &= \sum_{i=0}^n \varphi(\lambda_i)\varphi(a)^i \\ &= \varphi(m_{a,K}(a)) = \varphi(0) = 0. \end{aligned}$$

Also ist $\varphi(a)$ eine Nullstelle von $\sigma_*(m_{a,K})$ und damit von der Form wie in (a).

□

Korollar III.3.6. *Für $\sigma = \mathrm{id}_K\colon K \to K$ erhalten wir, dass es für $a, a' \in L$ mit $m_{a,K} = m_{a',K}$ genau einen K-Isomorphismus $\varphi\colon K(a) \to K(a')$ gibt mit $\varphi|_K = \mathrm{id}_K$ und $\varphi(a) = a'$.*

Vorlesung 24

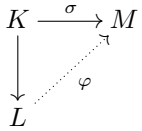
Beispiele III.3.7.

- Ist p eine Primzahl , so haben $\sqrt{p}$ und $-\sqrt{p}$ beide das Minimalpolynom
$$m_{\sqrt{p},\mathbb{Q}} = m_{-\sqrt{p},\mathbb{Q}} = X^2 - p$$
und der eindeutige $\mathbb{Q}$-Isomorphismus $\varphi\colon \mathbb{Q}(\sqrt{p}) \to \mathbb{Q}(-\sqrt{p})$ bildet $a + b\sqrt{p}$ auf $a - b\sqrt{p}$ ab.
- Für $\mathbb{Q}(i)$ ist $X^2 + 1$ Minimalpolynom für i und $-i$ und wir erhalten $\varphi\colon \mathbb{Q}(i) \to \mathbb{Q}(i)$:
$$\varphi(a + bi) = a - bi.$$

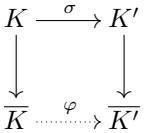
Wir können nun algebraische Abschlüsse vergleichen:

Satz III.3.8.

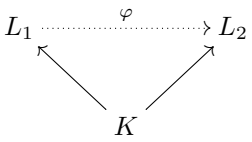
(a) *Ist $K \subset L$ eine algebraische Körpererweiterung, M ein algebraisch abgeschlossener Körper und $\sigma\colon K \to M$ sei ein Ringhomomorphismus. Dann gibt es einen Ringhomomorphismus $\varphi\colon L \to M$ mit $\varphi|_K = \sigma$.*



(b) *Ist $\sigma\colon K \to K'$ ein Isomorphismus zwischen Körpern, ist $\overline{K}$ ein algebraischer Abschluss von K und $\overline{K'}$ ein algebraischer Abschluss von K', so gibt es einen Isomorphismus $\varphi\colon \overline{K} \to \overline{K'}$ mit $\varphi|_K = \sigma$.*



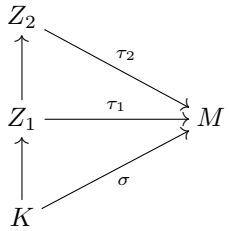
(c) *Sind L_1 und L_2 zwei algebraische Abschlüsse von K, so gibt es einen K-Isomorphismus $\varphi\colon L_1 \to L_2$.*



Beachten Sie, dass wir *nicht* behaupten, dass die Abbildungen φ eindeutig sind. Das werden sie auch nicht sein, ausser in trivialen Spezialfällen.

Beweis. Es ist klar, dass (b) die Aussage (c) impliziert, indem wir $\sigma = \mathrm{id}_K$ betrachten.
Für (a) brauchen wir Zorns Lemma: Wir betrachten
$$\mathfrak{Z} := \{(Z, \tau), K \subset Z \subset L, \tau\colon Z \to M, \tau_K = \sigma\},$$
wobei alle τ Abbildungen von Ringen sind.

Die Menge $\mathfrak{Z}$ ist nicht leer, weil $(K, \sigma) \in \mathfrak{Z}$ ist. Wir definieren eine partielle Ordnung auf $\mathfrak{Z}$ durch
$$(Z_1, \tau_1) \leqslant (Z_2, \tau_2) \Leftrightarrow Z_1 \subset Z_2 \text{ und } \tau_2|_{Z_1} = \tau_1.$$



Dann hat jede total geordnete Teilmenge von $\mathfrak{Z}$ eine obere Schranke und wir erhalten mit Zorns Lemma, dass $\mathfrak{Z}$ ein maximales Element (Z_∞, τ_∞) besitzt.

Wir behaupten, dass $Z_\infty = L$ ist. Nehmen wir an $Z_\infty \subsetneq L$. Dann gibt es also ein $a \in L \setminus Z_\infty$ mit einem Minimalpolynom m_{a,Z_∞}. Da M algebraisch abgeschlossen ist, hat $(\tau_\infty)_*(m_{a,Z_\infty})$ eine Nullstelle $a' \in M$.

Damit gibt es ein $\psi\colon Z_\infty(a) \to M$ mit $\psi|_{Z_\infty} = \tau_\infty$ und $\psi(a) = a'$. Das ist ein Widerspruch zur Maximalität von Z_∞, weil dann gilt

$$Z_\infty \subsetneq Z_\infty(a) \in \mathfrak{Z}.$$

Somit ist (Z_∞, τ_∞) das gesuchte Paar (L, φ).

Für (b) wissen wir nach (a), dass es einen Homomorphismus $\varphi\colon \overline{K} \to \overline{K'}$ gibt mit $\varphi|_K = \sigma$. Das Bild von φ ist ein algebraisch abgeschlossener Körper, weil φ injektiv ist. Außerdem ist $\overline{K'}$ algebraisch abgeschlossen über

$$K' = \sigma(K) = \varphi(K) \subset \varphi(\overline{K}) \subset \overline{K'}$$

und somit ist $\overline{K'}$ algebraisch abgeschlossen über $\varphi(\overline{K})$. Daher ist $\varphi(\overline{K}) = \overline{K'}$ und φ ist ein Isomorphismus. □

III.4. Zerfällungskörper

Definition III.4.1. Es sei K ein Körper. Ist $f \in K[X]$ mit $\mathrm{Grad}(f) = m \geqslant 1$, so heißt ein Körper $K \subset L$ ein *Zerfällungskörper von f über K*, falls gilt: Es gibt $a_1, \ldots, a_m \in L$ und ein $c \in K$, so dass

(a) $f = c\prod_{i=1}^m (X - a_i)$
(b) $L = K(a_1, \ldots, a_m)$.

Bemerkung III.4.2. Ist ein solches f gegeben und ist $K \subset \overline{K}$ ein algebraischer Abschluss von K, so zerfällt f über $\overline{K}$ in Linearfaktoren. Es gibt also $a_i \in \overline{K}$, so dass

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

Damit ist dann $L = K(a_1, \ldots, a_m)$ ein Zerfällungskörper von f über K. Ist umgekehrt L ein Zerfällungskörper von f über K, so haben wir $K \subset L \subset \overline{L}$ und damit ist $\overline{L}$ ein algebraischer Abschluss von K.

