Thomas Krämer

Algebra und Funktionentheorie

Vorlesung an der HU Berlin, Winter 2021/22

Dateiversion vom 1. April 2022

Inhaltsverzeichnis

Einführung 1
1 Konstruktionen mit Zirkel und Lineal 1
2 Lösung algebraischer Gleichungen durch Radikale 6

I Gruppen 9
1 Gruppen und Untergruppen 9
2 Gruppenhomomorphismen 15
3 Nebenklassen 18
4 Normalteiler und Quotienten 22
5 Präsentationen von Gruppen 27
6 Gruppenoperationen 31
7 Symmetrische und alternierende Gruppen 37
8 Die Sätze von Sylow 43
9 Kompositionsreihen 49

II Ringe und Polynome 59
1 Grundbegriffe 59
2 Homomorphismen und Ideale 63
3 Primideale und maximale Ideale 67
4 Quotientenkörper 70
5 Faktorielle Ringe und das Lemma von Gauss 71

III Körper und Galoistheorie 81
1 Endliche und algebraische Erweiterungen 81
2 Algebraischer Abschluss eines Körpers 89
3 Fortsetzungen von Homomorphismen 93
4 Zerfällungskörper und normale Erweiterungen 99
5 Separable Erweiterungen 103
6 Galoiserweiterungen 110
7 Kreisteilungskörper und Konstruierbarkeit 117
8 Auflösbarkeit durch Radikale 122

IV Ein wenig Funktionentheorie 127
1 Holomorphe Funktionen 127
2 Potenzreihen und analytische Funktionen 132
3 Ein Beispiel: Der komplexe Logarithmus 137
4 Der Integralsatz von Cauchy 140
5 Die Cauchy-Formel und Anwendungen 151
6 Singularitäten und Laurententwicklung 159
7 Der Residuensatz 166
8 Ausblick: Riemannsche Flächen 174

Einführung

Zusammenfassung Bevor wir mit dem systematischen Aufbau der Algebra und Galoistheorie beginnen, wollen wir uns als Motivation zunächst zwei historische Beispiele ansehen, aus denen sich die Theorie entwickelt hat: Die Frage nach der Konstruierbarkeit eines regelmäßigen n-Ecks mit Zirkel und Lineal und die Frage nach geschlossenen Formeln für die Lösungen algebraischer Gleichungen. Beide werden wir im Laufe der Vorlesung genauer verstehen.

1 Konstruktionen mit Zirkel und Lineal

Unter einer *Konstruktion mit Zirkel und Lineal* versteht man in der Euklidischen Geometrie die Konstruktion einer Figur in der Ebene, wobei als Hilfsmittel lediglich eine gegebene Menge von Punkten, ein Zirkel und ein Lineal ohne Längenmaßstab erlaubt sind. Im Folgenden identifizieren wir die Zeichenebene mit der komplexen Ebene $\mathbb{C}$. Etwas formaler können wir dann sagen:

Definition 1.1. Eine Zahl $z \in \mathbb{C}$ heißt aus einer Teilmenge $S_0 \subseteq \mathbb{C}$ *konstruierbar*, wenn es eine Folge von Punkten

$$p_1,\, p_2,\, \ldots,\, p_n \,\in\, \mathbb{C} \quad \text{mit} \quad p_n \,=\, z$$

gibt, sodass die Mengen $S_i := S_0 \cup \{p_1, \ldots, p_i\}$ sukzessive wie folgt entstehen: Der Punkt p_{i+1} ist

- der Schnittpunkt von zwei nicht zueinander parallelen Geraden $\overline{pq}$ und $\overline{rs}$ durch Punkte $p,q,r,s \in S_i$ mit $p \neq q$ und $r \neq s$, oder
- ein Schnittpunkt einer solchen Gerade durch zwei verschiedene Punkte aus S_i und einem Kreis mit Mittelpunkt p und Radius $|q-p|$ für $p,q \in S_i$, oder
- ein Schnittpunkt von zwei verschiedenen solchen Kreisen.

Eine Zahl heißt *konstruierbar*, wenn sie aus $S_0 = \{0,1\}$ konstruierbar ist.

Beispiel 1.2. Aus der Antike sind drei sprichwörtliche Probleme überliefert:

- *Quadratur des Kreises:* Kann man aus einem gegebenen Kreis in endlich vielen Schritten ein Quadrat mit dem gleichen Flächeninhalt konstruieren? Dies läuft hinaus auf die Frage, ob die Kreiszahl $z = \pi$ konstruierbar ist.
- *Würfelverdopplung:* Kann man zu einem Würfel gegebener Kantenlänge einen Würfel doppelten Volumens konstruieren? Dieses sogenannte Delische Problem läuft hinaus auf die Frage, ob die Zahl $z = \sqrt[3]{2}$ konstruierbar ist.
- *Dreiteilung des Winkels:* Kann man einen beliebig gegebenen Winkel α in drei gleiche Teile teilen? Dies läuft hinaus auf die Frage, ob die Zahl $z = \exp(2\pi i\alpha/3)$ aus der Menge $S_0 = \{0, 1, \exp(2\pi i\alpha)\}$ konstruierbar ist.

Die Antwort auf alle drei Fragen ist negativ, aber ein Beweis dafür, dass sie mit Zirkel und Lineal tatsächlich unlösbar sind, wurde erst im 19. Jh. möglich. Die Quadratur des Kreises berührt dabei die Analysis und wurde erst mit dem Beweis der Transzendenz von π durch Lindemann 1882 beantwortet. Im Gegensatz dazu handelt es sich bei der Würfelverdopplung und der Drittelung des Winkels um ein algebraisches Problem, die Antwort hat Pierre Wantzel 1837 ausgehend von den bahnbrechenden Arbeiten von Gauss und Galois gegeben – dem Ausgangspunkt für die bis heute in der Algebra und Zahlentheorie wichtige Galoistheorie. Wir wollen hier die Frage nach der Konstruierbarkeit mit Zirkel und Lineal an einem weiteren berühmten Beispiel veranschaulichen: Für welche $n \in \mathbb{N}$ kann man ein regelmäßiges n-Eck mit Zirkel und Lineal konstruieren, d.h. für welche $n \in \mathbb{N}$ ist die komplexe Zahl

$$z \;=\; e^{2\pi i/n}$$

konstruierbar? Für $n = 3, 4, 5$ ist dies der Fall, zudem sieht man leicht:

- Ist ein regelmäßiges n-Eck konstruierbar, so auch ein regelmässiges $2n$-Eck.
- Sind m, n zueinander teilerfremd und sind ein regelmäßiges n-Eck und n-Eck konstruierbar, dann ist auch ein regelmäßiges mn-Eck konstruierbar: Denn wegen der Teilerfremdheit von m und n existieren $a, b \in \mathbb{Z}$ mit $am + bn = 1$, und dann ist
$$e^{2\pi i/mn} \;=\; (e^{2\pi i/n})^a \cdot (e^{2\pi i/m})^b$$

Darüber hinaus ist allerdings weniger klar, was passiert: Kann man beispielsweise ein regelmäßiges 7-Eck konstruieren? Als Jugendlicher hat Gauß eine Konstruktion für das regelmäßige 17-Eck gefunden und wenig Jahre später die abschließende Antwort auf die Frage gegeben:

Satz 1.3 (Gauss). *Ein regelmäßiges n-Eck ist dann und nur dann mit Zirkel und Lineal konstruierbar, wenn*

$$n \;=\; 2^k \cdot \prod_{i=1}^{l} F_{m_i}$$

mit $k, l \in \mathbb{N}_0$ und paarweise verschiedene Primzahlen der Form $F_{m_i} = 2^{2^{m_i}} + 1$.

Die Zahlen $F_m = 2^{2^m} + 1$ werden auch als *Fermat-Zahlen* bezeichnet, unabhängig davon, ob sie prim sind oder nicht. Fermat-Zahlen, die prim sind, bezeichnet man als *Fermat-Primzahlen*. Sie sind sehr selten, die einzigen heute bekannten sind die ersten fünf Fermat-Zahlen:

$$\begin{aligned} F_0 &= 3, \\ F_1 &= 5, \\ F_2 &= 17, \\ F_3 &= 257, \\ F_4 &= 65537. \end{aligned}$$

Heuristische Argumente legen nahe, dass es keine weiteren Fermat-Primzahlen gibt, dies ist jedoch bis heute unbewiesen. Da die Folge der Fermat-Zahlen aber sehr schnell wächst, liefert uns der Satz von Gauss ein klares Bild: Das reguläre n-Eck ist konstruierbar genau für

$$n = 3, 4, 5, 6, 8, 10, 12, 15, 16, 17, 20, 24, 30, 32, 34, 40, 48, 51, 60, 64, 68, 80, 85, 96, \ldots$$

Dies beantwortet auch die Frage nach der Dreiteilung eines Winkels:

Korollar 1.4. *Der Winkel $\alpha = 2\pi/3$ lässt sich nicht mit Zirkel und Lineal dritteln.*

Beweis. Ein regelmäßiges Dreieck ist mit Zirkel und Lineal konstruierbar, aber ein regelmäßiges Neuneck nach dem Satz von Gauß nicht. □

Wir werden den Beweis des Satzes von Gauß in der Galoistheorie behandeln. Die Grundidee ist die folgende algebraische Charakterisierung der Menge sämtlicher konstruierbarer Zahlen:

Proposition 1.5. *Es gilt:*

a) Die Menge aller konstruierbaren Zahlen ist ein Teilkörper $K \subseteq \mathbb{C}$.

b) Dieser Teilkörper lässt sich charakterisieren als der kleinste Teilkörper von $\mathbb{C}$, der unter komplexen Quadratwurzeln abgeschlossen ist in dem Sinn, dass er die folgende Eigenschaft hat:

$$\forall\, z \in \mathbb{C}: \quad z^2 \in K \Rightarrow z \in K$$

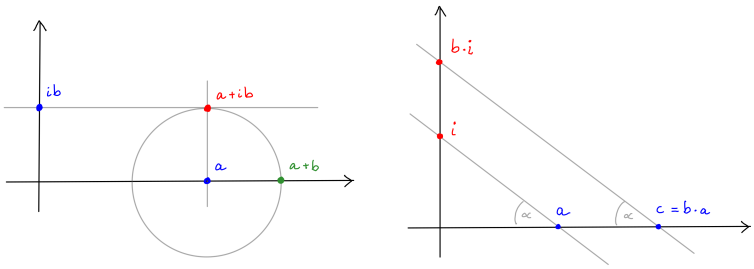
Beweis. *a*) Per Definition von Konstruierbarkeit ist $0, 1 \in K$. Die Gerade durch diese zwei Punkte ist die reelle Achse; durch Schneiden mit dem Kreis durch den Punkt 1 mit Mittelpunkt 0 erhalten wir den Punkt $-1 \in K$. Die zur reellen Achse senkrechte Gerade durch den Ursprung ist die imaginäre Achse, sie schneidet den Einheitskreis in $\pm i \in K$. Da sich mit Zirkel und Lineal die Orthogonalprojektion eines Punktes auf eine Gerade, hier konkret auf die reelle und imaginäre Achse, konstruieren lässt und umgekehrt für alle $x, y \in K \cap \mathbb{R}$ offenbar auch $x + iy \in K$ ist, folgt:

$$z \in K \quad \Longleftrightarrow \quad \mathrm{Re}(z),\, \mathrm{Im}(z) \in K$$

Um die Abgeschlossenheit der Teilmenge $K \subseteq \mathbb{C}$ unter Addition und Multiplikation nachzuprüfen, genügt es daher wegen

$$\begin{aligned} \mathrm{Re}(z+w) &= \mathrm{Re}(z)+\mathrm{Re}(w), \quad & \mathrm{Re}(zw) &= \mathrm{Re}(z)\mathrm{Re}(w)-\mathrm{Im}(z)\mathrm{Im}(w), \\ \mathrm{Im}(z+w) &= \mathrm{Im}(z)+\mathrm{Im}(w), \quad & \mathrm{Im}(zw) &= \mathrm{Re}(z)\mathrm{Im}(w)+\mathrm{Im}(z)\mathrm{Re}(w), \end{aligned}$$

die entsprechende Aussage für $K \cap \mathbb{R}$ zu zeigen. Um die Summe und das Produkt von Punkten $a, b \in K \cap \mathbb{R}$ zu konstruieren, kann man dann wie in der folgenden Skizze vorgehen:



Das zweite Bild lässt sich auch "rückwärts" lesen und zeigt, dass für $a, c \in K \cap \mathbb{R}$ und $a \neq 0$ auch $b = c/a \in K \cap \mathbb{R}$ ist. Somit ist $K \cap \mathbb{R}$ ein Körper. Dieses Resultat überträgt sich direkt vom reellen auf den komplexen Fall, denn da für jedes $z \in K$ auch

$$\bar{z} \;=\; \mathrm{Re}(z) - i\mathrm{Im}(z) \;\in\; K \quad \text{und} \quad |z|^2 \;=\; \mathrm{Re}(z)^2 + \mathrm{Im}(z)^2 \;\in\; K \cap \mathbb{R}$$

ist, folgt für $z \neq 0$ aus $|z|^{-2} \in K \cap \mathbb{R} \subseteq K$ und der multiplikativen Abgeschlossenheit wie gewünscht

$$\frac{1}{z} \;=\; \frac{1}{|z|^2} \cdot \bar{z} \;\in\; K.$$

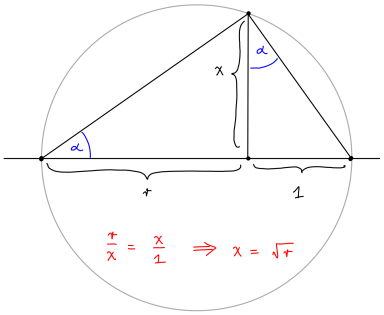
b) Zunächst beachte man, dass für jede komplexe konstruierbare Zahl $z \in K$ auch ihr Absolutbetrag $|z| \in K \cap \mathbb{R}$ konstruierbar ist: Hierzu muß man lediglich den Kreis durch z um den Ursprung mit der reellen Achse schneiden. Außerdem lässt sich mit Zirkel und Lineal jeder Winkel halbieren. Da sich die Quadratwurzeln einer komplexen Zahl aus ihrer Darstellung in Polarkoordinaten durch die Formel

$$\sqrt{z} \;=\; \pm\sqrt{r} \cdot e^{i\alpha/2} \quad \text{für} \quad z \;=\; r \cdot e^{i\alpha} \quad \text{mit} \quad r \;=\; |z| \quad \text{und} \quad \alpha \;\in\; \mathbb{R}_{\geq 0}$$

ergeben, genügt es für den Beweis der Abgeschlossenheit des Teilkörpers $K \subseteq \mathbb{C}$ unter komplexen Quadratwurzeln, dies nur für positive reelle konstruierbare Zahlen zu zeigen:

$$r \;\in\; K \cap \mathbb{R}_{>0} \quad \Rightarrow \quad \sqrt{r} \;\in\; K \cap \mathbb{R}_{>0}$$

Hierzu kann man einen Kreis mit Durchmesser $r+1$ betrachten wie in der folgenden Skizze angedeutet:



Wegen $r/x = x/1$ gilt $x^2 = r$ und damit haben wir $x = \sqrt{r}$ konstruiert. Damit ist klar, dass der Körper der konstruierbaren Zahlen abgeschlossen unter komplexen Quadratwurzeln ist. Um zu zeigen, dass er der kleinste solche Teilkörper von $\mathbb{C}$ ist, müssen wir noch zeigen, dass sich umgekehrt auch jede konstruierbare Zahl aus den Zahlen $0,1$ durch endlich viele Additionen, Multiplikationen, Divisionen und Quadratwurzeln erhalten lässt. Aber das folgt direkt aus der Definition von Konstruierbarkeit: Der Schnittpunkt zweier Geraden ist die Lösung einer linearen Gleichung, während die Real- und Imaginärteile der Schnittpunkte von einem Kreis mit einer Geraden oder von zwei Kreisen sich durch quadratische Gleichungen berechnen und somit durch die bekannten Formeln mit Wurzeln ausdrücken lassen. □

Der Beweis hat uns genauer gezeigt, dass wir den Körper der konstruierbaren Zahlen induktiv aus sehr einfachen Schritten konstruieren können:

Übung 1.6. Sei $k \subseteq \mathbb{C}$ ein Teilkörper und $a \in \mathbb{C}$ mit $a^2 \in k$. Dann ist auch die Menge

$$k(a) \;:=\; \big\{x + y \cdot a \in \mathbb{C} \mid x, y \in k\big\} \;\subseteq\; \mathbb{C}$$

ein Teilkörper der komplexen Zahlen. Im Fall $a \notin k$ bezeichnen wir das Paar $k \subseteq k(a)$ auch als eine *quadratische* Körpererweiterung.