Wir erhalten die Eindeutigkeit von Zerfällungskörpern wieder bis auf Isomorphie:

Satz III.4.3. *Es sei $\sigma\colon K \to K'$ ein Isomorphismus von Körpern und $f \in K[X]\backslash K$. Ist L ein Zerfällungskörper von f über K und L' ein Zerfällungskörper von $\sigma_*(f)$ über K', dann gibt es einen Isomorphismus $\varphi\colon L \to L'$ mit $\varphi|_K = \sigma$. Jeder solche Isomorphismus bildet die Menge der Nullstellen von f in L auf die Menge der Nullstellen von $\sigma_*(f)$ in L' ab.*

Ist also $f = c\prod_{i=1}^m (X - a_i)$ über L, so ist $\sigma_*(f) = c'\prod_{i=1}^m (X - a_i')$ und für jedes i ist $\varphi(a_i) = a_j'$ für ein j.

Indem wir $\sigma = \mathrm{id}_K$ betrachten, erhalten wir aus Satz III.4.3, dass je zwei Zerfällungskörper von f über K zueinander isomorph sind.

Beweis. Wir betrachten wiederum die algebraischen Abschlüsse

$$\begin{array}{ccc} \overline{K} & & \overline{K'} \\ \uparrow & & \uparrow \\ K & \xrightarrow{\sigma} & K' \end{array}$$

und erhalten mit Satz III.3.8 (b) einen Isomorphismus $\psi\colon \overline{K} \to \overline{K'}$ mit $\psi|_K = \sigma$. Es gibt ein $c \in K$ und $a_1, \ldots, a_m \in \overline{K}$, so dass $f = c\prod_{i=1}^m (X - a_i)$ also ist $L = K(a_1, \ldots, a_m)$. Es gilt

$$\sigma_*(f) = \psi_*(f) = \sigma(c)\prod_{i=1}^m (X - \psi(a_i))$$

und somit sind die $\psi(a_i)$ die Nullstellen von $\sigma_*(f)$ in $\overline{K'}$. Daraus folgt, dass

$$L' := K'(\psi(a_1), \ldots, \psi(a_m)) = \psi(K(a_1, \ldots, a_m)) = \psi(L)$$

ist und $\varphi = \psi|_L$ erfüllt die Behauptung. □

Bemerkung III.4.4. Ähnlich wie beim algebraischen Abschluss sagt man auch oft, *der* Zerfällungskörper, obwohl dieser nicht eindeutig ist, sondern nur eindeutig bis auf Isomorphismus. Vorsicht: Aus einem Zerfällungskörper kann das Polynom nicht rekonstruieren: Der Körper $\mathbb{C}$ ist zum Beispiel Zerfällungskörper von X^2+1 aber auch von $(X-(1+i))(X-(1-i)) = X^2-2X+2$.

Definition III.4.5. Ist $F \subset K[X] \setminus K$, so heißt L *Zerfällungskörper von F über K*, falls alle $f \in F$ über L in Linearfaktoren zerfallen und falls es kein $K \subsetneq L' \subsetneq L$ gibt, der dies leistet.

Satz III.4.6. *Es sei $F \subset K[X] \setminus K$.*

(a) *Zu einem algebraischen Abschluss $K \subset \overline{K}$ gibt es genau einen Zerfällungskörper von F über K, der in $\overline{K}$ enthalten ist.*
(b) *Sind L, L' Zerfällungskörper von F über K, so sind L und L' K-isomorph.*

Beweis. Zu (a) setzen wir S an als die Menge aller Nullstellen in $\overline{K}$ der Polynome in F. Dann ist $L := K(S)$ der gesuchte Zerfällungskörper.

Wir betrachten für (b) die algebraischen Abschlüsse $\overline{L} \supset L \supset K \subset L' \subset \overline{L'}$ der beiden Zerfällungskörper von F über K. Dann sind $\overline{L}$ und $\overline{L'}$ beides algebraische Abschlüsse von K und wir finden eine K-Isomorphismus $\psi\colon \overline{L} \to \overline{L'}$. Wir wissen, dass $L = K(S)$ und $L' = K(S')$, wobei S die Menge der Nullstellen von F in $\overline{L}$ und S' die Menge der Nullstellen von F in $\overline{L'}$ ist. Wie im Beweis von Satz III.4.3 folgern wir, dass $\psi(S) = S'$ ist und $L' = \psi(L)$, so dass $\psi|_L$ der gesuchte K-Isomorphismus ist. □

Definition III.4.7. Eine Körpererweiterung $K \subset L$ heißt *normal*, wenn es eine Menge $F \subset K[X] \setminus K$ gibt, so dass L der Zerfällungskörper von F über K ist.

Beispiele III.4.8.
- $\mathbb{R} \subset \mathbb{C}$ ist normal.
- Sie überlegen sich, dass $\mathbb{F}_7 \subset \mathbb{F}_7[X]/X^3-2$ normal ist.
- Ist $K \subset L$ eine Körpererweiterung mit $[L:K] = 2$, so ist $K \subset L$ immer normal. Warum?

Vorlesung 25

Satz III.4.9. *Ist $K \subset \overline{K}$ ein algebraischer Abschluss, so sind für $K \subset L \subset \overline{K}$ äquivalent:*

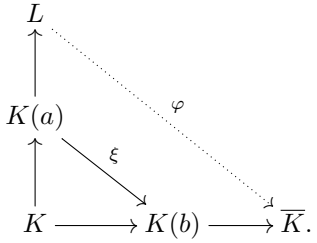
(a) *Jedes irreduzible $f \in K[X] \setminus K$, das in L eine Nullstelle hat, zerfällt über L in Linearfaktoren.*
(b) *$K \subset L$ ist normal.*
(c) *Ist $\varphi\colon L \to \overline{L}$ ein K-Homomorphismus, so ist $\varphi(L) = L$.*

Bemerkung III.4.10. Kriterium (a) finden Sie in der Literatur auch oft als die Definition der Normalität. Kriterium (c) ist häufig nützlich, um Normalität in Beispielen nachzuweisen.