Korollar 1.7. *Eine Zahl $z \in \mathbb{C}$ ist konstruierbar genau dann, wenn es eine Folge von Teilkörpern*

$$K_0 = \mathbb{Q} \;\subseteq\; K_1 \;\subseteq\; \cdots \;\subseteq\; K_n \quad \text{mit} \quad z \;\in\; K_n$$

gibt, sodass jedes $K_i \subseteq K_{i+1}$ eine quadratische Körpererweiterung ist.

Beweis. Folgt direkt aus dem obigen Beweis. □

Mit den richtigen Begriffen der Körpertheorie, die wir im Laufe der Vorlesung entwickeln werden, wird dann die Unmöglichkeit der Würfelverdopplung zu einem Zweizeiler. Der Satz von Gauss ist schwieriger. Allgemein fragt sich: Wie sieht man einer Zahl $z \in \mathbb{C}$ an, ob sie die Bedingung im obigen Korollar gilt? Wir werden sehen, dass sukzessive Körpererweiterungen von der obigen Form sehr spezielle Eigenschaften haben. In der Galoistheorie werden wir diese beschreiben, indem wir jeder Körpererweiterung ihre "Symmetriegruppe" zuordnen. Die Bedingung in dem

Korollar liefert dann eine Bedingung an die Galoisgruppe, die sich mit etwas mehr Verständnis der Struktur von Gruppen in den Satz von Gauss übersetzen lässt. Dazu benötigen wir aber zunächst etwas mehr Gruppentheorie! Als Nebenprodukt werden wir nicht nur einen Beweis des obigen Satzes von Gauß erhalten, sondern viele weitere Anwendungen.

2 Lösung algebraischer Gleichungen durch Radikale

Eine weiteres sehr altes Problem ist die Frage nach der Lösbarkeit algebraischer Gleichungen: Gibt es eine geschlossene Formel für die Lösung von Gleichungen der Form

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \;=\; 0,$$

die nur rationale Funktionen in den Koeffizienten $a_0, a_1, \ldots, a_{n-1}$ und k-te Wurzeln beinhaltet?

Beispiel 2.1. Die quadratische Gleichung

$$x^2 + px + q \;=\; 0$$

kann man mittels quadratischer Ergänzung lösen: Für die neue Variable $t = x + p/2$ wird die Gleichung zu

$$t^2 \;=\; \left(\frac{p}{2}\right)^2 - q$$

und somit $t = \pm\sqrt{\left(\frac{p}{2}\right)^2 - q}$, was zu der bekannten Formel führt:

$$x \;=\; -\frac{p}{2} \pm \sqrt{\left(\frac{p}{2}\right)^2 - q}$$

Man beachte, dass diese Formel auch dann noch gilt, wenn der Ausdruck unter der Quadratwurzel negativ ist, die Wurzel ist dann als komplexe Zahl zu verstehen. So gilt die Formel für beliebige $p, q \in \mathbb{C}$.

Beispiel 2.2. Die kubische Gleichung

$$x^3 + ax^2 + bx + c \;=\; 0$$

ist bereits komplizierter. Zunächst können wir mit der Substitution $t = x + a/3$ wie zuvor einen Koeffizienten zu Null machen und erhalten eine äquivalente Gleichung von der Form

$$t^3 + pt + q \;=\; 0 \quad \text{mit} \quad \begin{cases} p \;=\; \ldots \\ q \;=\; \ldots \end{cases}$$

Für die Lösungen dieser kubischen Gleichung gibt es eine berühmte Formel, die von Gerolamo Cardano 1545 in seinem Buch *Ars magna* publiziert wurde, aber

von Nicolo Tartaglia oder laut Cardano noch früher von Scipione del Ferro entdeckt wurde. Die folgende Formulierung ist ein Anachronismus, da die komplexen Zahlen damals noch nicht zur Verfügung standen:

Satz 2.3 (Cardanische Formel). *Jede Lösung der Gleichung $t^3 + pt + q = 0$ lässt sich schreiben als*

$$t \;=\; \sqrt[3]{-\frac{q}{2}+\sqrt{\Delta}} \;+\; \sqrt[3]{-\frac{q}{2}-\sqrt{\Delta}} \quad \textit{mit} \quad \Delta \;:=\; \left(\frac{p}{3}\right)^3 + \left(\frac{q}{2}\right)^2$$

für eine geeignete Wahl der auftretenden komplexen dritten Wurzeln.

Beweis (nach Lagrange). Seien $t_1, t_2, t_3 \in \mathbb{C}$ die drei gesuchten Lösungen, also die Nullstellen des komplexen Polynoms

$$t^3 + pt + q \;=\; \prod_{i=1}^{3} (t - t_i) \;\in\; \mathbb{C}[t].$$

Ausmultiplizieren der rechten Seite und Koeffizientenvergleich liefert

$$\begin{aligned} t_1 + t_2 + t_3 &= 0, \\ t_1t_2 + t_1t_3 + t_2t_3 &= p, \\ -t_1t_2t_3 &= q. \end{aligned}$$

An dieser Stelle scheinen wir nicht viel weiter zu sein als zuvor: Wir haben eine Gleichung in einer Variablen durch drei Gleichungen in drei Variablen ersetzt. Aber wir substituieren nun die Variablen geschickt und setzen

$$\begin{pmatrix} s_1 \\ s_2 \\ s_3 \end{pmatrix} \;=\; \frac{1}{3} \begin{pmatrix} 1 & 1 & 1 \\ 1 & \zeta & \zeta^2 \\ 1 & \zeta^2 & \zeta \end{pmatrix} \begin{pmatrix} t_1 \\ t_2 \\ t_3 \end{pmatrix} \quad \text{für} \quad \zeta \;=\; e^{2\pi i/3}.$$

Die dazu inverse Substitution ergibt sich mit linearer Algebra wegen $1 + \zeta + \zeta^2 = 0$ leicht zu

$$\begin{pmatrix} t_1 \\ t_2 \\ t_3 \end{pmatrix} \;=\; \begin{pmatrix} 1 & 1 & 1 \\ 1 & \zeta^2 & \zeta \\ 1 & \zeta & \zeta^2 \end{pmatrix} \begin{pmatrix} s_1 \\ s_2 \\ s_3 \end{pmatrix} \quad \text{wegen} \quad \zeta^3 \;=\; 1.$$

Es genügt daher, das System in den neuen Variablen zu lösen. Unter Benutzung der Relation $1 + \zeta + \zeta^2 = 0$ werden die obigen drei Gleichungen für t_1, t_2, t_3 in den neu eingeführten Variablen s_1, s_2, s_3 nach kurzer Rechnung zu

$$\begin{aligned} s_1 &= 0, \\ 3s_2s_3 &= -p, \\ s_2^3 + s_3^3 &= -q. \end{aligned}$$

Wenn wir die zweite dieser drei Gleichungen zur dritten Potenz nehmen, erhalten wir, dass s_2^3 und s_3^3 die beiden Nullstellen des quadratischen Polynoms

$$(u-s_2^3)(u-s_3^3) \;=\; u^2+q\cdot u-p^3/27 \;\in\; \mathbb{C}[u]$$

sind. Man beachte, dass das auf der rechten Seite hingeschriebene Polynom nur von den Koeffizienten p,q abhängt! Die Lösungsformel für quadratische Gleichungen liefert

$$s_2^3,\, s_3^3 \;=\; -\frac{q}{2}\pm\sqrt{\Delta} \quad \text{mit} \quad \Delta \;=\; \left(\frac{q}{2}\right)^2+\left(\frac{p}{3}\right)^3$$

und somit

$$s_2, s_3 \;=\; \sqrt[3]{-\frac{q}{2}\pm\sqrt{\Delta}},$$

wobei die komplexen dritten Wurzeln so zu wählen sind, dass $3s_2s_3=-p$ ist. Durch Rücktransformation zu t_1,t_2,t_3 erhalten wir die Cardano'schen Formeln. □

Ähnliche Formeln gibt es auch noch für Gleichungen vierten Grades. Danach hört der Spaß aber auf, und wieder ist dies ein berühmter Satz aus dem 19. Jh.:

Satz 2.4 (Abel 1862). *Für $n\geq 5$ gibt es keine allgemeine Formel, die die Lösungen der Gleichung*

$$t^n+a_{n-1}t^{n-1}+\cdots+a_0 \;=\; 0$$

aus $a_0,\ldots,a_{n-1}\in\mathbb{C}$ nur mithilfe von Additionen, Subtraktionen, Multiplikationen, Divisionen und komplexem Wurzelziehen berechnen würde.

Man beachte, dass es in diesem Satz nur um Formeln geht, die für beliebige Wahl der Koeffizienten gelten. Spezielle Gleichungen wie etwa

$$x^n-c \;=\; 0$$

lassen sich natürlich durch *Radikale*, also komplexes Wurzelziehen, lösen. Aber die Nullstellen solcher Polynome sind sehr spezielle Zahlen. Wie bei konstruierbaren Zahlen können wir sie wieder mit Methoden der Körpertheorie studieren:

Bemerkung 2.5. Die Menge aller Zahlen, welche man aus $\mathbb{Q}$ durch Anwenden von Addition, Multiplikation, Subtraktion, Division und komplexen Wurzeln beliebiger Ordnung erhalten kann, bilden einen Teilkörper von $\mathbb{C}$.

Im Unterschied zum Fall konstruierbarer Zahlen lassen wir jetzt auch Wurzeln höherer Ordnung zu. Trotzdem wird uns Galoistheorie auch in diesem Fall erlauben, die spezielle induktiv erhaltene Struktur dieses Körpers durch gruppentheoretische Eigenschaften zu charakterisieren und so den Satz von Abel zu beweisen. An dieser Stelle verlassen wir den historischen Pfad jedoch erst einmal und bauen die Theorie aus moderner Sicht systematisch auf. Dazu beginnen wir mit einigen Grundlagen der Gruppentheorie, die auch unabhängig von der Galoistheorie von Interesse sind und vielseitige Anwendungen in der Mathematik und Physik besitzen.

Kapitel I
Gruppen

Zusammenfassung In diesem Kapitel werfen wir einen genaueren Blick auf die Struktur endlicher Gruppen. Die Sätze von Sylow lassen bereits viel Information aus der Primfaktorzerlegung der Gruppenordnung ablesen. Im Satz von Jordan-Hölder werden wir sehen, wie sich jede endliche Gruppe im Wesentlichen eindeutig in ihre einfachen Bestandteile zerlegen lässt. Schließlich werden wir die wichtige Klasse der auflösbaren Gruppen kennenlernen, die sich durch sukzessive Erweiterungen abelscher Gruppen gewinnen lassen.

1 Gruppen und Untergruppen

Der Begriff einer Gruppe gehört zu den grundlegensten Strukturen der gesamten Mathematik und spielt eine wichtige Rolle bei der Beschreibung von Symmetrien in der Natur. Wir erinnern kurz an die Definition:

Definition 1.1. Eine *Gruppe* ist ein Paar $(G,\circ)$ bestehend aus einer Menge G und einer Verknüpfung

$$\circ: \quad G\times G \longrightarrow G,$$

sodass gilt:

a) Neutrales Element: Es gibt ein $e\in G$ mit $e\circ g = g\circ e = g$ für alle $g\in G$.

b) Assoziativität: Es ist $(g\circ h)\circ k = g\circ(h\circ k)$ für alle $g,h,k\in G$.

c) Inverse: Zu jedem $g\in G$ existiert ein $g^{-1}\in G$ mit $g\circ g^{-1} = g^{-1}\circ g = e$.

Die Gruppe heißt *kommutativ* oder *abelsch*, wenn $a\circ b = b\circ a$ für alle $a,b\in G$ ist.

Das neutrale Element einer Gruppe bezeichnet man auch als *Einselement* und schreibt $e = 1\in G$. Für die Verknüpfung werden oft auch andere Symbole benutzt, je nach Kontext schreibt man statt $a\circ b$ auch $a\cdot b$, $a\bullet b$ oder einfach ab. Nur im Fall abelscher Gruppen wird auch die additive Notation $+$ verwendet, in diesem Fall wird das neutrale Element mit $0\in G$ bezeichnet und heißt *Nullelement*.