Beweis. Für (b) ⇒ (c) sei $F \subset K[X] \setminus K$ gegeben, so dass L der Zerfällungskörper von F über K ist. Damit können wir L schreiben als $K(S)$, wobei S die Menge der Nullstellen aller $f \in F$ sind. Ist $\varphi\colon L \to \overline{K}$ ein K-Homomorphismus, so ist $\varphi_*(f) = f$ für alle $f \in F$. Ist $f = c\prod_{i=1}^m (X-a_i)$, so ist $f = \varphi_*(f) = c\prod_{i=1}^m (X-\varphi(a_i))$ und damit ist a_i genau dann Nullstelle, wenn $\varphi(a_i)$ es ist und insgesamt erhalten wir $\varphi(S) = S$, so dass

$$\varphi(L) = \varphi(K(S)) = K(S) = L.$$

Für (c) ⇒ (b) sei $a \in L$ und $m_{a,K}$ sei das Minimalpolynom von a über K. Es sei $b \in \overline{K}$ eine Nullstelle von $m_{a,K}$. Dann gibt es einen K-Isomorphismus $\xi\colon K(a) \to K(b)$ mit $\xi(a) = b$. Betrachte



Nach Satz III.3.5 gibt es eine Fortsetzung $\varphi\colon L \to \overline{K}$ von ξ. Nach Voraussetzung in (c) gilt $\varphi(L) = L$ und somit ist $b = \xi(a) = \varphi(a) \in L$. Daher zerfällt $m_{a,K}$ über L in Linearfaktoren und $K \subset L$ ist Zerfällungskörper von $F = \{m_{a,K}, a \in L\}$.

Für (c) $\Rightarrow$ (a) betrachten wir eine Nullstelle $a \in L$ eines irreduziblen Polynoms $f \in K[X] \setminus K$. Dann ist f bis auf einen konstanten Faktor gleich dem Minimalpolynom $m_{a,K}$ und die Behauptung folgt wie bei (c) $\Rightarrow$ (b).

Für (a) $\Rightarrow$ (c) sei $a \in L$ beliebig. Dann ist $m_{a,K}$ irreduzibel mit Nullstelle a und nach Annahme zerfällt $m_{a,K}$ über L in Linearfaktoren, also

$$m_{a,K} = c\prod_{i=1}^{m}(X - a_i) \text{ mit } a_i \in L, \text{ falls Grad}(m_{a,K}) = m$$

Ist $\varphi\colon L \to \overline{K}$ ein K-Isomorphismus, so ist $\varphi_*(m_{a,K}) = m_{a,K}$ und wiederum gilt

$$\{a_1, \ldots, a_m\} = \{\varphi(a_1), \ldots, \varphi(a_m)\}.$$

Also ist für jedes $a \in L$ auch $\varphi(a) \in L$. Umgekehrt gibt es einen Index i, so dass $\varphi(a_i) = a$, also ist $a \in \varphi(L)$, so dass insgesamt $\varphi(L) = L$ gilt.

□

Beispiel III.4.11. Die Körpererweiterung $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2})$ ist *nicht* normal: Das Minimalpolynom ist $m_{\sqrt[3]{2},\mathbb{Q}} = X^3 - 2$ aber

$$X^3 - 2 = (X - \sqrt[3]{2})(X - \sqrt[3]{2}\zeta_3)(X - \sqrt[3]{2}\zeta_3^2),$$

wobei ζ_3 eine dritte Einheitswurzel ist. Damit zerfällt $X^3 - 2$ in $\mathbb{Q}(\sqrt[3]{2}, \zeta_3) \subset \mathbb{C}$, aber nicht in $\mathbb{Q}(\sqrt[3]{2})$.

Satz III.4.12. *Ist $K \subset L$ normal und sind $a, b \in L$, so gibt es genau dann ein $\sigma \in \mathsf{Aut}_K(L)$ mit $\sigma(a) = b$, wenn $m_{a,K} = m_{b,K}$.*

Beweis. Ist $m_{a,K} = m_{b,K}$, so gibt es einen K-Isomorphismus $\varphi\colon K(a) \to K(b)$ mit $\varphi(a) = b$ und es gibt eine Fortsetzung $\sigma\colon L \to \overline{K}$ von φ. Nach Satz III.4.9 ist $\sigma(L) = L$, so dass $\sigma \in \mathsf{Aut}_K(L)$.

Ist umgekehrt $\sigma \in \mathsf{Aut}_K(L)$ mit $\sigma(a) = b$, so ist $\sigma(f(a)) = f(b)$ für alle $f \in K[X]$. Insbesondere ist b Nullstelle von $m_{a,K}$ und $m_{a,K} = m_{b,K}$. □

Normalität von Körpererweiterungen vererbt sich auf Zwischenkörper in der folgenden Weise.

Satz III.4.13. *Ist $K \subset L$ normal und ist $K \subset M \subset L$ ein Zwischenkörper, so ist $M \subset L$ normal.*

Beweis. Es ist $L = K(S)$, wobei S eine Menge von Nullstellen von $F \subset K[X] \setminus K$ ist. Da $S \subset L$ gilt und $M \subset L$ ist auch $L = M(S)$. □

Sie haben in Beispiel III.4.11 gesehen, dass in der obigen Situation $K \subset M$ nicht normal sein muss.

Wir hatten in Definition III.1.7 das Kompositum zweier Körper kennengelernt.

Satz III.4.14. *Ist $K \subset L$ normal und ist $K \subset M$ eine Körpererweiterung, so ist $M \subset L \cdot M$ normal.*

$$\begin{array}{ccc} L & \longrightarrow & L \cdot M \\ \uparrow & & \uparrow \\ K & \longrightarrow & M \end{array}$$

Beweis. Wir wissen $L = K(S)$ für ein geeignetes $S \subset \overline{K}$. Also ist $S \subset L$ und $K \subset M$, so dass

$$M(L) = M(K(S)) = M(S)$$

und damit ist $L \cdot M = M(L) = M(S)$. □

Beispiel III.4.15. Es sei $f = X^4 - 2 \in \mathbb{Q}[X]$. Dann ist $\mathbb{Q} \subset \mathbb{Q}(\sqrt[4]{2}) = \mathbb{Q}[X]/(X^4 - 2)$ nicht normal, aber $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2})$ und $\mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt[4]{2})$ sind normal, weil der Körpergrad jeweils 2 ist. Normalität ist also *keine* transitive Eigenschaft. Aber $\mathbb{Q} \subset \mathbb{Q}(\sqrt[4]{2}, i)$ ist normal.