Beispiel 1.2. Erinnern wir uns an einige Beispiele aus der linearen Algebra:

a) Die additiven Gruppen $(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{R},+),\dots$ sind abelsch.

b) Die multiplikativen Gruppen $\mathbb{Q}^\times = (\mathbb{Q}\setminus\{0\},\cdot)$, $\mathbb{Q}^\times_{>0} = (\mathbb{Q}_{>0},\cdot),\dots$ sind abelsch.

c) Die *allgemeine lineare Gruppe*

$$\mathrm{GL}_n(\mathbb{Q}) \;=\; \{A \in \mathrm{Mat}_{n\times n}(\mathbb{Q}) \mid \det(A) \neq 0\}$$

mit der Matrizenmultiplikation als Verknüpfung ist für $n > 1$ nicht abelsch.

d) Die *symmetrische Gruppe*

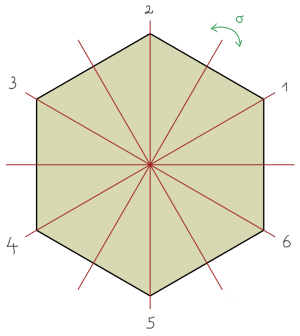
$$\mathfrak{S}_n \;:=\; \{\text{Bijektive Abbildungen } \sigma : \{1,\dots,n\} \to \{1,\dots,n\}\}$$

mit der Verkettung als Verknüpfung ist für $n > 2$ nicht abelsch. Ihre Elemente heißen *Permutationen* und werden oft als Wertetabelle in Klammern angegeben, d.h. wir schreiben

$$\sigma \;=\; \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ i_1 & i_2 & i_3 & \cdots & i_n \end{pmatrix} \;\in\; \mathfrak{S}_n$$

für die durch $\sigma(k) = i_k$ gegebene Permutation. Eine effizientere Notation für Permutationen werden wir im Abschnitt 6 mit der Zykelnotation kennenlernen.

e) Die *Diedergruppe* D_n der Symmetrien eines regelmäßigen n-Ecks ist für $n > 2$ nicht abelsch. Sie besteht aus genau $2n$ Elementen, den Drehungen um Vielfache von $2\pi/n$ und den Spiegelungen an den Symmetrieachsen:



Eine nützliche allgemeine Konstruktion von neuen Gruppen aus bereits bekannten Gruppen sind Produkte. Die Indexmenge muß dabei nicht endlich sein:

Definition 1.3. Sei I eine Indexmenge, und für jedes $i \in I$ sei eine Gruppe $(G_i, \circ_i)$ gegeben. Unter dem *Produkt* dieser Familie versteht man die Menge

$$\prod_{i\in I} G_i$$

mit der komponentenweisen Verknüpfung

$$(g_i)_{i\in I} \circ (h_i)_{i\in I} \;:=\; (g_i \circ_i h_i)_{i\in I}.$$

Aus der Definition folgt direkt, dass diese Verknüpfung das Produkt wieder zu einer Gruppe macht. Im Fall endlicher Indexmengen $I = \{1,\dots,n\}$ schreibt man dieses Produkt auch kurz

$$\prod_{i=1}^{n} G_i \;=\; G_1 \times \cdots \times G_n$$

und lässt hierbei die Verknüpfung in der Notation gerne weg, wenn keine Gefahr von Mißverständnissen besteht.

Viele interessante Gruppen erhält man aus einer gegebenen größeren Gruppe durch Einschränken der Verknüpfung auf eine geeignete Teilmenge. Dies führt auf den folgenden Begriff:

Definition 1.4. Eine *Untergruppe* einer Gruppe $(G,\circ)$ ist eine Teilmenge $H \subseteq G$ mit den folgenden beiden Eigenschaften:

a) Es ist $e \in H$.

b) Für alle $g,h \in H$ ist $g \circ h \in H$ und $g^{-1} \in H$.

Wie wir in der linearen Algebra gesehen haben, lassen sich diese zwei Bedingungen auch kürzer fassen in der folgenden äquivalenten Form:

a) Es ist $H \neq \varnothing$.

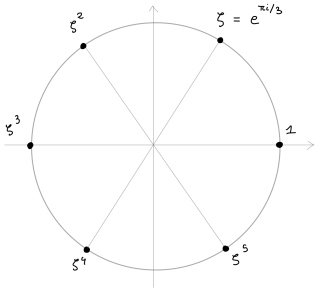
b) Es ist $g \circ h^{-1} \in H$ für alle $g,h \in H$.

Wir schreiben auch kurz $H \leq G$, wenn H eine Untergruppe von G ist.

Beispiel 1.5. Die multiplikative Gruppe $\mathbb{C}^\times$ enthält für jedes $n \in \mathbb{N}$ die Untergruppe der n-ten Einheitswurzeln

$$\mu_n(\mathbb{C}) \;=\; \{z \in \mathbb{C}^\times \mid z^n = 1\} \;\leq\; \mathbb{C}^\times$$

In Polarkoordinaten sieht man, dass ihre Elemente genau die Potenzen von $\exp(2\pi i/n)$ sind:



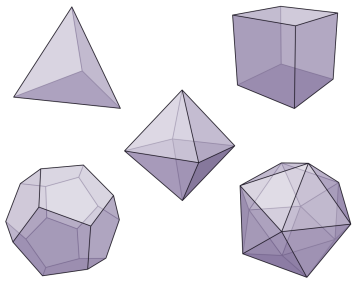
Beispiel 1.6. Die allgemeine lineare Gruppe $\mathrm{GL}_n(\mathbb{R})$ enthält die spezielle lineare Gruppe

$$\mathrm{SL}_n(\mathbb{R}) \;:=\; \{A \in \mathrm{GL}_n(\mathbb{R}) \mid \det(A) = 1\} \;\leq\; \mathrm{GL}_n(\mathbb{R}).$$

Diese enthält die spezielle orthogonale Gruppe

$$\mathrm{SO}_n(\mathbb{R}) \;:=\; \{A \in \mathrm{SL}_n(\mathbb{R}) \mid A^{\mathsf{t}} \cdot A = \mathbf{1}\} \;\leq\; \mathrm{SL}_n(\mathbb{R}),$$

deren Elemente genau die Drehungen um den Ursprung sind. Für $n = 3$ enthält sie als endliche Untergruppen die Gruppen aller Drehungen, welche ein reguläres Polyeder (auch bekannt als Platonische Körper) in sich abbilden. Das folgende Bild aus `https://commons.wikimedia.org/w/index.php?curid=77742585` zeigt die fünf regulären Polyeder:



Ein Satz von Felix Klein besagt, dass jede endliche Untergruppe von $\mathrm{SO}_3(\mathbb{C})$ die Symmetriegruppe eines regulären Polyeders ist oder die abelsche Untergruppe der Drehungen um Vielfache eines festen Winkels um eine feste Achse. Der Beweis ist elementar. Für $n \geq 4$ wird die Situation allerdings deutlich komplizierter!

Der Schnitt zweier Untergruppen ist wieder eine Untergruppe. Allgemeiner gilt für beliebige Indexmengen:

Lemma 1.7. *Sei G eine Gruppe. Für jede Familie $(H_i)_{i\in I}$ von Untergruppen $H_i \leq G$ ist der Schnitt*

$$H \;:=\; \bigcap_{i\in I} H_i \;\leq\; G \quad \text{eine Untergruppe.}$$

Beweis. Folgt direkt aus der Definition. □

Korollar 1.8. *Sei G eine Gruppe. Für jede Teilmenge S existiert dann genau eine Untergruppe*

$$\langle S \rangle \;\leq\; G$$

mit folgenden beiden Eigenschaften:

a) Es ist $S \subseteq \langle S \rangle$.

b) Für jede Untergruppe $H \leq G$ mit $S \subseteq H$ gilt auch $\langle S \rangle \subseteq H$.

Beweis. Sei $(G_i)_{i\in I}$ die Familie aller Untergruppen von G, welche die Teilmenge S enthalten. Nach dem vorigen Lemma ist

$$\langle S\rangle \;:=\; \bigcap_{i\in I} G_i \;\leq\; G$$

eine Untergruppe, und diese hat per Konstruktion die gewünschte Eigenschaft. Wir können die gesuchte Untergruppe natürlich direkt hinschreiben: Man prüft leicht nach, dass

$$\langle S\rangle \;=\; \Big\{ \prod_{i=1}^{k} s_i \;\mid\; k\in\mathbb{N}_0,\, s_i\in S\cup S^- \Big\}.$$

für die Menge $S^- := \{s^{-1} \mid s\in S\}$ ist. □

Ein besonders wichtiger Spezialfall ist derjenige von Gruppen, welche sich mit endlich vielen Elementen erzeugen lassen:

Definition 1.9. Eine Gruppe G heißt

a) *endlich erzeugt*, wenn es $g_1,\dots,g_n\in G$ gibt mit $G=\langle\{g_1,\dots,g_n\}\rangle$. Man schreibt dann kurz

$$G \;=\; \langle g_1,\dots,g_n\rangle$$

und sagt, die Gruppe G werde von den Elementen $g_1,\dots,g_n$ erzeugt.

b) *zyklisch*, wenn ein Element $g\in G$ existiert mit $G=\langle g\rangle$. Dann besteht G genau aus den Potenzen von g, die sich rekursiv wie folgt definieren lassen:

$$g^n \;:=\; \begin{cases} 1 & \text{für } n=0,\\ g\cdot g^{n-1} & \text{für } n>0,\\ g^{-1}\cdot g^{n+1} & \text{für } n<0. \end{cases}$$

Im Fall additiv geschriebener abelscher Gruppen $(G,+)$ verwenden wir statt der obigen Exponentenschreibweise g^n die in diesem Fall passendere Notation $n\cdot g$.

Beispiel 1.10. Es gilt:

a) Die Gruppe $\mu_n(\mathbb{C})\subset\mathbb{C}$ ist zyklisch, erzeugt von $g=\exp(2\pi i/n)$.

b) Die additive Gruppe $(\mathbb{Z},+)$ ist zyklisch, additiv erzeugt von $g=1$.

c) Jede Untergruppe von $(\mathbb{Z},+)$ ist zyklisch. Genauer haben wir uns in der linearen Algebra durch Division mit Rest überlegt, dass jede solche Untergruppe von der Form

$$H \;=\; m\mathbb{Z} \;:=\; \{m\cdot a \mid a\in\mathbb{Z}\} \;\leq\; \mathbb{Z} \quad\text{für}\quad m \;:=\; \begin{cases} 0 & \text{für } H=\{0\},\\ \min H\cap\mathbb{N} & \text{für } H\neq\{0\}, \end{cases}$$

ist. Man beachte unsere Konvention, dass $0\notin\mathbb{N}$ ist.

d) Die Definition einer zyklischen Gruppen sagt, dass diese von einem *geeigneten* Element erzeugt wird. Nicht jedes Element ist ein Erzeuger. Zudem kann eine zyklische Gruppe durchaus ein Erzeugendensystem mit mehr als einem Element haben, in dem kein Element ersatzlos weggelassen werden darf: Man denke an die Darstellung

$$m\mathbb{Z} \;=\; \langle a,b\rangle \quad \text{für alle } a,b\in\mathbb{Z} \text{ mit } \mathrm{ggT}(a,b)=m.$$

e) Die additive Gruppe $(\mathbb{Q},+)$ ist nicht endlich erzeugt: Denn angenommen, diese Gruppe wäre additiv erzeugt von Elementen $g_1,\dots,g_n\in\mathbb{Q}$. Wähle ein $N\in\mathbb{N}$ mit $N\cdot g_i\in\mathbb{Z}$ für alle i. Jedes $q\in\mathbb{Q}$ hätte in unserem Erzeugendensystem eine Darstellung

$$q \;=\; a_1g_1+\cdots+a_ng_n$$

mit $a_1,\dots,a_n\in\mathbb{Z}$. Aber dann wäre $N\cdot q\in\mathbb{Z}$ für alle $q\in\mathbb{Q}$, was absurd ist.

f) Die Diedergruppe D_n lässt sich von zwei Elementen erzeugen: Sei $\rho\in D_n$ eine Drehung um den Ursprung mit Drehwinkel $\alpha=2\pi/n$, und es bezeichne $\sigma\in D_n$ eine Spiegelung an einer um $\alpha/2$ geneigten Achse durch den Ursprung. Dann gilt

$$D_n \;=\; \langle \rho,\sigma\rangle \quad \text{mit der Relation} \quad \sigma\circ\rho\circ\sigma=\rho^{-1}.$$

Die Diedergruppe ist nicht zyklisch, da sie nicht abelsch ist. Allgemein gilt:

Lemma 1.11. *Zyklische Gruppen sind abelsch.*

Beweis. In jeder Gruppe G erhält man aus dem Assoziativgesetz per Induktion die Potenzregel

$$g^a\cdot g^b \;=\; g^{a+b} \;=\; g^b\cdot g^a$$

für alle $g\in G$ und alle Exponenten $a,b\in\mathbb{Z}$. □

Die Umkehrung des vorigen Lemmas gilt im Allgemeinen nicht, wie man bereits an dem folgenden einfachen Beispiel sieht:

Bemerkung 1.12. Die Gruppe $G=\mathbb{Z}\times\mathbb{Z}$ ist abelsch, aber nicht zyklisch.

Beweis. Die Gruppe G ist als Produkt von zwei abelschen Gruppen offensichtlich abelsch. Wäre sie zyklisch, dann wäre jedes ihrer Elemente ein Vielfaches eines festen Erzeugers $g=(a,b)$. Insbesondere gäbe es dann $m,n\in\mathbb{Z}$ mit

$$\begin{aligned}(0,1) \;&=\; m\cdot(a,b),\\ (1,0) \;&=\; n\cdot(a,b),\end{aligned}$$

was offensichtlich unmöglich ist. □

2 Gruppenhomomorphismen

Um die Struktur verschiedener Gruppen in Bezug zueinander zu setzen, betrachten wir Abbildungen, die mit der Verknüpfung kompatibel sind:

Definition 2.1. Ein *Homomorphismus* einer Gruppe $(G,\circ)$ in eine Gruppe $(H,\cdot)$ ist eine Abbildung $f : G \to H$ mit

$$f(g_1 \circ g_2) \;=\; f(g_1)\cdot f(g_2) \quad \text{für alle } g_1, g_2 \in G.$$

Ein Homomorphismus f heißt

- *Monomorphismus*, wenn er injektiv ist; wir schreiben dann $G \hookrightarrow H$.
- *Epimorphismus*, wenn er surjektiv ist; wir schreiben dann $G \twoheadrightarrow H$.
- *Isomorphismus*, wenn er bijektiv ist; wir schreiben dann $G \simeq H$.

Zwei Gruppen heißen *isomorph*, wenn es einen Isomorphismus zwischen ihnen gibt. Einen Homomorphismus $f : G \to G$ von einer Gruppe in sich selbst bezeichnet man als *Endomorphismus*, und im bijektiven Fall als *Automorphismus*. Wir schreiben

$$\begin{aligned} \mathrm{Hom}(G,H) &:= \{\text{Homomorphismen } \varphi : G \to H\}, \\ \mathrm{Aut}(G) &:= \{\text{Automorphismen } \varphi : G \to G\}, \end{aligned}$$

für die Menge aller solcher Homomorphismen bzw. Automorphismen.

Beispiel 2.2. Es gilt:

a) Für jedes feste $m \in \mathbb{Z}$ ist $f : (\mathbb{Z},+) \longrightarrow (\mathbb{Z},+), n \mapsto mn$ ein Endomorphismus; dieser ist
   - ein Monomorphismus genau für $m \neq 0$,
   - ein Automorphismus genau für $m = \pm 1$.

b) Für jedes $n \in \mathbb{Z}$ ist die Abbildung $f : \mathbb{C}^\times \longrightarrow \mathbb{C}^\times, z \mapsto z^n$ ein Endomorphismus; dieser ist
   - ein Epimorphismus genau für $n \neq 0$,
   - ein Automorphismus genau für $n = \pm 1$.

c) Für jedes $a \in \mathbb{C}$ ist die Exponentialabbildung $f : (\mathbb{R},+) \to \mathbb{C}^\times,\ x \mapsto \exp(ax)$ ein Homomorphismus; dieser ist ein Monomorphismus genau für $\mathrm{Re}(a) \neq 0$.

d) Für jede Untergruppe $U \subseteq G$ ist die Inklusion $i : U \hookrightarrow G$ ein Monomorphismus.

In der Definition von Homomorphismen $\varphi : G \to H$ haben wir nur Kompatibilität mit der Verknüpfung gefordert. Hieraus folgt die Kompatibilität mit den neutralen Elementen $e_G \in G$, $e_H \in H$ und mit Inversen:

Lemma 2.3. *Sei $\varphi : G \to H$ ein Homomorphismus. Dann gilt*

$$\varphi(e_G) = e_H \quad \textit{und} \quad \varphi(g^{-1}) = (\varphi(g))^{-1} \quad \textit{für alle } g \in G.$$

Beweis. Die erste Aussage erhält man durch Multiplikation mit $(\varphi(e_G))^{-1} \in H$ in der Gleichung

$$\begin{aligned} \varphi(e_G) &= \varphi(e_G \cdot e_G) && \text{wegen } e_G = e_G \cdot e_G \\ &= \varphi(e_G) \cdot \varphi(e_G) && \text{weil } \varphi \text{ Homomorphismus ist} \end{aligned}$$

Die zweite Aussage folgt dann aus $e_H = \varphi(e_G) = \varphi(g \cdot g^{-1}) = \varphi(g) \cdot \varphi(g^{-1})$. □

Die Verkettung von zwei Homomorphismen ist wieder ein Homomorphismus, genauer gilt:

Lemma 2.4. *Seien $f : G \to H$ und $g : H \to K$ Homomorphismen von Gruppen.*

a) Dann ist auch die Verkettung $g \circ f : G \to K$ ein Homomorphismus.

b) Ist f ein Isomorphismus, so auch die inverse Abbildung $f^{-1} : H \to G$.

Beweis. *a*) Für alle $a, b \in G$ ist

$$(g \circ f)(ab) = g(f(ab)) = g(f(a)f(b)) = g(f(a))g(f(b)) = (g \circ f)(a) \cdot (g \circ f)(b)$$

Der Beweis von *b*) ist analog (siehe Lineare Algebra). □

Korollar 2.5. *Für jede Gruppe G bildet $(\mathrm{Aut}(G), \circ)$ eine Gruppe.*

Beweis. Das neutrale Element für die Verkettung von Abbildungen ist $id_G \in \mathrm{Aut}(G)$, und nach dem vorigen Lemma liegen für $f, g \in \mathrm{Aut}(G)$ auch die Verkettung $f \circ g$ und das Inverse f^{-1} in $\mathrm{Aut}(G)$. Somit ist $\mathrm{Aut}(G)$ eine Untergruppe in der Gruppe aller bijektiven Selbstabbildungen $f : G \to G$. □

Bemerkung 2.6. Wir werden im Folgenden $\mathrm{Aut}(G)$ stets als Gruppe bezüglich der Verkettung von Abbildungen betrachten. Diese hat *nichts* zu tun mit dem für uns weniger wichtigen punktweisen Produkt von Homomorphismen: Falls H abelsch ist, bildet auch $\mathrm{Hom}(G, H)$ eine Gruppe, wobei das Produkt von $f, g \in \mathrm{Hom}(G, H)$ punktweise definiert ist durch

$$fg : \quad G \to H, \quad (fg)(x) := f(x)g(x).$$

Es ist $fg \in \mathrm{Hom}(G, H)$ wegen

$$\begin{aligned} (fg)(xy) &= f(xy)g(xy) && \text{per Definition von } fg \\ &= f(x)f(y)g(x)g(y) && \text{da } f \text{ und } g \text{ Homomorphismen sind} \\ &= f(x)g(x)f(y)g(y) && \text{wegen } f(y)g(x) = g(x)f(y) \text{ für } H \text{ abelsch} \\ &= ((fg)(x))((fg)(y)) && \text{per Definition von } fg \end{aligned}$$

Man beachte, dass dies nur für *abelsche* Gruppen H funktioniert!

Definition 2.7. Unter dem *Kern* und dem *Bild* eines Homomorphismus $f : G \to H$ versteht man die Teilmengen

$$\begin{aligned} \ker(f) &:= \{g \in G \mid f(g) = 1\} \subseteq G, \\ \operatorname{im}(f) &:= \{f(g) \in H \mid g \in G\} \subseteq H. \end{aligned}$$

Eine Folge von Homomorphismen

$$\cdots \longrightarrow G_{i-1} \xrightarrow{f_{i-1}} G_i \xrightarrow{f_i} G_{i+1} \longrightarrow \cdots$$

heißt eine *exakte Sequenz*, wenn $\ker(f_i) = \operatorname{im}(f_{i-1})$ für alle i ist.

Anschaulich mißt der Kern die Abweichung von der Injektivität, während das Bild die Surjektivität kontrolliert:

Lemma 2.8. *Sei $f : G \to H$ ein Gruppenhomomorphismus. Dann gilt:*

a) $\ker(f) \leq G$ *und* $\operatorname{im}(f) \leq H$ *sind Untergruppen.*

b) f ist ein Monomorphismus genau für $\ker(f) = \{1\}$.

c) f ist ein Epimorphismus genau für $\operatorname{im}(f) = H$.

Beweis. Folgt direkt aus den Definitionen (siehe Lineare Algebra). □

Beispiel 2.9. Es gilt:

a) Sei $m \in \mathbb{Z}$ und $f : (\mathbb{Z}, +) \to (\mathbb{Z}, +), n \mapsto mn$. Dann ist

$$\operatorname{im}(f) = m\mathbb{Z} \quad \text{und} \quad \ker(f) = \begin{cases} \{0\} & \text{für } m \neq 0, \\ \mathbb{Z} & \text{für } m = 0. \end{cases}$$

b) Für $f : \mathbb{C}^\times \to \mathbb{C}^\times, z \mapsto z^n$ mit $n \in \mathbb{N}$ ist $\operatorname{im}(f) = \mathbb{C}^\times$ und $\ker(f) = \mu_n(\mathbb{C})$.

c) Für $f : (\mathbb{R}, +) \to \mathbb{C}^\times, x \mapsto \exp(2\pi i x)$ ist $\operatorname{im}(f) = \{z \in \mathbb{C} \mid |z| = 1\}$ und $\ker(f) = \mathbb{Z}$.

Zyklische Untergruppen lassen sich einfach charakterisieren als die Bilder von Homomorphismen $(\mathbb{Z}, +) \to (G, \circ)$:

Lemma 2.10. *Sei $(G, \circ)$ eine Gruppe. Dann gilt:*

a) Für jedes $g \in G$ existiert genau ein Homomorphismus

$$\varphi_g : \quad (\mathbb{Z}, +) \longrightarrow (G, \circ) \quad \textit{mit} \quad \varphi_g(1) = g,$$

konkret ist dieser Homomorphismus gegeben durch $m \mapsto g^m$ für $m \in \mathbb{Z}$.

b) Die zyklischen Untergruppe von G sind genau die Bilder $\operatorname{im}(\varphi_g) = \langle g \rangle$ *für $g \in G$.*

Beweis. *a*) Wenn ein Homomorphismus $\varphi_g : \mathbb{Z} \to G$ mit $\varphi_g(1) = g$ existiert, dann ist dieser eindeutig, denn die Rechenregeln für Homomorphismen liefern für $m \in \mathbb{N}_0$ notwendigerweise

$$\varphi_g(m) \;=\; \varphi_g(1+\cdots+1) \;=\; \varphi_g(1)\cdot\cdots\cdot\varphi_g(1) \;=\; g\circ\cdots\circ g \;=\; g^m$$

und hierdurch ist auch $\varphi_g(-m) = (\varphi_g(m))^{-1} = (g^m)^{-1} = g^{-m}$ festgelegt. Dass die hier angegebenen Formeln tatsächlich einen wohldefinierten Homomorphismus φ_g liefern, folgt ebenso. Teil *b*) gilt per Definition. □

Korollar 2.11. *Sei G eine Gruppe. Dann gibt es für jedes $g \in G$ genau ein $m \in \mathbb{N}_0$ mit*

$$g^k \;=\; 1 \quad\Longleftrightarrow\quad k \;\in\; m\mathbb{Z}.$$

Beweis. Der Kern $\ker(\varphi_g)$ ist eine zyklische Untergruppe von $(\mathbb{Z},+)$ und hat somit die Form $m\mathbb{Z}$ für ein eindeutig bestimmtes $m \in \mathbb{N}_0$. □

Die im obigen Korollar auftretende Zahl m hängt zusammen mit der Ordnung der von g erzeugten zyklischen Gruppe:

Definition 2.12. Die *Ordnung* einer Gruppe G ist die Anzahl $|G| \in \mathbb{N} \cup \{\infty\}$ ihrer Elemente. Für $g \in G$ nennen wir

$$\operatorname{ord}(g) \;:=\; |\langle g\rangle| \;=\; \begin{cases} m & \text{falls } \ker(\varphi_g) = m\mathbb{Z} \neq 0, \\ \infty & \text{falls } \ker(\varphi_g) = 0 \end{cases}$$

die *Ordnung* des Gruppenelementes $g \in G$.

Beispiel 2.13. Für die Elemente $g \in D_n$ der Diedergruppe gilt

$$\operatorname{ord}(g) \;=\; \begin{cases} n/\operatorname{ggT}(a,n) & \text{falls } g \text{ eine Drehung um den Winkel } 2\pi a/n \text{ ist,} \\ 2 & \text{falls } g \text{ eine Spiegelung an einer Symmetrieachse ist.} \end{cases}$$

Denn für Spiegelungen ist das klar, für Drehungen beachte man, dass $k \cdot a/n \in \mathbb{Z}$ ist genau für $ak \in n\mathbb{Z}$. Die Menge aller Drehungen in D_n ist eine zyklische Untergruppe erzeugt von der Drehung ρ um den Ursprung mit Drehwinkel $2\pi/n$, sie ist das Bild des Homomorphismus

$$\varphi_\rho : \quad \mathbb{Z} \;\longrightarrow\; D_n, \quad k \;\mapsto\; \rho^k \quad \text{mit} \quad \ker(\varphi_\rho) \;=\; a\mathbb{Z}.$$

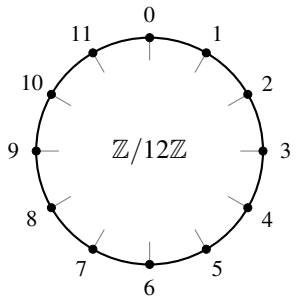
Jede Spiegelung erzeugt ferner eine Untergruppe von D_n isomorph zu $\{\pm 1\}$.

3 Nebenklassen

In der linearen Algebra haben wir für $n \in \mathbb{N}$ die Menge $\mathbb{Z}/n\mathbb{Z} = \{[0],[1],\ldots,[n-1]\}$ der Restklassen

$$[g] := g+H := \{g+h \mid h \in H\} \quad \text{bezüglich der Untergruppe} \quad H := n\mathbb{Z} \leq \mathbb{Z}$$

zu einer abelschen Gruppe gemacht mit der Addition $[a]+[b] := [a+b]$. Wir kennen das vom Rechnen mit Uhrzeiten:



$$[9]+[4]=[1] \quad \text{in} \quad \mathbb{Z}/12\mathbb{Z}$$

Für einen analogen Begriff von Restklassen in beliebigen Gruppen ist zu beachten, dass es im Fall nichtabelscher Gruppen Restklassen "von links" und "von rechts" gibt, die sorgfältig zu unterscheiden sind:

Definition 3.1. Sei G eine Gruppe. Eine *Linksnebenklasse* einer Untergruppe $H \leq G$ ist eine Teilmenge der Form

$$gH := \{gh \mid h \in H\} \subseteq G.$$

Analog werden wir später *Rechtsnebenklassen* $Hg := \{hg \mid h \in H\} \subseteq G$ betrachten.

Lemma 3.2. *Sei G eine Gruppe und $H \leq G$ eine Untergruppe. Für $a,b \in G$ sind dann äquivalent:*

a) $aH \cap bH \neq \varnothing$.

b) $aH = bH$.

c) $a \in bH$.

d) $b^{-1}a \in H$.

Beweis. Falls $a)$ gilt, gibt es $h_1, h_2 \in H$ mit $ah_1 = bh_2 \in aH \cap bH$. Wegen $h_iH = H$ folgt dann

$$aH = ah_1H = bh_2H = bH$$

und somit gilt $b)$. Aus $b)$ folgt $a = a \cdot 1 \in aH = bH$ und damit $c)$. Aus $c)$ folgt $d)$ durch Multiplikation mit b^{-1} von links. Und wenn $d)$ gilt, ist $h := b^{-1}a \in H$, woraus man $bh \in aH$ und somit $a)$ erhält. □

Korollar 3.3. *Sei G eine Gruppe und $H \leq G$ eine Untergruppe. Dann ist G eine disjunkte Vereinigung*

$$G = \bigsqcup_{g \in R} gH$$

von Linksnebenklassen für eine geeignete Teilmenge $R \subseteq G$.