Der letzte Schritt funktioniert immer:

Satz III.4.16. *Ist $K \subset L$ eine endliche Körpererweiterung, so gibt es ein $L \subset N$, so dass $K \subset N$ eine endliche normale Körpererweiterung ist.*

BEWEIS. Wir wissen $L = K(a_1, \ldots, a_m)$ für geeignete $a_i \in L$. Es sei $m_{a_i,K}$ das Minimalpolynom von a_i über K. Wir setzen $f = \prod_{i=1}^{m} m_{a_i,K}$. Dies ist ein Polynom in $K[X] \setminus K$ und wir betrachten seinen Zerfällungskörper N. Also ist $K \subset N$ normal, der Grad $[N : K]$ ist endlich und $L \subset N$ gilt nach Konstruktion. □

III.5. Separabilität

Separabilität sorgt für Wohlverhalten von Körpererweiterungen in endlicher Charakteristik. Zur Wiederholung:

Definition III.5.1. Es sei K ein Körper und $f \in K[X]$. Eine Nullstelle a von f hat *Vielfachheit* m, falls $(X-a)^m$ f teilt, aber $(X-a)^{m+1}$ teilt f nicht. Ist $m > 1$, so heißt a eine *mehrfache Nullstelle*.

Definition III.5.2.

(a) Es sei K ein Körper und $f \in K[X]$ sei irreduzibel. Dann heißt f *separabel über* K, falls f keine mehrfache Nullstelle in L hat für jeden Zerfällungskörper L von f über K.

(b) Ein beliebiges $f \in K[X] \setminus K$ heißt *separabel*, falls jeder seiner irreduziblen Faktoren separabel über K ist.

Beispiele III.5.3.

- Das Polynom $(X-1)^q$ ist reduzibel für $q > 1$ und $X - 1$ ist irreduzibel und immer separabel.
- $X^2 - 2$ ist separabel über $\mathbb{Q}$.
- Ist die Charakteristik des Körpers K gleich p mit p prim, so betrachten wir $f = X^p - a \in K[X]$. Ist a keine p-te Wurzel in K, so ist f irreduzibel. Ist L ein Zerfällungskörper von f, so gibt es ein $b \in L$ mit $b^p = a$ und wegen der binomischen Formel in Charakteristik p gilt

$$f = X^p - a = X^p - b^p = (X-b)^p.$$

Somit ist f also nicht separabel.

Wir wollen ein einfach nachzurechnendes Kriterium für Separabilität. Zunächst halten wir fest:

Lemma III.5.4. *Es seien $f, g \in K[X]$ und K sei ein Körper.*

(a) *Hat f keine mehrfachen Nullstellen in einem beliebigen Zerfällungskörper L von f über K, so ist f separabel über K.*

(b) *Teilt g f und ist f separabel über K, so ist g separabel über K.*

(c) *Sind $f_1, \ldots, f_n$ separabel über K, so auch $f_1 \cdot \ldots \cdot f_n$.*

(d) *Ist f separabel über K und ist $K \subset K'$ eine Körpererweiterung, so ist f separabel über K'.*

□

Hilfreich zum Studium der Separabilität ist das folgende Konzept.

Definition III.5.5. Ist $f = a_n X^n + a_{n-1} X^{n-1} + \ldots + a_1 X + a_0 \in K[X]$, so ist die *formale Ableitung von f*

$$f' = n a_n X^{n-1} + (n-1) a_{n-1} X^{n-2} + \ldots + a_1.$$

Bemerkung III.5.6. Machen Sie sich bitte klar, dass die Abbilung $f \mapsto f'$ eine K-lineare Abbildung ist und dass die Leibnizregel gilt: $(fg)' = f'g + f(g')$.

Vorsicht: In anderen Aspekten verhält sich die formale Ableitung anders, als Sie das von der gewöhnlichen Ableitung gewöhnt sind: Ist $X^p - a \in \mathbb{F}_p[X]$ für p prim und $a \in \mathbb{F}_p$ beliebig, so ist

$$(X^p - a)' = p X^{p-1} = 0.$$

Satz III.5.7. *Ist $f \in K[X] \setminus K$, so hat f genau dann keine mehrfache Nullstellen in einem beliebigen Zerfällungskörper L von f über K, wenn* $\mathsf{ggT}(f, f') = 1$.

BEWEIS. Wir zeigen erst, dass gilt

$$\mathsf{ggT}(f,f') = 1 \in K[X] \Leftrightarrow \mathsf{ggT}(f,f') = 1 \in L[X].$$

Ist $\mathsf{ggT}(f,f') = 1 \in K[X]$, so gibt es $g_1, g_2 \in K[X]$ mit $fg_1 + f'g_2 = 1$. Diese Gleichung gilt dann auch in $L[X]$.

Ist umgekehrt $\mathsf{ggT}(f,f') = 1 \in L[X]$ und ist $\mathsf{ggT}(f,f') = g \in K[X]$, dann gilt wegen $K[X] \subset L[X]$, dass g die 1 in $L[X]$ teilt, aber die einzigen Einheiten in $L[X]$ sind die $a \in L^\times$.

Kommen wir nun zum Hauptbeweis. Ist $a \in L$ eine Nullstelle von f, dann gilt $f = (X-a)g$ für ein $g \in L[X]$. Dann ist aber wegen der Leibnizregel

$$f' = q + (X-a)q'$$

und $f'(a) = q(a)$. Also gilt, dass a genau dann mehrfache Nullstelle von f ist, wenn $q(a) = 0 = f'(a)$ ist.

Nehmen wir an, dass $\mathsf{ggT}(f,f') = 1 \in K[X]$ ist. Es sei L' ein Zerfällungskörper von $F := \{f, f'\}$ über K. Ist $a \in L'$ eine gemeinsame Nullstelle von f und f', so teilt $X - a$ sowohl f als auch f'.

Haben f und f' dagegen keine gemeinsame Nullstelle und ist $d := \mathsf{ggT}(f,f')$, dann zerfällt d über L in Linearfaktoren $(X - a_i)$. Aber jedes solche a_i wäre eine gemeinsame Nullstelle, also muss $d = 1$ gewesen sein und damit sind f und f' teilerfremd. □

Vorlesung 26

Satz III.5.8. *Es sei $f \in K[X]$ irreduzibel.*

(a) *Ist die Charakteristik von K gleich 0, so ist f immer separabel.*
(b) *Ist die Charakteristik von K gleich p für eine Primzahl p, so ist f genau dann separabel, wenn $f' \neq 0$ ist und dies ist äquivalent dazu, dass wir f nicht schreiben können als ein Polynom in X^p.*
(c) *Allgemeiner gilt: Ist die Charakteristik von K gleich p, p prim, so gibt es ein $m \in \mathbb{N}_0$ und ein irreduzibles separables $g \in K[X]$, so dass $f(X) = g(X^{p^m})$ ist.*

BEWEIS. Ist f irreduzibel, so kann der $\mathsf{ggT}(f,f')$ nur eine Konstante oder f sein. Ist die Charakteristik von K gleich 0, so gilt

$$\mathrm{Grad}(f') = \mathrm{Grad}(f) - 1$$

und damit kann f die formale Ableitung nicht teilen und wir erhalten $\mathsf{ggT}(f,f') = 1$.