Beweis. Offensichtlich ist G die Vereinigung von Linksnebenklassen. Nach dem vorigen Lemma sind diese paarweise disjunkt; wenn wir aus jeder Linksnebenklasse ein Element wählen, erhalten wir ein $R \subseteq G$ mit der gewünschten Eigenschaft. □

Definition 3.4. Die Elemente einer Nebenklasse heißen ihre *Repräsentanten*. Eine Teilmenge $R \subseteq G$ mit der Eigenschaft aus dem vorigen Korollar nennen wir daher ein *Repräsentantensystem* für die Linksnebenklassen. Wir bezeichnen die Menge aller Linksnebenklassen mit

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

Ein Repräsentantensystem für die Linksnebenklassen ist also eine Teilmenge $R \subseteq G$, auf der sich die Abbildung

$$G \longrightarrow G/H, \quad g \mapsto gH$$

sich zu einer Bijektion $R \longrightarrow G/H$ einschränkt. Der *Index von H in G* ist definiert als die Kardinalität

$$[G:H] := |G/H| = |R| \in \mathbb{N} \cup \{\infty\},$$

also die Anzahl der Nebenklassen. Dies ist besonders nützlich für endliche Gruppen:

Satz 3.5 (Lagrange). *Sei G eine endliche Gruppe und $H \leq G$ eine Untergruppe, dann gilt*

$$|G| = [G:H] \cdot |H|.$$

Beweis. Für jede Linksnebenklasse $gH \subseteq G$ ist die Abbildung $H \to gH, h \mapsto gh$ bijektiv, denn die Umkehrabbildung dazu erhält man durch Multiplikation mit dem Inversen $g^{-1} \in G$. Somit besitzt jede Linsksnebenklasse genau $|H|$ Elemente. Nach dem vorigen Lemma ist andererseits G die disjunkte Vereinigung von genau $[G:H]$ solchen Linksnebenklassen. □

Korollar 3.6. *Sei G eine endliche Gruppe.*

a) Für jede Untergruppe $H \leq G$ ist die Ordnung $|H|$ ein Teiler von $|G|$.

b) Insbesondere gilt der sogenannte kleine Fermat'sche Satz: Für jedes $g \in G$ ist die Ordnung $\operatorname{ord}(g)$ *ein Teiler der Gruppenordnung $|G|$.*

Beweis. $a)$ folgt direkt aus dem Satz von Lagrange, und $b)$ erhält man als Spezialfall für die zyklische Untergruppe $H = \langle g \rangle \leq G$. □

Korollar 3.7. *Jede Gruppe von Primzahlordnung ist zyklisch.*

Beweis. Sei G eine endliche Gruppe, deren Ordnung $p = |G|$ eine Primzahl ist; nach dem vorigen Korollar ist $\operatorname{ord}(g) \in \{1, p\}$ für jedes $g \in G$. Der Fall $\operatorname{ord}(g) = 1$ tritt offenbar nur für $g = 1$ auf. Für jedes von Einselement verschiedene Element g gilt somit

$$|\langle g \rangle| = \operatorname{ord}(g) = p = |G|$$

und folglich ist $\langle g \rangle = G$, d.h. die Gruppe G wird von g erzeugt. □

Wir haben uns bisher auf Linksnebenklassen konzentriert. Natürlich hätte man dasselbe auch für Rechtsnebenklassen machen können! Wir bezeichnen mit $H \setminus G$ die Menge der Rechtsnebenklassen (nicht zu verwechseln mit dem Komplement von Mengen). Die Abbildung $G \to G, g \mapsto g^{-1}$ induziert dann eine Bijektion

$$G/H \longrightarrow H \setminus G, \quad gH \mapsto Hg^{-1}$$

zwischen der Menge der Linksnebenklassen und der der Rechtsnebenklassen. Die Rechtsnebenklasse Hg^{-1} hängt nur von der Linksnebenklasse gH und nicht von dem konkret gewählten Repräsentanten $g \in G$ für diese Nebenklasse ab: Für $h \in H$ ist

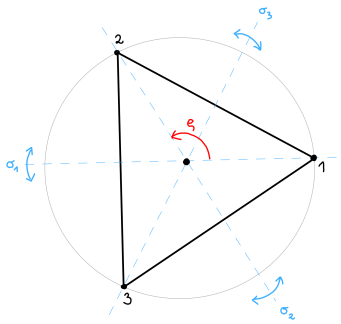
$$H(gh)^{-1} = Hh^{-1}g^{-1} = Hg^{-1}$$

Ohne die Inversion der Repräsentanten wäre dies nicht der Fall. Die Rechnung zeigt auch: Ist $R \subseteq G$ ein Repräsentantensystem für die Linksnebenklassen, dann bildet das System der dazu Inversen $S := \{s = r^{-1} \mid r \in R\}$ ein Repräsentantensystem für die Rechtsnebenklassen. Wir haben also zwei Partitionen

$$G = \bigsqcup_{r \in R} rH = \bigsqcup_{s \in S} Hs$$

Im Allgemeinen handelt es sich hierbei um echt verschiedene Partitionen, nicht jede Rechtsnebenklasse ist eine Linksnebenklasse:

Beispiel 3.8. Sei $G = D_3$. Sei ρ eine Drehung um $2\pi/3$, und seien $\sigma_1, \sigma_2, \sigma_3$ die drei in der folgenden Skizze gezeigten Spiegelungen:



Für die von der Spiegelung an der x-Achse erzeugte Untergruppe $H = \{1, \sigma_1\}$ sind die Links- bzw. Rechtsnebenklassen:

$$\begin{aligned} 1 \cdot H &= \{1, \sigma_1\} & H \cdot 1 &= \{1, \sigma_1\} \\ \rho \cdot H &= \{\rho, \sigma_3\} & H \cdot \rho &= \{\rho, \sigma_2\} \\ \rho^2 \cdot H &= \{\rho^2, \sigma_2\} & H \cdot \rho^2 &= \{\rho^2, \sigma_3\} \end{aligned}$$

Hier ist $1 \cdot H = H \cdot 1$ die einzige Linksnebenklasse, die auch Rechtsnebenklasse ist.

4 Normalteiler und Quotienten

Die Unterscheidung zwischen Links- und Rechtsnebenklassen ist lästig. In manchen Fällen sieht die Situation besser aus:

Definition 4.1. Sei G eine Gruppe. Eine Untergruppe $N \leq G$ heißt ein *Normalteiler* von G, wenn die dazu gehörigen Links- und Rechtsnebenklassen übereinstimmen, d.h. wenn gilt:

$$gN = Ng \quad \text{für alle} \quad g \in G.$$

Wir schreiben in diesem Fall auch $N \trianglelefteq G$. Die obige Eigenschaft ist äquivalent zu der Bedingung

$$gNg^{-1} = N \quad \text{für alle} \quad g \in G.$$

Die Normalteiler sind also genau diejenigen Untergruppen, die stabil sind unter der Konjugationsabbildung

$$c_g : \quad G \longrightarrow G, \quad x \mapsto gxg^{-1}$$

für alle $g \in G$. Man beachte, dass $c_g \in \mathrm{Aut}(G)$ ist (Übungsaufgabe).

Bemerkung 4.2. Unsere Konvention, bei der Konjugation das Inverse rechts zu schreiben, ist kompatibel mit der Verkettung von Automorphismen in dem Sinne, dass

$$c_{g \circ h} = c_g \circ c_h \quad \text{für alle} \quad g,h \in G$$

ist. In manchen Situationen ist auch die Exponentialnotation $x^g := g^{-1}xg$ für $x, g \in G$ praktisch, hier wählt man das Inverse üblicherweise auf der linken Seite, damit die intuitive Regel $x^{gh} = (x^g)^h$ für alle $x, g \in G$ gilt.

Beispiel 4.3. Es gilt:

a) Für G abelsch ist jede Untergruppe $N \leq G$ ein Normalteiler.

b) In der Diedergruppe $G = D_n$ bilden die Drehungen um Vielfache von $2\pi/n$ einen Normalteiler

$$N = \{1, \rho, \rho^2, \ldots, \rho^{n-1}\} \trianglelefteq D_n.$$

Genauer gilt

$$\tau \circ \rho^i \circ \tau^{-1} = \begin{cases} \rho^i \in N & \text{falls } \tau \text{ eine Drehung ist,} \\ \rho^{-i} \in N & \text{falls } \tau \text{ eine Spiegelung ist.} \end{cases}$$

c) Für $G = \mathrm{GL}_n(\mathbb{R})$ beschreibt die Konjugation mit $g \in G$ einen Basiswechsel für Abbildungsmatrizen. Nach linearer Algebra haben ähnliche Matrizen dieselbe Determinante, denn $\det(ghg^{-1}) = \det(g)\det(h)\det(g)^{-1} = \det(h)$. Wir erhalten also

$$\mathrm{SL}_n(\mathbb{R}) = \{h \in \mathrm{GL}_n(\mathbb{R}) \mid \det(h) = 1\} \trianglelefteq \mathrm{GL}_n(\mathbb{R}).$$

Eine analoge Rechnung zeigt, dass Kerne von beliebigen Gruppenhomomorphismen immer Normalteiler sind. Genauer gilt:

Proposition 4.4. *Sei G eine Gruppe. Für Untergruppen $N \leq G$ sind äquivalent:*

a) $N = \ker(\varphi)$ ist der Kern eines Homomorphismus $\varphi : G \to H$ in eine Gruppe H.

b) $N \trianglelefteq G$ ist ein Normalteiler.

c) Die Menge G/N der Linksnebenklassen trägt eine Gruppenstruktur, sodass die Abbildung

$$p: \quad G \longrightarrow G/N, \quad g \mapsto gN \quad \text{ein Homomorphismus ist.}$$

Beweis. Wenn $N = \ker(\varphi)$ ist, gilt

$$\begin{aligned}
x \in N &\iff \varphi(x) = 1 && \text{per Definition von } N = \ker(\varphi) \\
&\iff h\varphi(x)h^{-1} = 1 && \text{für beliebiges } h \in H \\
&\iff \varphi(gxg^{-1}) = 1 && \text{wenn man speziell } h = \varphi(g) \text{ wählt} \\
&\iff gxg^{-1} \in N && \text{per Definition von } N = \ker(\varphi)
\end{aligned}$$

und es folgt $N \trianglelefteq G$. Wenn letzteres gilt, dann wird auf der Nebenklassenmenge G/N durch

$$*: \quad G/N \times G/N \longrightarrow G/N, \quad aN * bN := abN$$

eine Verknüpfung wohldefiniert: Denn seien $a, a' \in G$ mit $aN = a'N$ und $b, b' \in G$ mit $b'N = bN$ verschiedene Repräsentanten von denselben Linksnebenklassen, dann folgt

$$\begin{aligned}
a'b'N &= a'bN && \text{wegen } b'N = bN \\
&= a'Nb && \text{wegen } bN = Nb \\
&= aNb && \text{wegen } a'N = aN \\
&= abN && \text{wegen } Nb = bN
\end{aligned}$$

und somit $aN * bN = a'N * b'N$. Also ist die Verknüpfung $* : G/N \times G/N \to G/N$ wohldefiniert. Dass diese Verknüpfung eine Gruppenstruktur definiert, folgt direkt aus den Gruppenaxiomen für G. Ebenso ist klar, dass mit dieser (und nur dieser) Wahl der Verknüpfung die Abbildung

$$p: \quad G \longrightarrow G/N, \quad g \mapsto gN$$

ein Homomorphismus wird. Ist umgekehrt letzteres der Fall, so ist $N = \ker(p)$ als Kern eines Homomorphismus erkannt. □

Für Normalteiler $N \trianglelefteq G$ nennen wir die Gruppe G/N den *Quotient* von G modulo dem Normalteiler, und der Epimorphismus

$$p: \quad G \twoheadrightarrow G/N, \quad g \mapsto gN$$

heißt die *Quotientenabbildung*. Jeden Homomorphismus lässt sich zerlegen in eine Quotientenabbildung und einen Isomorphismus auf sein Bild:

Satz 4.5 (Homomorphiesatz). *Jeder Homomorphismus $f : G \to H$ von Gruppen faktorisiert über einen Isomorphismus*

$$\bar{f}: \quad G/\ker(f) \xrightarrow{\sim} \operatorname{im}(f)$$

Beweis. Sei $K = \ker(f)$. Für jedes Element $g \in G$ hängt dann der Wert $f(g) \in \operatorname{im}(f)$ nur von der Nebenklasse $gK \in G/K$ ab, denn für $k \in K$ ist per Definition $f(k) = e_H$ und somit

$$f(gk) \;=\; f(g) \cdot f(k) \;=\; f(g) \cdot e_H \;=\; f(g).$$

Wir erhalten somit eine wohldefinierte Abbildung $\bar{f} : G/K \to \operatorname{im}(f), gK \mapsto f(g)$, sodass das Diagramm

$$\begin{array}{ccc} G & \xrightarrow{\quad f \quad} & H \\ {\scriptstyle p}\big\downarrow & & \big\uparrow{\scriptstyle i} \\ G/K & \xrightarrow{\exists!\bar{f}} & \operatorname{im}(f) \end{array}$$

kommutiert. Hierbei bezeichnet p die Quotientenabbildung modulo dem Kern und i die Inklusion des Bildes. Mit f ist auch $\bar{f}$ ein Homomorphismus, und

$$\begin{aligned} \operatorname{im}(\bar{f}) \;&=\; \{\bar{f}(gK) \mid gK \in G/K\} \\ &=\; \{f(g) \mid g \in G\} = \operatorname{im}(f), \\ \ker(\bar{f}) \;&=\; \{gK \in G/K \mid \bar{f}(gK) = e_H\} \\ &=\; \{gK \in G/K \mid f(g) = e_H\} \\ &=\; \{gK \in G/K \mid g \in \ker(f) = K\} \;=\; \{e_{G/K}\}. \end{aligned}$$

Somit ist $\bar{f} : G/K \to \operatorname{im}(f)$ ein Isomorphismus. □

Beispiel 4.6. Es gilt:

a) Sei G eine zyklische Gruppe, erzeugt von einem Element $g \in G$. Dann induziert der Homomorphismus $f : (\mathbb{Z}, +) \longrightarrow G, m \mapsto g^m$ einen Isomorphismus

$$\mathbb{Z}/n\mathbb{Z} \xrightarrow{\sim} G \quad \text{mit} \quad n \;=\; \begin{cases} 0 & \text{für } \operatorname{ord}(g) = \infty, \\ \operatorname{ord}(g) & \text{sonst.} \end{cases}$$

Slogan: Jede zyklische Gruppe ist isomorph zu $\mathbb{Z}/n\mathbb{Z}$ für ein eindeutiges $n \in \mathbb{N}_0$.

b) Für $n \in \mathbb{N}$ induzieren der Homomorphismus $\det : \mathrm{GL}_n(\mathbb{R}) \longrightarrow \mathbb{R}^\times$ und seine Einschränkung auf die orthogonale Gruppe Isomorphismen

$$\mathrm{GL}_n(\mathbb{R})/\mathrm{SL}_n(\mathbb{R}) \;\simeq\; \mathbb{R}^\times \quad \text{und} \quad \mathrm{O}_n(\mathbb{R})/\mathrm{SO}_n(\mathbb{R}) \;\simeq\; \{\pm 1\}.$$

c) In der linearen Algebra haben wir gezeigt, dass das Signum von Permutationen ein Homomorphismus

$$sgn: \quad \mathfrak{S}_n \longrightarrow \{\pm 1\}, \quad \sigma \mapsto sgn(\sigma) := \prod_{i<j} \frac{\sigma(i)-\sigma(j)}{i-j}$$

ist. Die *alternierende Gruppe* ist somit ein Normalteiler

$$\mathfrak{A}_n := \ker(sgn) \trianglelefteq \mathfrak{S}_n \quad \text{mit Quotient} \quad \mathfrak{S}_n/\mathfrak{A}_n \simeq \{\pm 1\}.$$

Eine einfache, aber oft vorkommende Folgerung aus dem Homomorphiesatz sind die beiden Isomorphiesätze:

Korollar 4.7 (Isomorphiesätze). *Sei G eine Gruppe.*

a) Erster Isomorphiesatz: Für Normalteiler $N \trianglelefteq G$ und jede Untergruppe $H \leq G$ ist auch

$$HN := \{ hn \in G \mid h \in H, n \in N \} \leq G$$

eine Untergruppe, und es gilt:

- $N \trianglelefteq HN$,
- $H \cap N \trianglelefteq H$,
- $H/H \cap N \simeq HN/N$ *("Erweiterungsregel").*

b) Zweiter Isomorphiesatz: Seien $N, H \trianglelefteq G$ zwei Normalteiler, und sei $N \subseteq H$. Dann folgt

- $N \trianglelefteq H$,
- $H/N \trianglelefteq G/N$,
- $G/H \simeq (G/N)/(H/N)$ *("Kürzungsregel").*

Beweis. $a)$ Zunächst ist $HN \leq G$ eine Untergruppe, denn für $h_1, h_2 \in H$, $n_1, n_2 \in N$ gilt

$$(h_1 n_1) \cdot (h_2 n_2)^{-1} = h_1 n_1 n_2^{-1} h_2^{-1} = \underbrace{h_1 h_2^{-1}}_{\in H} \cdot \underbrace{h_2 \cdot n_1 n_2^{-1} \cdot h_2^{-1}}_{\in h_2 N h_2^{-1} = N} \in HN$$

weil $H \leq G$ eine Untergruppe und $N \trianglelefteq G$ ist. Dass $N \trianglelefteq HN$ und $H \cap N \trianglelefteq H$ ist, folgt direkt aus den Definitionen. Um die Erweiterungsregel zu erhalten, wenden wir den Homomorphiesatz an auf den aus der Inklusion und der Quotientenabbildung zusammengesetzten Homomorphismus

$$f: \quad H \hookrightarrow HN \twoheadrightarrow HN/N, \quad h \mapsto hN.$$

Dieser ist offenbar surjektiv mit $\ker(f) = H \cap N$, somit folgt die Behauptung.

b) Dass $N \trianglelefteq H$ und $H/N \trianglelefteq G/N$ gilt, folgt direkt aus den Definitionen. Um die Kürzungsregel zu erhalten, wenden wir den Homomorphiesatz an auf den aus den folgenden zwei Quotientenabbildungen zusammengesetzten Homomorphismus

$$f: \quad G \twoheadrightarrow G/N \twoheadrightarrow (G/N)/(H/N).$$

Dieser ist offenbar surjektiv mit $\ker(f) = H$, somit folgt die Behauptung. □

Beispiel 4.8. Es gilt:

a) Ist G eine endliche Gruppe und $N \trianglelefteq G$, dann gilt für $H \leq G$ nach dem ersten Isomorphiesatz

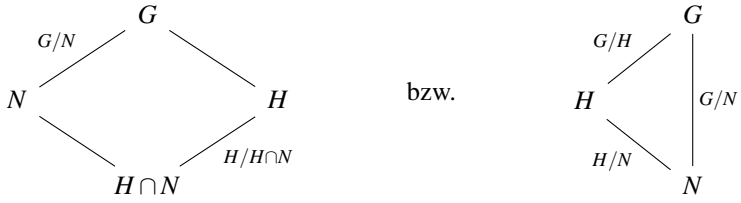
$$|H| \cdot |N| \;=\; |H \cap N| \cdot |HN|.$$

b) Für $n \in \mathbb{N}$ zeigt der erste Isomorphiesatz

$$\mathrm{SL}_n(\mathbb{R})\mathrm{O}_n(\mathbb{R})/\mathrm{SL}_n(\mathbb{R}) \simeq \mathrm{O}_n(\mathbb{R})/\mathrm{SL}_n(\mathbb{R}) \cap \mathrm{O}_n(\mathbb{R}) \simeq \mathrm{O}_n(\mathbb{R})/\mathrm{SO}_n(\mathbb{R}) \simeq \{\pm 1\}$$

c) Für $m, n \in \mathbb{N}$, $m \mid n$ zeigt der zweite Isomorphiesatz $\mathbb{Z}/m\mathbb{Z} \simeq (\mathbb{Z}/n\mathbb{Z})/(m\mathbb{Z}/n\mathbb{Z})$.

Um die Inklusionsrelationen zwischen diversen Untergruppen einer gegebenen Gruppe übersichtlicher darzustellen, kann man ein sogenanntes *Hasse-Diagramm* benutzen. Hierunter versteht man den Graphen der Inklusionsrelation: Die Ecken des Graphen entsprechen den Untergruppen, und für jede Inklusion von Gruppen wird eine Kante zwischen den entsprechenden Ecken eingezeichnet, wobei man die größere der beiden Gruppen jeweils weiter oben im Diagramm anordnet. Im Fall normaler Untergruppen schreibt man die entsprechende Quotientengruppe neben das zugehörige Inklusionssymbol. Die Situation in den beiden Isomorphiesätzen wird dann durch die Hasse-Diagramme



wiedergegeben. Natürlich wird es im Allgemeinen noch viele weitere Untergruppen geben: Ein vollständiges Hasse-Diagramm für *alle* Untergruppen einer gegebenen Gruppe wird man nur für kleine Gruppen explizit angeben.

Mit Blick auf den Homomorphiesatz stellt sich die Frage, wie man Normalteiler in einer Gruppe am besten beschreibt. Wir haben gesehen, dass man Untergruppen

konkret durch Erzeugendensysteme angeben kann. Im Fall von Normalteilern geht es effizienter, wenn wir auch die Konjugation mit Gruppenelementen nutzen: Wenn ein Normalteiler $N \trianglelefteq G$ eine Teilmenge $S \subseteq G$ enthält, dann enthält er bereits die gesamte Menge

$$S^G := \{g^{-1}sg \in G \mid s \in S, g \in G\}$$

und somit enthält er auch die davon erzeugte Untergruppe $\langle S^G \rangle$. Wir nennen diese Untergruppe die *normale Hülle* von $S \subseteq G$.

Lemma 4.9. *Sei G eine Gruppe und $S \subseteq G$. Dann gilt:*

a) Die normale Hülle $\langle S^G \rangle \trianglelefteq G$ ist ein Normalteiler, der S enthält.

b) Für jeden anderen Normalteiler $N \trianglelefteq G$ mit $S \subseteq N$ gilt auch $\langle S^G \rangle \subseteq N$.

Beweis. Zu zeigen ist nur noch, dass die normale Hülle selber ein Normalteiler ist. Das ist aber klar: Denn die Teilmenge $S^G \subseteq G$ ist per Konstruktion stabil unter Konjugation mit beliebigen Gruppenelementen, also gilt dasselbe für die hiervon erzeugte Untergruppe $\langle S^G \rangle \leq G$, die somit ein Normalteiler ist. □

5 Präsentationen von Gruppen

Untergruppen einer gegebenen Gruppe kann man durch Erzeuger definieren: Z.B. ist die Diedergruppe

$$D_n = \langle \rho, \sigma \rangle \leq \mathrm{GL}_2(\mathbb{R})$$

die Untergruppe erzeugt von einer Drehung ρ um $2\pi/n$ und einer Spiegelung σ an einer Achse. Diese Art der Definition setzt aber eine konkrete Realisierung als Untergruppe der $\mathrm{GL}_2(\mathbb{R})$ voraus: Würden wir diese nicht kennen, so müßten wir für die Definition neben den Erzeugern der Gruppe auch die von diesen erfüllten Relationen $\sigma^2 = (\rho\sigma)^2 = 1$ angeben, da diese ohne weitere Information über die Erzeuger nicht ersichtlich sind! Wir gehen dazu formal wie folgt vor:

Definition 5.1. Sei S eine Menge von Symbolen, die wir im Folgenden als formale Variablen für Gruppenelemente ansehen. Das Symbol 1 sei in dieser Menge nicht enthalten. Unter einem *Wort* in den Variablen aus S verstehen wir einen formalen Ausdruck der Form

$$w = s_1^{m_1} s_2^{m_2} \cdots s_p^{m_p}$$

mit $s_i \in S$ und $m_i \in \mathbb{Z} \setminus \{0\}$. Das leere Wort $w = 1$ ist dabei als Spezialfall $p = 0$ erlaubt. Das Produkt von zwei Wörtern ist definiert durch Hintereinanderschreiben von formalen Ausdrücken: Für je zwei Wörter $w = s_1^{m_1} \cdots s_p^{m_p}$ und $x = t_1^{n_1} \cdots t_q^{n_q}$ setzen wir

$$wx := s_1^{m_1} \cdots s_p^{m_p} t_1^{n_1} \cdots t_q^{n_q} \quad \text{für Wörter} \quad \begin{cases} w = s_1^{m_1} \cdots s_p^{m_p} \\ x = t_1^{n_1} \cdots t_q^{n_q} \end{cases}$$

Wir bezeichnen zwei Wörter als *äquivalent*, wenn sie auseinander durch endlich viele der folgenden Transformationen hervorgehen:

- Entfernen oder Hinzufügen von Faktoren $s^0 := 1$,
- Ersetzen von $\cdots s^a s^b \cdots$ durch $\cdots s^{a+b} \cdots$ oder umgekehrt,

Dies definiert eine Äquivalenzrelation $\sim$ auf der Menge von Wörtern in S, und die Menge

$$F_S := \{\text{Wörter in den Variablen aus } S\}/\sim$$

bildet eine Gruppe mit der durch Hintereinanderschreiben von Wörtern gegebenen Verknüpfung. Wir bezeichnen diese als die *freie Gruppe* erzeugt von S.

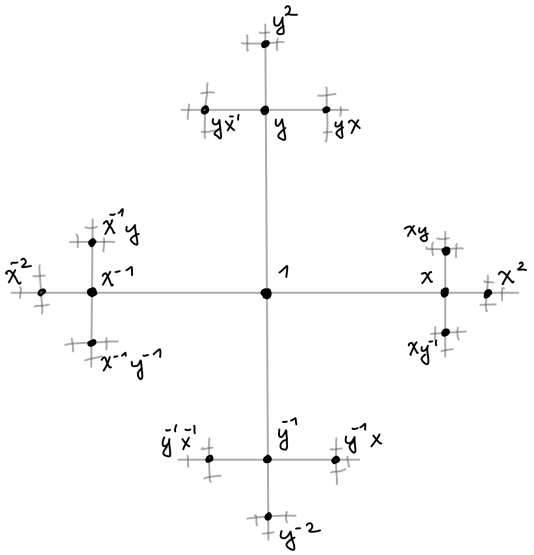
Beispiel 5.2. Es gilt:

a) Für $S = \{x\}$ ist $F_S = \{x^n \mid n \in \mathbb{Z}\} \simeq (\mathbb{Z}, +)$.

b) Für $S = \{x, y\}$ enthält F_S jedoch bereits viel mehr Elemente und ist nicht mehr abelsch, beispielsweise sind die folgenden Elemente für $a, b, c, \cdots \in \mathbb{Z} \setminus \{0\}$ alle verschieden:

$$x^a,\ y^a,\ x^a y^b,\ y^a x^b,\ x^a y^b x^c,\ y^a x^b y^c,\ \ldots \in F_S$$

Sie lassen sich in einem sogenannten *Cayley-Graph* veranschaulichen: Dieser enthält für jedes Gruppenelement genau eine Ecke, und zwei Ecken werden durch eine Kante verbunden, wenn die zugehörigen Gruppenelemente durch Links- oder Rechtsmultiplikation mit $x^{\pm 1}$ oder $y^{\pm 1}$ auseinander hervorgehen. Der Graph ist unendlich, er lässt sich rekursiv konstruieren:



Kehren wir zurück zum Fall einer beliebigen Menge S. Indem wir jedes $s \in S$ mit dem Wort s^1 identifizieren, können wir die gegebene Menge von Variablen auffassen als eine Teilmenge

$$S \subseteq F_S$$

und erhalten die folgende sogenannte *universelle Eigenschaft* freier Gruppen:

Satz 5.3. *Sei G eine Gruppe. Dann setzt jede Abbildung $f : S \longrightarrow G$ sich eindeutig fort zu einem Gruppenhomomorphismus*

$$\hat{f}: \quad F_S \longrightarrow G \quad \textit{mit} \quad \hat{f}|_S = f.$$

Beweis. Wenn eine solche Fortsetzung existiert, dann muß für Worte $w = s_1^{m_1} \cdots s_p^{m_p}$ jedenfalls

$$\hat{f}(w) = \hat{f}(s_1^{m_1} \cdots s_p^{m_p}) = (\hat{f}(s_1))^{m_1} \cdots (\hat{f}(s_p))^{m_p} = f(s_1)^{m_1} \cdots f(s_p)^{m_p}$$

gelten. Umgekehrt prüft man sofort nach, dass der Ausdruck auf der rechten Seite nur von der Äquivalenzklasse des Wortes w abhängt. Dieser Ausdruck definiert also eine Abbildung

$$\hat{f}: \quad F_S \longrightarrow G,$$

und dass diese ein Homomorphismus ist, folgt direkt aus der Definition. □

Korollar 5.4. *Sei G eine Gruppe. Für jedes Erzeugendensystem $S \subseteq G$ erhalten wir dann einen Epimorphismus*

$$F_S \twoheadrightarrow G.$$

Beweis. Wende den vorigen Satz auf die Inklusion $f : S \to G$ an. □

Jede Gruppe lässt sich nach dem Homomorphiesatz also schreiben als Quotient einer freien Gruppe. Natürlich ist eine solche Darstellung nicht eindeutig, sie läuft auf die Wahl von Erzeugern hinaus. Für den Fall endlich vieler Erzeuger und endlich vieler Relationen führen wir folgende Notation ein:

Definition 5.5. Gegeben seien

- eine endliche Menge $S = \{x_1, \ldots, x_n\}$ von formalen Variablen.
- eine endliche Menge $R = \{r_1, \ldots, r_m\} \subseteq F := F_S$ von Wörtern in den Variablen.