Ist die Charakteristik von K dagegen gleich p und $f \in K[X]$, dann gilt $\mathrm{Grad}(f') \leqslant \mathrm{Grad}(f) - 1$ und damit kann nur für $f' = 0$ das Polynom f f' teilen.

Ist $f = a_n X^n + a_{n-1}X^{n-1} + \ldots + a_1 X + a_0$, so ist f' genau dann das Nullpolynom, wenn $ia_i = 0$ gilt für alle $0 < i \leqslant n$. Ist $i \not\equiv 0 \bmod p$ so ist $i \neq 0 \in K$ und somit muss $a_i = 0$ sein. Damit ist $f = \sum_{pj \leqslant n} a_{pj} X^{pj}$ und damit folgen (b) und (c). □

Definition III.5.9.

(a) Ist $K \subset L$ algebraisch und $a \in L$, so heißt a *separabel über K*, falls $m_{a,K}$ separabel ist über K.
(b) Eine algebraische Körpererweiterung $K \subset L$ heißt *separabel*, falls jedes $a \in L$ separabel ist über K.

Bemerkung III.5.10. Wir wissen schon, dass jede algebraische Körpererweiterung $K \subset L$ in Charakteristik null separabel ist.

Ein $a \in \overline{K}$ ist genau dann separabel, wenn $m'_{a,K} \neq 0$ ist.

Für ein separables Element a hat $m_{a,K}$ nur einfache Nullstellen, also $a_1, \ldots, a_m$, falls $m = \mathrm{Grad}(m_{a,K})$. Für jedes solche a_i gibt es einen K-Homomorphismus $\varphi\colon K(a) \to K(a_i) \subset \overline{K}$.

Genauer erhalten wir mit Korollar III.3.6, dass

$$|\{\varphi\colon K(a) \to \overline{K} \quad K\text{-Homomorphismus}\}| = |\{a_i, a_i \text{ Nullstelle von } m_{a,K}\}|.$$

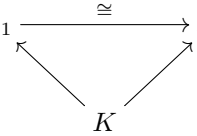
Wir wissen also für separables a, dass

$$\mathrm{Grad} m_{a,K} = [K(a) : K] = |\{\varphi\colon K(a) \to \overline{K} \quad K\text{-Homomorphismus}\}|.$$

Definition III.5.11. Es sei $K \subset L \subset \overline{K}$. Die Anzahl der verschiedenen K-Homomorphismen $\varphi\colon L \to \overline{K}$ heißt der *Separabilitätsgrad von L über K* und wird mit $[L:K]_s$ notiert.

Beispiel III.5.12. Ist a separabel über K, so gilt zum Beispiel $[K(a):K]_s = [K(a):K]$.

Bemerkung III.5.13.

- Die Zahl $[L:K]_s$ ist unabhängig von der Wahl von $\overline{K}$: Ist $\sigma\colon K \to M$ und ist M algebraisch abgeschlossen, so gilt für jeden K-Homomorphismus $\varphi\colon L \to M$ mit $\varphi|_K = \sigma$, dass $\varphi(L)$ algebraisch ist über $\varphi(K)$. Damit folgt
$$\varphi(L) \subset \overline{\varphi(K)} = \overline{\sigma(K)} \subset M.$$
Daher gibt es einen Isomorphismus $\psi\colon \overline{K} \to \overline{\sigma(K)}$ mit $\psi|_K = \sigma$ und wir erhalten eine Bijektion
$$\{\xi\colon L \to \overline{K} \quad K\text{-Homomorphismus}\} \cong \{\tilde{\xi}\colon L \to \overline{\sigma(K)}, \tilde{\xi}|_K = \sigma\},$$
die ξ auf $\psi \circ \xi$ beziehungsweise $\tilde{\xi}$ auf $\psi^{-1} \circ \tilde{\xi}$ abbildet.
- Gilt $L_1 \xrightarrow{\cong} L_2$, so ist $[L_1:K]_s = [L_2:K]_s$.


- Ist $K \subset L$ normal, so gilt für alle K-Homomorphismen $\sigma\colon L \to \overline{K}$, dass $\sigma(L) = L$ und damit ist
$$[L:K]_s = |\mathsf{Aut}_K(L)|.$$

Lemma III.5.14.

(a) *Sind $K \subset L \subset M$ algebraische Erweiterungen, so gilt*

$$[M:K]_s = [M:L]_s[L:K]_s. \tag{III.5.1}$$

(b) *Ist $K \subset L$ endlich, so ist $[L:K]_s \leqslant [L:K]$.*

Beweis. Ist $\varphi\colon M \to \overline{K}$ ein K-Homomorphismus, so ist $\varphi|_L\colon L \to \overline{K}$ ebenfalls ein K-Homomorphismus.

Wir können umgekehrt jeden K-Homomorphismus $\psi\colon L \to \overline{K}$ fortsetzen zu einem $\tilde{\psi}$ auf M und damit ist jedes ψ von der Form $\tilde{\psi}|_L$.

Es sei also $\beta\colon L \to \overline{K}$ ein K-Homomorphismus und $\tilde{\beta}\colon \overline{K} \to \overline{K}$ eine Fortsetzung von β. Dann ist $\tilde{\beta} \in \mathsf{Aut}_K(\overline{K})$ und $\tilde{\beta}|_M\colon M \to \overline{K}$ ist ein K-Homomorphismus.

Ist $\beta'\colon M \to \overline{K}$ beliebig mit $\beta'|_L = \beta$, so ist

$$\tilde{\beta}^{-1} \circ \beta'\colon M \xrightarrow{\beta'} \overline{K} \xrightarrow{\tilde{\beta}^{-1}} \overline{K}.$$

Ist $a \in L$ beliebig, so gilt
$$\tilde{\beta}^{-1} \circ \beta'(a) = \tilde{\beta}^{-1}(\beta(a)) = \beta^{-1}(\beta(a)) = a$$
und somit ist $\tilde{\beta}^{-1} \circ \beta'$ ein L-Homomorphismus.

Für jedes $\gamma\colon M \to \overline{K}$, welches ein L-Homomorphismus ist, ist $\tilde{\beta} \circ \gamma$ ein K-Homomorphismus, der β fortsetzt:
$$\tilde{\beta} \circ \gamma(x) = \tilde{\beta}(x) = \beta(x) \text{ für alle } x \in L.$$

Damit erhalten wir eine Bijektion zwischen der Menge der Fortsetzungen von β zu K-Homomorphismen von M nach $\overline{K}$ und der Menge aller L-Homomorphismen von M nach $\overline{K}$, indem wir mit $\tilde{\beta}$ beziehungsweise $\tilde{\beta}^{-1}$ verketten. Die Mächtigkeit der letzten Menge entspricht dem Separabilitätsgrad $[M:L]_s$.