Unter der *Gruppe erzeugt von $x_1, \ldots, x_n$ modulo den Relationen $r_1, \ldots, r_m$* verstehen wir den Quotienten

$$\langle x_1, \ldots, x_n \mid r_1 = \cdots = r_m = 1 \rangle := F / \langle R^F \rangle$$

wobei $\langle R^F \rangle \trianglelefteq F$ die normale Hülle der Teilmenge $R \subseteq F$ bezeichne. Gruppen, die isomorph zu einem solchen Quotienten sind, heißen *endlich präsentiert*, und die Angabe von Erzeugern und Relationen bezeichnet man als eine *Präsentation* der jeweiligen Gruppe. Schauen wir uns einige Beispiele an:

Lemma 5.6. *Sei G eine zyklische Gruppe der Ordnung $|G| = n$. Dann hat G eine Präsentation*

$$G \simeq \langle x \mid x^n = 1 \rangle$$

Beweis. Denn sei $g \in G$ ein Erzeuger der Gruppe. Die universelle Eigenschaft freier Gruppen liefert einen eindeutigen Epimorphismus $p : F_{\{x\}} \twoheadrightarrow G$ mit $p(x) = g$, und sein Kern wird offenbar von $x^n \in F_{\{x\}}$ erzeugt; somit folgt die Behauptung aus dem Homomorphiesatz. Das ist natürlich nichts anderes als Beispiel 4.6(a)! □

Lemma 5.7. *Die Diedergruppe hat eine Präsentation*

$$D_n \simeq \langle x, y \mid x^n = y^2 = (yx)^2 = 1 \rangle$$

Beweis. Seien $\rho, \sigma \in D_n$ eine Drehung um den Winkel $2\pi/n$ um den Ursprung bzw. eine Spiegelung. Die universelle Eigenschaft freier Gruppen liefert uns einen eindeutigen Epimorphismus

$$p : \quad F_{\{x,y\}} \twoheadrightarrow D_n \quad \text{mit} \quad p(x) = \rho \quad \text{und} \quad p(y) = \sigma.$$

Dabei gilt:

- $p(x^n) = \rho^n = id$ und somit $x^n \in \ker(p)$,
- $p(y^2) = \sigma^2 = id$ und somit $y^2 \in \ker(p)$,
- $p((yx)^2) = (\sigma\rho)^2 = id$ und somit $(yx)^2 \in \ker(p)$.

Somit erhalten wir einen Epimorphismus

$$\langle x, y \mid x^n = y^2 = (yx)^2 = 1 \rangle \twoheadrightarrow D_n.$$

Unter Benutzung der Relationen sieht man aber leicht, dass jedes Element in der Quotientengruppe auf der linken Seite in der Form x^k oder yx^k für ein $k \in \{1, \ldots, n\}$ geschrieben werden kann. Somit besteht die Quotientengruppe aus höchstens $2n$ Elementen. Wegen $|D_n| = 2n$ besteht die Gruppe dann aus genau $2n$ Elementen und der Epimorphismus ist ein Isomorphismus. □

Bemerkung 5.8. In den obigen zwei Beispielen ist das Rechnen mit Präsentationen einfach, dies ist jedoch nicht immer so. Unter dem *Wortproblem* versteht man die Frage, wann ein Wort in einer gegebenen endlichen Präsentation einer Gruppe das neutrale Element der Gruppe repräsentiert. Die Schwierigkeit besteht darin, dass die normale Hülle der gegebenen endlich vielen Relationen im Allgemeinen riesig ist; tatsächlich gibt es endlich präsentierte Gruppen, für die das Wortproblem sich nicht durch einen in endlicher Zeit terminierenden Algorithmus beantworten lässt. Für viele Klassen von Gruppen, insbesondere für alle endlichen Gruppen, besitzt das Wortproblem jedoch eine positive Lösung.

6 Gruppenoperationen

In der Natur treten Gruppen in der Regel nicht als abstrakte Gruppen auf, sondern als Symmetriegruppen, also Gruppen von Abbildungen einer Menge in sich. Dies führt auf folgenden Begriff:

Definition 6.1. Eine *Operation* oder auch *Wirkung* einer Gruppe $(G,\circ)$ auf einer Menge M ist eine Abbildung

$$G\times M \longrightarrow M, \quad (g,m) \mapsto g\cdot m$$

sodass gilt:

a) Es ist $e\cdot m = m$ für das neutrale Element $e\in G$ und alle $m\in M$.

b) Es ist $(g_1\circ g_2)\cdot m = g_1\cdot(g_2\cdot m)$ für alle $g_1,g_2\in G$ und $m\in M$.

Beispiel 6.2. Es gilt:

a) Die Gruppe $G = D_n$ operiert auf einem regulären n-Eck M.

b) Für $n\in\mathbb{N}$ operiert die symmetrische Gruppe $G=\mathfrak{S}_n$ auf $M=\{1,\ldots,n\}$ durch Permutationen:

$$\mathfrak{S}_n\times\{1,\ldots,n\} \longrightarrow \{1,\ldots,n\}, \quad (\sigma,i) \mapsto \sigma(i).$$

c) Für jeden Körper K operiert die Gruppe $G=\mathrm{GL}_n(K)$ auf $M=K^n$ durch lineare Transformationen:

$$\mathrm{GL}_n(K)\times M \longrightarrow M, \quad (A,v) \mapsto A\cdot v.$$

d) Jede Gruppe $(G,\circ)$ operiert auf der Menge $M=G$ auf mehrere Arten:

- durch die Linkstranslation $G\times G\to G, (g,h)\mapsto g\circ h$.
- durch die Rechtstranslation $G\times G\to G, (g,h)\mapsto h\circ g^{-1}$.
- durch die Konjugation $G\times G\to G, (g,h)\mapsto g\circ h\circ g^{-1}$.

Bemerkung 6.3. Wir betrachten hier nur sogenannte Linksoperationen. Analog kann man Rechtsoperationen definieren als Abbildungen $M\times G\to G$ mit $m\cdot e_G = m$ und $(m\cdot g)\cdot h = m\cdot(g\circ h)$. Man beachte:

- Für Linksoperationen operiert $g\circ h$, indem erst h und dann g operiert.
- Für Rechtsoperationen operiert $g\circ h$, indem erst g und dann h operiert.

Der Wechsel zwischen beiden ist einfach: Ist $\lambda : G\times M\to M$ eine Linksoperation, dann ist

$$\rho: \quad M\times G \longrightarrow M, \quad \rho(m,g) := \lambda(g^{-1},m)$$

eine Rechtsoperation, und umgekehrt. Linksoperationen sind praktisch, weil wir die Verkettung von Abbildungen von rechts nach links lesen:

Lemma 6.4. *Sei G eine Gruppe und M eine Menge. Dann existiert eine Bijektion zwischen*

a) Linksoperationen $\lambda : G \times M \longrightarrow M$.

b) Gruppenhomomorphismen

$$f: \quad G \longrightarrow \mathfrak{S}_M := \big\{\text{bijektive Abbildungen } M \to M\big\}$$

Beweis. Sei zunächst eine Linksoperation von G auf M gegeben. Für jedes $g \in G$ sei $f(g) : M \to M$ durch $m \mapsto g \cdot m$ definiert. Per Definition von Linksoperationen gilt dann

- $f(e_G) = id_M$,
- $f(gh) = f(g) \circ f(h)$ für alle $g, h \in G$.

Indem wir speziell $h = g^{-1}$ wählen, sehen wir, dass $f(g) : M \to M$ bijektiv ist. Wir erhalten also eine Abbildung

$$f: \quad G \longrightarrow \mathfrak{S}_M, \quad g \mapsto g \cdot (-),$$

und nach den obigen Eigenschaften ist diese ein Homomorphismus. Ist umgekehrt ein solcher Homomorphismus gegeben, dann erhält man eine Linksoperation von G auf M, indem man $g \cdot m := (f(g))(m)$ für $g \in G, m \in M$ setzt. Man prüft sofort nach, dass diese beiden Konstruktionen zueinander invers sind. □

Im Folgenden meinen wir mit *Gruppenoperation* stets Linksoperationen. Sollte doch einmal eine Rechtsoperation auftauchen, dann wird dies explizit dazugesagt.

Definition 6.5. Eine Gruppenoperation $G \times M \to M, (g, m) \mapsto g \cdot m$ heißt *treu*, wenn der Homomorphismus

$$G \longrightarrow \mathfrak{S}_M, \quad g \mapsto g \cdot m$$

injektiv ist, d.h. wenn das Einselement das einzige Element der Gruppe ist, welches alle $m \in M$ fixiert:

$$\Big(\forall m \in M : \; g \cdot m = m\Big) \quad \Longrightarrow \quad g = e_G$$

Beispiel 6.6. a) Die Gruppe $G = \mathfrak{S}_n$ operiert treu auf $M = \{1, \ldots, n\}$.

b) Jede Gruppe G operiert treu auf sich selbst durch Linkstranslation.

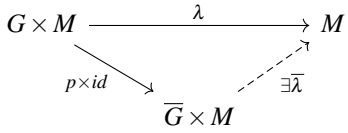
Das letzte Beispiel zeigt insbesondere, dass jede endliche Gruppe als Untergruppe einer symmetrischen Gruppe angesehen werden kann:

Korollar 6.7. *Jede endliche Gruppe der Ordnung n ist zu einer Untergruppe der symmetrischen Gruppe $\mathfrak{S}_n$ isomorph.*

Beweis. Die Operation jeder Gruppe G auf sich durch Linkstranslation ist treu; wenn die Gruppe endlich ist und wir ihre Elemente durchnumerieren als $1, \ldots, n$, erhalten wir einen injektiven Homomorphismus $G \hookrightarrow \mathfrak{S}_n$. □

Natürlich ist nicht jede in der Natur auftretende Gruppenoperation treu, aber das folgende Lemma zeigt, dass wir uns im Prinzip auf treue Operationen beschränken können:

Lemma 6.8. *Sei G eine Gruppe. Dann faktorisiert jede Operation $\lambda : G \times M \to M$ in der Form*



für einen Quotienten $p : G \twoheadrightarrow \overline{G}$ und eine treue Operation $\overline{\lambda} : \overline{G} \times M \to M$.

Beweis. Sei $f : G \to \mathfrak{S}_M$ der die Operation beschreibende Homomorphismus. Nach dem Homomorphiesatz faktorisiert dieser als

$$f \;=\; \overline{f} \circ p : \qquad G \xrightarrow{\;p\;} \overline{G} \;:=\; G/\ker(f) \xhookrightarrow{\;\overline{f}\;} \mathfrak{S}_M$$

wobei $\overline{f}$ injektiv ist und somit eine treue Operation von $\overline{G}$ auf M definiert. □

Beispiel 6.9. Es gilt:

a) Die Gruppe $G = (\mathbb{R}, +)$ operiert auf dem Einheitskreis $S^1 = \{z \in \mathbb{C} \mid |z| = 1\}$ mittels

$$\lambda : \quad \mathbb{R} \times S^1 \;\longrightarrow\; S^1, \quad (a,z) \;\mapsto\; \exp(2\pi i a) \cdot z.$$

Diese Operation ist nicht treu. Sie faktorisiert über eine treue Operation von $\mathbb{R}/\mathbb{Z}$.

b) Sei G eine Gruppe und $M = G$. Die Operation $\lambda : G \times M \to M, (g,x) \mapsto gxg^{-1}$ durch Konjugation ist im Allgemeinen nicht treu. Sie faktorisiert über eine treue Operation

$$\overline{\lambda} : \quad \overline{G} \times M \;\longrightarrow\; M \quad \text{des Quotienten} \quad \overline{G} \;=\; G/Z(G)$$

modulo dem *Zentrum* $Z(G) := \{z \in G \mid \forall x \in G : zx = xz\} \trianglelefteq G$ (siehe Übungen).

Auch für treue Gruppenoperationen kann ein jeweils festes Elemente $m \in M$ von Gruppenelementen $g \neq e_G$ fixiert werden. Dies führt auf den wichtigen Begriff des Stabilisators:

Definition 6.10. Sei $G \times M \to M$ eine Gruppenoperation.

a) Der *Stabilisator* von $m \in M$ ist $\mathrm{Stab}_G(m) := G_m := \{g \in G \mid g \cdot m = m\}$.

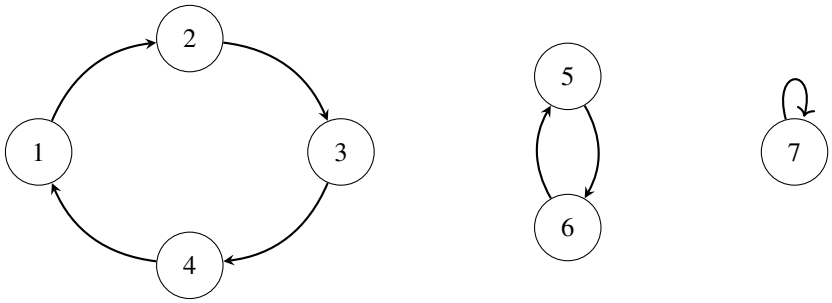
Die Gruppenoperation heißt *frei*, falls $\mathrm{Stab}_G(m) = \{e_G\}$ für alle $m \in M$ ist.

b) Für $m \in M$ heißt $G \cdot m := \{g \cdot m \mid g \in G\}$ der *Orbit* oder auch die *Bahn* von m.

Die Operation heißt *transitiv*, wenn M aus einem einzigen Orbit besteht, d.h. wenn ein $m \in M$ existiert mit

$$G \cdot m \;=\; M.$$

Beispiel 6.11. Die zyklische Gruppe $G = \mathbb{Z}/4\mathbb{Z}$ operiere auf $M = \{1,2,\ldots,7\}$ wie in der folgenden Skizze gezeigt, wobei mit den Pfeilen jeweils die Wirkung des Erzeugers $[1] \in \mathbb{Z}/4\mathbb{Z}$ dargestellt sei:



Hier gilt:

- Für $m = 1,2,3,4$ ist $G \cdot m = \{1,2,3,4\}$ und $\mathrm{Stab}_G(m) = \{[0]\}$.
- Für $m = 5,6$ ist $G \cdot m = \{5,6\}$ und $\mathrm{Stab}_G(m) = \{[0],[2]\}$.
- Für $m = 7$ ist $G \cdot m = \{7\}$ und $\mathrm{Stab}_G(m) = \{[0],[1],[2],[3]\} = G$.