Die Mächtigkeit der Menge aller βs ist der Separabilitätsgrad $[L:K]_s$, so dass wir insgesamt die gewünschte Gleichung
$$[L:K]_s[M:L]_s = [M:K]_s$$
erhalten.

Für (b) können wir $L = K(a_1, \ldots, a_m)$ schreiben mit $a_i \in L$. Wir setzen $L_0 := K$ und $L_i = K(a_1, \ldots, a_i)$ für $0 < i \leqslant m$.

Es gilt jeweils, dass $[L_i : L_{i-1}]$ der Grad von $m_{a_i, L_{i-1}}$ ist, während $[L_i : L_{i-1}]_s$ die Anzahl der Nullstellen von $m_{a_i, L_{i-1}}$ in L_i ist. Also gilt
$$[L_i : L_{i-1}]_s \leqslant [L_i : L_{i-1}]$$
und damit mit (a) auch $[L:K]_s \leqslant [L:K]$. □

Für einfache Erweiterungen $K \subset K(a)$ gilt, dass genau dann $[K(a) : K] = [K(a) : K]_s$ ist, wenn $m_{a,K}$ keine mehrfachen Nullstellen hat. Das gilt allgemeiner.

Satz III.5.15. *Es sei $K \subset L$ eine endliche Körpererweiterung. Dann sind äquivalent:*

(a) $[L : K]_s = [L : K]$.
(b) *$K \subset L$ ist separabel.*
(c) *Es gibt $a_1, \ldots, a_m \in L$, so dass a_i separabel ist über K und $L = K(a_1, \ldots, a_m)$.*

Beweis. Für (a) $\Rightarrow$ (b) sei $a \in L$ und wir betrachten $K \subset K(a) \subset L$. Ist $[L : K]_s = [L : K]$, so muss auch $[K(a) : K] = [K(a) : K]_s$ gelten, also ist jedes $a \in L$ separabel über K.

Für (b) $\Rightarrow$ (c) wissen wir, dass L endlich erzeugt ist über K, also ist $L = K(a_1, \ldots, a_m)$ mit $a_i \in L$. Da jedes $a_i \in L$ separabel ist nach Voraussetzung, folgt (c).

Für (c) $\Rightarrow$ (a) setzen wir wieder $L_0 = K$ und $L_i = K(a_1, \ldots, a_m)$ für $0 < i \leqslant m$. Wegen (III.5.1) genügt es zu zeigen, dass für alle i $[L_i : L_{i-1}] = [L_i : L_{i-1}]_s$ gilt.

Da aber a_i separabel ist über K, hat $m_{a_i,K}$ nur einfache Nullstellen in $\overline{K}$, aber damit hat auch $m_{a_i,L_{i-1}}$ nur einfache Nullstellen in $\overline{K}$. □

Satz III.5.16. *Ist $K \subset L$ eine Körpererweiterung. Dann ist*

$$L_s := \{a \in L, a \text{ ist separabel über } K\}$$

ein Zwischenkörper von K und L.

Der Körper L_s heißt die *separable Hülle von K in L.*

Beweis. Es ist klar, dass als Mengen gilt $K \subset L_s \subset L$. Zu zeigen ist, dass L_s ein Körper ist. Sind $a, b \in L_s$, so ist $K \subset K(a, b)$ separabel nach Satz III.5.15. Darin sind aber die Elemente $a + b$, ab, $-a, -b$ und a^{-1}, b^{-1} für $0 \neq a, b$ enthalten und damit sind sie auch in L_s. □

Satz III.5.17. *Ist $K \subset L$ separabel und ist $K \subset K' \subset L$ ein Zwischenkörper, so sind $K \subset K'$ und $K' \subset L$ separabel.*

Der Satz ist klar für endliche $K \subset L$. Wir geben einen allgemeinen Beweis.

Beweis. Es sei $a \in L$. Wir betrachten $m_{a,K}$ und $m_{a,K'}$. Es gilt $m_{a,K'} | m_{a,K} \in K'[X]$, weil $m_{a,K} \in (m_{a,K'})$. Hat $m_{a,K}$ nur einfache Nullstellen in $\overline{K}$, so hat auch $m_{a,K'}$ nur einfache Nullstellen in $\overline{K} = \overline{K'}$. Damit ist $K' \subset L$ separabel.

Da $K' \subset L$ ist jedes $x \in K'$ auch in L und damit separabel über K. □

Satz III.5.18. *Es sei $f \in K[X] \setminus K$. Dann sind äquivalent:*

(a) *Jeder Zerfällungskörper von f ist separabel über K.*
(b) *f ist separabel in $K[X]$.*

Beweis. Für (a) $\Rightarrow$ (b) betrachten wir einen normierten irreduziblen Teiler h von f und es sei L ein Zerfällungskörper von f. Damit zerfällt auch h über L in Linearfaktoren, hat also insbesondere eine Nullstelle a in L. Dann ist h aber gleich $m_{a,K}$ und da $a \in L$ ist a nach Voraussetzung separabel und $h' = m_{a,K} \neq 0$.

Für (b) $\Rightarrow$ (a) schreiben wir f über seinem Zerfällungskörper L als

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

mit $a_i \in L$ und $c \in K$. Dann ist $L = K(a_1, \ldots, a_n)$. Es gilt, dass jedes $m_{a_i,K}$ f teilt. Da f separabel ist, ist es auch jedes $m_{a_i,K}$ und die a_i sind separabel. Dann ist nach Satz III.5.15 L separabel.

□

Korollar III.5.19. *Ist $K \subset L$ endlich und separabel, so gibt es eine Körpererweiterung $L \subset N$, so dass $K \subset N$ normal, separabel und endlich ist.*

Beweis. Wir können L schreiben als $K(a_1, \ldots, a_n)$, wobei die a_i separabel sind über K. Wir setzen N an als den Zerfällungskörper von $\prod_{i=1}^{n} m_{a_i,K}$ über L. □

Der folgende Satz ist zentral für die gesamte Galoistheorie.

Satz III.5.20 (Satz vom primitiven Element)**.** *Ist $K \subset L$ eine endliche und separable Körpererweiterung. Dann ist L einfach, das heißt es gibt ein $a \in L$ mit*

$$L = K(a).$$

Beweis. Ist K ein endlicher Körper, dann ist auch L endlich. Damit wissen wir, dass $L^\times$ eine endliche zyklische Gruppe ist. Ist $a \in L^\times$ ein Erzeuger, so ist $L = K(a)$.

Es sei K ein unendlicher Körper. Wir wissen, dass $L = K(a_1, \ldots, a_n)$ ist mit $a_i \in L$ separabel. Wir machen Induktion über n. Ist $n = 1$, so ist nichts zu zeigen. Für den Schritt von n auf $n+1$ betrachten wir $K(a_1, \ldots, a_n, a_{n+1}) = K(a_1, \ldots, a_n)(a_{n+1})$. Nach Induktionsannahme gibt es ein $b \in L$, so dass $K(a_1, \ldots, a_n) = K(b)$ ist. Damit ist nur der Fall $n = 2$ zu zeigen.

Es sei also $L = K(b, c)$. Wir wählen ein $\overline{K}$ mit $K \subset L \subset \overline{K}$ und es seien $\varphi_1, \ldots, \varphi_m$ die verschiedenen K-Homomorphismen $\varphi_i \colon L \to \overline{K}$. Wir wissen $m = [L : K] = [L : K]_s$.

Wir definieren

$$g := \prod_{i<j} ((\varphi_i(b) - \varphi_j(b))X + (\varphi_i(c) - \varphi_j(c))) \in \overline{K}[X].$$

Da $L = K(b, c)$ und $\varphi_i \neq \varphi_j$ für $i < j$, gilt dass $\varphi_i(b) \neq \varphi_j(b)$ oder $\varphi_i(c) \neq \varphi_j(c)$. Somit ist g nicht das Nullpolynom. Da $|K| = \infty$ gilt, gibt es ein $\lambda \in K$, so dass $g(\lambda) \neq 0$, also

$$g(\lambda) = \prod_{i<j} ((\varphi_i(b) - \varphi_j(b))\lambda + (\varphi_i(c) - \varphi_j(c))) \neq 0.$$

Also unterscheidet sich $\varphi_i(\lambda b) - \varphi_j(\lambda b)$ von $-(\varphi_i(c) - \varphi_j(c))$ und

$$\varphi_i(\lambda b + c) = \lambda\varphi_i(b) + \varphi_i(c) \neq \varphi_j(\lambda b + c) = \lambda\varphi_j(b) + \varphi_j(c) \text{ für alle } i < j.$$

Wir setzen $a = \lambda b + c$. Da die $\varphi_i(a)$ alle verschieden sind und alle Wurzeln von $m_{a,K}$ sind, gilt, dass

$$[K(a) : K] = \mathrm{Grad}(m_{a,K}) \geqslant n = [L : K] = [L : K(a)][K(a) : K].$$

Dies geht nur, wenn $[L : K(a)] = 1$ ist, also wenn $L = K(a)$.

□

Vorlesung 27

III.6. Galois-Korrespondenz

Ist $K \subset L$, so operiert die Gruppe $\mathsf{Aut}_K(L)$ auf L. Wir wollen für geeignete $K \subset L$ *alle* Zwischenkörper $K \subset K' \subset L$ beschreiben und zwar als

$$L^H := \{x \in L, \varphi(x) = x \text{ für alle } \varphi \in H\},$$

falls $H < \mathsf{Aut}_K(L)$.

Was heißt *geeignet*?

Definition III.6.1.

(a) Eine algebraische Körpererweiterung $K \subset L$ heißt eine *Galoiserweiterung* (oder auch *galoissch*), falls sie normal und separabel ist.

(b) Ist $K \subset L$ galoissch, so heißt $\mathsf{Aut}_K(L)$ die *Galoisgruppe von L über K* und wir notieren sie mit $G(L/K) = \mathsf{Aut}_K(L)$.

Évariste Galois (1811–1832)

Bemerkung III.6.2. Es sei $K \subset L$ endlich. Wir wissen, dass für normale Erweiterungen gilt $[L : K]_s = |\mathsf{Aut}_K(L)|$ und ist $K \subset L$ separabel, so ist $[L : K] = [L : K]_s$. Also gilt für jede endliche Galoiserweiterung

$$[L : K] = |G(L/K)|.$$

Definition III.6.3. Ist G eine Gruppe, die aus Körperautomorphismen eines Körpers L besteht, so heißt

$$L^G := \{x \in L, \varphi(x) = x \text{ für alle } \varphi \in G\}$$

der *Fixkörper von G in L*.

Bemerkung III.6.4. Rechnen Sie bitte nach, dass L^G wirklich ein Körper ist.

Satz III.6.5. *Ist $K \subset L$ galoissch, so ist $L^{G(L/K)} = K$.*

Beweis. Nach Definition von $G(L/K) = \mathsf{Aut}_K(L)$ ist $K \subset L^{G(L/K)}$. Es sei $a \in L \setminus K$. Dann hat das Minimalpolynom $m_{a,K}$ mindestens Grad 2. Da $K \subset L$ normal ist, zerfällt $m_{a,K}$ über L in Linearfaktoren und weil a separabel ist, ist a nur eine einfache Nullstelle von $m_{a,K}$. Dann gibt es also ein $b \in L$ mit $b \neq a$ und $m_{a,K}(b) = 0$. Damit gibt es dann aber auch ein $\varphi \in G(L/K)$ mit $\varphi(a) = b$ und $a \notin L^{G(L/K)}$. □

Satz III.6.6. *Ist L ein beliebiger Körper und H eine beliebige endliche Untergruppe von Automorphismen von L. Dann ist $L^H \subset L$ galoissch mit $G(L/L^H) = H$ und $[L : L^H] = |H|$.*

Beweis. Wir betrachten zu $a \in L$ die Bahn

$$Ha = \{\varphi(a), \varphi \in H\}.$$

Da H endlich ist und $|Ha| \leqslant |H|$ können wir Ha schreiben als

$$Ha = \{a_1, \ldots, a_n\}$$

und $|Ha| = n$. Jedes $\varphi \in H$ permutiert die Menge Ha. Damit gilt für

$$f_a := \prod_{i=1}^{n}(X - a_i),$$

dass für alle $\varphi \in H$ $\varphi_*(f_a) = f_a$ ist. Damit sind die Koeffizienten von f_a in L^H und $f_a \in L^H[X]$.

- Da a eine Nullstelle von f_a ist, ist a algebraisch über L^H.
- Nach Konstruktion ist L Zerfällungskörper von
$$F := \{f_a, a \in L\} \subset L^H[X] \setminus L^H$$
über L^H und somit ist $L^H \subset L$ normal.
- Da f_a separabel ist über L^H ist jedes $a \in L$ separabel über L^H.

Insgesamt ist $L^H \subset L$ galoissch.

Nach Konstruktion teilt m_{a,L^H} das Polynom f_a und damit ist

$$\text{Grad}(m_{a,L^H}) \leqslant \text{Grad}(f_a) = n \leqslant |H| \text{ für alle } a \in L. \tag{III.6.1}$$

(Wir wissen noch nicht, dass $L^H \subset L$ endlich ist. Sonst könnten wir direkt aus dem Satz vom primitiven Element schließen, dass $[L : L^H] \leqslant |H|$ ist.)

Annahme, es gilt $|H| < [L : L^H]$. Da $L^H \subset L$ algebraisch ist, gibt es ein $S \subset L$ mit

$$|H| < [L^H(S) : L^H] < \infty.$$

Mit dem Satz vom primitiven Element gibt es ein $a_0 \in L$ mit $L^H(a_0) = L^H(S)$. Daraus folgt, dass

$$\text{Grad}(m_{a_0,L^H}) = [L^H(a_0) : L^H] > H$$

und dies ist ein Widerspruch zu (III.6.1). Damit ist also gezeigt, dass $[L : L^H] \leqslant |H|$.

- Wir wissen, dass $H < \mathsf{Aut}_{L^H}(L)$, weil H die Elemente aus L^H fix läßt.
- $L^H \subset L$ ist endlich und damit erhalten wir
$$|H| \leqslant \mathsf{Aut}_{L^H}(L) = [L : L^H]_s = [L : L^H] \leqslant |H|.$$
Also muss $H = \mathsf{Aut}_{L^H}(L)$ sein und insbesondere ist H die Galoisgruppe von L über L^H.

□

Bemerkung III.6.7. Als Nebenergebnis erhalten wir, dass für alle $a \in L$ gilt, dass $f_a = m_{a,L^H}$ ist: Wir hatten schon gesehen, dass gilt $m_{a,L^H} | f_a$. Da a eine Nullstelle von m_{a,L^H} ist und $H = \mathsf{Aut}_K(L)$ gilt, sind auch alle $b \in Ha$ Nullstellen von m_{a,L^H} und damit gilt Gleicheit.

Satz III.6.8 (Galois-Korrespondenz)**.** *Es sei $K \subset L$ eine endliche Galoiserweiterung. Es sei $\mathfrak{U}$ die Menge aller Untergruppen von $G(L/K)$ und $\mathfrak{Z}$ sei die Menge aller Zwischenkörper zwischen K und L. Dann gilt:*

(a) *Die Zuordnungen $\gamma\colon \mathfrak{Z} \to \mathfrak{U}$ und $\varrho\colon \mathfrak{U} \to \mathfrak{Z}$ mit*

$$\gamma(M) := G(L/M), \quad \varrho(H) := L^H$$

sind zueinander inverse Bijektionen.

(b) *Für alle $\varphi \in G(L/K)$ und für alle $H \in \mathfrak{U}$ gilt*

$$\varphi(L^H) = L^{\varphi H \varphi^{-1}}.$$

(c) *Für einen Zwischenkörper $K \subset M \subset L$ ist $K \subset M$ genau dann normal, falls gilt $G(L/M) \lhd G(L/K)$. In diesem Fall definiert*

$$\mathrm{res}\colon G(L/K) \to G(M/K), \quad \varphi \mapsto \varphi|_M$$

einen Epimorphismus mit Kern $G(L/M)$ und somit gilt

$$G(M/K) \cong G(L/K)/G(L/M).$$

Vorsicht: Sowohl γ als auch ϱ verkehren die Teilmengenrelation. Sind $M_1, M_2 \in \mathfrak{Z}$ mit $M_1 \subset M_2$, so ist $G(L/M_2) \subset G(L/M_1)$. Sind $H_1, H_2 \in \mathfrak{U}$ mit $H_1 \subset H_2$, so ist $L^{H_2} \subset L^{H_1}$.

Beweis. Zu (a) sei $M \in \mathfrak{Z}$. Dann ist $M \subset L$ galoissch, weil es normal und separabel ist. Es gilt weiterhin

$$M = L^{G(L/M)} = L^{\gamma(M)} = \varrho(\gamma(M)).$$

Für $H \in \mathfrak{U}$ ist $\varrho(H) = L^H$. Wir wissen, dass $L^H \subset L$ galoissch ist mit $K \subset L^H \subset L$ und $G(L/L^H) = H$, so dass

$$\gamma(\varrho(H)) = \gamma(L^H) = G(L/L^H) = H.$$

Für (b) ist nach Definition klar, dass ein $a \in L$ genau dann in L^H liegt, wenn $\sigma(a) = a$ gilt für alle $\sigma \in H$. Dies ist genau dann der Fall, wenn für alle $\varphi \in G(L/K)$ gilt:

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

Aber das sagt nichts anderes als dass $\varphi(a) \in L^{\varphi H \varphi^{-1}}$ liegt.

Zu (c): Ist $H \in \mathfrak{U}$ und ist $K \subset L^H$ normal, so gilt

$$\varphi(L^H) = L^H \text{ für alle } \varphi \in G(L/K).$$

Aber $\varphi(L^H) = L^{\varphi H \varphi^{-1}}$ und somit ist $L^H = L^{\varphi H \varphi^{-1}}$. Da ϱ bijektiv ist, besagt dies schon, dass für alle $\varphi \in G(L/K)$ gelten muss, dass

$$\varphi H \varphi^{-1} = H.$$

Somit ist H normal in $G(L/K)$.

Ist umgekehrt $N \lhd G(L/K) =: G$, so gilt $G(L/L^N) = N$. Die Gruppe G/N operiert auf L^N durch

$$gN.a := g(a).$$

Dies ist wohldefiniert und es gilt $(L^N)^{G/N} = L^G = K$, also ist $K \subset L^N$ eine Galoiserweiterung mit Galoisgruppe $G/N = G(L^N/K)$ und $G/N = G(L/K)/G(L/L^N)$.

□

Literaturverzeichnis

[1] Jens Carsten Jantzen, Joachim Schwermer, *Algebra*, 2. Auflage, Springer-Verlag Berlin Heidelberg 2014.

[2] Felix Klein, *Vorlesungen über das Ikosaeder und die Auflösung der Gleichungen vom fünften Grade*, Reprint of the 1884 original. Edited, with an introduction and commentary by Peter Slodowy. Birkhäuser Verlag, Basel; B. G. Teubner, Stuttgart, 1993.

[3] Tsit Yuen Lam, *Lectures on modules and rings*, Graduate Texts in Mathematics, 189. Springer-Verlag, New York, 1999.

[4] Serge Lang, *Algebra*, Revised third edition. Graduate Texts in Mathematics, 211. Springer-Verlag, New York, 2002.

[5] Falko Lorenz, *Einführung in die Algebra. Teil I*, Second edition. Bibliographisches Institut, Mannheim, 1992.

[6] Falko Lorenz, *Einführung in die Algebra. Teil II*, Bibliographisches Institut, Mannheim, 1990.

[7] Patrick Morandi, *Field and Galois theory*, Graduate Texts in Mathematics, 167. Springer-Verlag, New York, 1996.