In diesem Beispiel ist M eine disjunkte Vereinigung von Orbiten, die Stabilisatoren sind Untergruppen, und der Index dieser Untergruppen gibt die Anzahl der Elemente im zugehörigen Orbit an. Allgemein gilt:

Satz 6.12. *Sei $G \times M \to M$ eine Gruppenoperation. Dann gilt:*

a) Für jedes $m \in M$ ist der Stabilisator $\mathrm{Stab}_G(m) \leq G$ eine Untergruppe, und die Menge ihrer Linksnebenklassen lässt sich identifizieren mit dem Orbit $G \cdot m$ via der Bijektion

$$G/\mathrm{Stab}_G(m) \longrightarrow G \cdot m, \quad g \mapsto g \cdot m.$$

b) Die Stabilisatoren aller Elemente in demselben Orbit sind zueinander konjugiert, genauer gilt

$$\mathrm{Stab}_G(g \cdot m) = g \cdot \mathrm{Stab}_G(m) \cdot g^{-1} \quad \text{für alle } g \in G,\ m \in M.$$

c) Je zwei Orbiten sind entweder disjunkt oder gleich, d.h. für je zwei $m_1, m_2 \in M$ gilt:

$$G \cdot m_1 \cap G \cdot m_2 \neq \varnothing \quad \Longleftrightarrow \quad G \cdot m_1 = G \cdot m_2.$$

Beweis. $a)$ folgt direkt aus den Definitionen. Für $b)$ berechnet man

$$\begin{aligned} \mathrm{Stab}_G(g \cdot m) &= \{x \in G \mid x \cdot (g \cdot m) = g \cdot m\} \\ &= \{x \in G \mid (g^{-1} \cdot x \cdot g) \cdot m = m\} \\ &= \{x \in G \mid g^{-1} \cdot x \cdot g \in \mathrm{Stab}_G(m)\} = g \cdot \mathrm{Stab}_G(m) \cdot g^{-1} \end{aligned}$$

Für c) nehmen wir an, dass $G \cdot m_1 \cap G \cdot m_2 \neq \varnothing$ ist; sei etwa $g_1 \cdot m_1 = g_2 \cdot m_2$ für geeignete $g_1, g_2 \in G$. Dann folgt

$$G \cdot m_1 \;=\; \{gm_1 \mid g \in G\} \;=\; \{hg_1m_1 \mid h \in G\} \;=\; \{hg_2m_2 \mid h \in G\} \;=\; G \cdot m_2,$$

da mit h auch $h \cdot g_1$ bzw. $h \cdot g_2$ alle Elemente der Gruppe G durchläuft. □

Korollar 6.13. *Sei $G \times M \to M$ eine Gruppenoperation und $R \subseteq M$ eine Teilmenge, die aus jeder Bahn genau ein Element enthält. Für die Kardinalität der Menge M gilt dann die* Bahnformel

$$|M| \;=\; \sum_{m \in R} |G \cdot m| \quad \textit{mit} \quad |G \cdot m| \;=\; [G : \mathrm{Stab}_G(m)].$$

Beweis. Die erste Formel gilt, weil M eine disjunkte Vereinigung von Bahnen ist; die zweite, weil für jede Bahn die Abbildung $G/\mathrm{Stab}_G(m) \to G \cdot m$ bijektiv ist. □

Im Beispiel 6.11 gibt es genau drei Orbiten: Einen mit vier, einen mit zwei und einen mit einem Element; in der Tat ist hier $|M| = 7 = 4 + 2 + 1$. Die folgenden Beispiele und die Transformationsformel

$$\mathrm{Stab}_G(g \cdot m) \;=\; g \cdot \mathrm{Stab}_G(m) \cdot g^{-1}$$

zeigen, dass Stabilisatoren von Elementen im Allgemeinen keine Normalteiler sein müssen; somit erben der Quotient $G/\mathrm{Stab}_G(m)$ und die Bahn $G \cdot m$ im Allgemeinen keine Gruppenstruktur, sie sind lediglich Mengen!

Beispiel 6.14. Es gilt:

a) Die Gruppe $G = \mathfrak{S}_n$ operiert transitiv auf $M = \{1, \ldots, n\}$. Hier besteht $\mathrm{Stab}_G(n)$ aus allen Permutationen

$$\sigma \;=\; \begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ * & * & \cdots & * & n \end{pmatrix} \;\in\; \mathfrak{S}_n.$$

Diese Permutationen operieren in natürlicher Weise auf $M \setminus \{n\} = \{1, \ldots, n-1\}$ und bilden die Untergruppe

$$\mathrm{Stab}_G(n) \;\simeq\; \mathfrak{S}_{n-1} \quad \text{vom Index} \quad [\mathfrak{S}_n : \mathrm{Stab}_G(n)] \;=\; n.$$

b) Die Gruppe $G = \mathrm{GL}_n(K)$ operiert für $n > 0$ nicht transitiv auf $M = K^n$, denn es gibt genau zwei Orbiten

$$K^n \setminus \{0\} \quad \text{und} \quad \{0\}.$$

Der Stabilisator des Vektors $(1, 0, \ldots, 0) \in K^n$ ist die Untergruppe aller Matrizen der Form

$$\begin{pmatrix} 1 & * & \cdots & * \\ 0 & * & \cdots & * \\ \vdots & \vdots & \ddots & \vdots \\ 0 & * & \cdots & * \end{pmatrix} \;\in\; \mathrm{GL}_n(K).$$

c) Sei H eine Gruppe. Jede Untergruppe $G \leq H$ operiert auf der Menge $M = H$ durch Linkstranslation

$$\lambda : \quad G \times M \longrightarrow M, \quad (g,h) \mapsto g \cdot h.$$

Diese Operation ist frei, denn für alle $h \in H$ ist

$$\mathrm{Stab}_G(h) \;=\; \{g \in G \mid gh = h\} \;=\; \{e_G\}.$$

Die Orbiten dieser Operation sind genau die Rechtsnebenklassen $Gh \in G \setminus H$.

d) Jede Gruppe G operiert auf sich durch Konjugation. In diesem Fall haben die Orbiten und die Stabilisatoren von Elementen $x \in G$ einen eigenen Namen:

- Der Orbit von x heißt die *Konjugationsklasse* $x^G = \{gxg^{-1} \mid g \in G\} \subseteq G$.
- Der Stabilisator von x heißt Zentralisator $Z_G(x) = \{g \in G \mid gxg^{-1} = x\} \leq G$.

Eine sehr nützliche Folgerung aus der Bahnformel ist das sogenannte Lemma von Burnside, das allerdings schon auf Cauchy und Frobenius zurückgeht. Um dies zu formulieren, bezeichnen wir für eine Gruppenoperation $G \times M \to M$ die Menge der Bahnen mit M/G. Wir bezeichnen mit

$$\begin{aligned} \mathrm{Fix}(g) \;&:=\; \{m \in M \mid g \cdot m = m\} \\ &=\; \{m \in M \mid g \in \mathrm{Stab}_G(m)\} \end{aligned}$$

die Menge der *Fixpunkte* eines Elementes $g \in G$. Dann gilt:

Korollar 6.15 (Lemma von Burnside). *Es sei $G \times M \longrightarrow M$ eine Operation einer endlichen Gruppe auf einer endlichen Menge. Dann gilt für die Anzahl ihrer Bahnen die Formel*

$$|M/G| \;=\; \frac{1}{|G|} \sum_{g \in G} |\mathrm{Fix}(g)|.$$

Beweis. Es ist

$$\sum_{g \in G} |\mathrm{Fix}(g)| \;=\; |\{(g,m) \in G \times M \mid gm = m\}| \;=\; \sum_{m \in M} |\mathrm{Stab}_G(m)| \;=\; \sum_{m \in M} \frac{|G|}{|G \cdot m|},$$

wobei wir im letzten Schritt die Bahnformel verwendet haben. Nach Division durch die Gruppenordnung $|G|$ erhalten wir somit

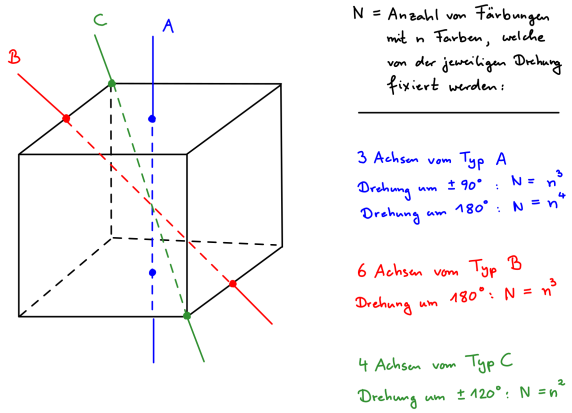
$$\frac{1}{|G|} \sum_{g \in G} |\mathrm{Fix}(g)| \;=\; \sum_{m \in M} \frac{1}{|G \cdot m|}.$$

Auf der rechten Seite gibt es für jedes $m \in M$ einen Summanden, die Summanden in demselben Orbit $G \cdot m \subseteq M$ werden aber alle mit dem Faktor $1/|G \cdot m|$ gewichtet; insgesamt wird daher jeder Orbit genau einmal gezählt. □

Beispiel 6.16. Gegeben seien n verschiedene Farben. Wieviele Möglichkeiten gibt es, die Seiten eines Würfels mit jeweils einer dieser Farben einzufärben? Dabei wollen wir die Möglichkeiten nur bis auf Drehung zählen, also die Kardinalität der Menge M/G der Bahnen für die Operation $G \times M \to M$ finden, wobei

- G die Gruppe aller Drehungen sei, die den Würfel auf sich abbilden,
- M die Menge aller möglichen Färbungen des Würfels bezeichne.

Nach dem Lemma von Burnside müssen wir dazu die Anzahl der Elemente in den Stabilisatoren ausrechnen. Die Identität lässt alle n^6 Färbungen invariant. Für jede andere Drehung gibt die folgende Liste die Anzahl N der Färbungen, die invariant unter der jeweiligen Drehung sind:



Die Gesamtzahl der Färbungen ist nach Burnside also

$$|M/G| \;=\; \tfrac{1}{24} \cdot \left(n^6 + 3n^4 + 12n^3 + 8n^2\right).$$

7 Symmetrische und alternierende Gruppen

Eine praktische Anwendung der Zerlegung einer Menge in disjunkte Orbiten ist eine Kurznotation für Permutationen. Die Bausteine hierfür sind sogenannte Zykel:

Definition 7.1. Sei $n \in \mathbb{N}$. Eine Permutation $\sigma \in \mathfrak{S}_n$ ist ein *Zykel der Länge* $k > 1$ oder kurz ein *k-Zykel*, wenn paarweise verschiedene Indices $i_1, \ldots, i_k \in \{1, \ldots, n\}$ existieren mit

$$\sigma(i_\nu) \;=\; \begin{cases} i_{\nu+1} & \text{für } \nu < k, \\ i_1 & \text{für } \nu = k, \end{cases}$$

und $\sigma(i) = i$ für alle $i \notin \{i_1, \ldots, i_k\}$. Wir schreiben dann kurz $\sigma = (i_1 i_2 \ldots i_k)$.

Beispiel 7.2. Der 2-Zykel $\sigma = (ij)$ vertauscht die zwei verschiedenen Punkte i, j und lässt alle übrigen Punkte fest. Wir nennen 2-Zykel auch *Transpositionen*. Man beachte, dass in der obigen Notation für Zykel die Indices nur bis auf zyklische Vertauschung relevant sind, z.B. gilt

$$\sigma \;=\; (123) \;=\; (231) \;=\; (312)$$

Die Permutation

$$\sigma \;=\; \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & \cdots & n \\ 3 & 5 & 2 & 4 & 1 & 6 & 7 & 8 & \cdots & n \end{pmatrix} \;\in\; \mathfrak{S}_n$$

ist ein 4-Zykel, genauer gilt in unserer obigen Notation $\sigma = (1325)$. Für $n \gg 0$ wird klar, warum die Zykelschreibweise praktischer ist als unsere bisherige Notation mit Wertetabellen...

Definition 7.3. Der *Träger* (engl. *support*) eines Zykels $\sigma = (i_1 i_2 \dots i_k)$ mit $k > 1$ ist definiert als

$$\mathrm{Supp}(\sigma) \;:=\; \{i_1, \dots, i_k\}.$$

Zwei Zykel $\sigma, \tau \in \mathfrak{S}_n$ heißen *disjunkt*, wenn $\mathrm{Supp}(\sigma) \cap \mathrm{Supp}(\tau) = \varnothing$ ist.

Mit Zykeln kann man sehr einfach rechnen. Das folgende Lemma stellt einige nützliche Regeln zusammen:

Lemma 7.4. *Für Zykel in $\mathfrak{S}_n$ gilt:*

a) Es ist $(i_1 i_2 \dots i_k) = (i_1 i_2) \circ (i_2 i_3) \circ \cdots \circ (i_{k-1} i_k)$.

b) Das Inverse eines Zykels ist der Zykel $(i_1 i_2 \dots i_k)^{-1} = (i_k i_{k-1} \dots i_1)$.

c) Konjugation mit $\tau \in \mathfrak{S}_n$ liefert $\tau \circ (i_1 i_2 \dots i_k) \circ \tau^{-1} = (\tau(i_1)\tau(i_2)\dots\tau(i_k))$.

d) Für je zwei disjunkte Zykel $\sigma, \tau \in \mathfrak{S}_n$ gjlt $\sigma \circ \tau = \tau \circ \sigma$.

Beweis. Für $a)$ prüft man direkt nach, dass das Produkt von Transpositionen auf der rechten Seite dieselbe Abbildung wie $(i_1 i_2 \dots i_k)$ darstellt. Teil $b)$ folgt aus $a)$ und der Tatsache, dass Transpositionen zu sich selbst invers sind; man beachte, dass sich bei der Inversion von Produkten die Reihenfolge der Faktoren umkehrt. Teil $c)$ ist klar wegen

$$(\tau \circ \sigma \circ \tau^{-1})(\tau(i)) \;=\; \tau(\sigma(i))$$

für $1 \le i \le n$. Teil $d)$ ist ein Spezialfall der Aussage in $c)$: Denn wenn τ ein zu σ disjunkter Zykel ist, gilt per Definition $\tau(i) = i$ für alle $i \in \mathrm{Supp}(\sigma) = \{i_1, \dots, i_k\}$, also $\tau \circ \sigma \circ \tau^{-1} = \sigma$ nach $c)$. Damit folgt die Behauptung. □

Man beachte, dass in $a)$ die Transpositionen *nicht* disjunkt zueinander sind. Sie dürfen daher nicht miteinander vertauscht werden, da die Aussage in $d)$ nur für disjunkte Zykel gilt: Dies sieht man schon an dem Beispiel

$$(23) \circ (12) \;=\; (132) \;\neq\; (231) \;=\; (12) \circ (23).$$

Wenn wir uns auf Zerlegungen als Produkt paarweise disjunkter Zykel beschränken, treten solche Mehrdeutigkeiten nicht auf:

Satz 7.5. *Jedes $\sigma \in \mathfrak{S}_n$ ist ein Produkt paarweise disjunkter nichttrivialer Zykel*

$$\sigma \;=\; (i_{11}i_{12}\dots i_{1k_1}) \circ (i_{21}i_{22}\dots i_{2k_2}) \circ \dots \circ (i_{r1}i_{r2}\dots i_{rk_r}),$$

und diese Produktzerlegung ist bis auf die Reihenfolge der Faktoren eindeutig.

Beweis. Die zyklische Gruppe $G = \langle\sigma\rangle$ operiert auf der Menge $M = \{1,2,\dots,n\}$ durch Permutationen. Nach Satz 6.12 ist M eine disjunkte Vereinigung von Orbiten

$$M \;=\; \{i_{11},\dots,i_{1k_1}\} \sqcup \dots \sqcup \{i_{r1},\dots,i_{rk_r}\},$$

wobei wir die Indizes derart numerieren können, dass $\sigma(i_{\nu,\mu}) = i_{\nu,\mu+1 \bmod k_\nu}$ für alle μ,ν gilt. Indem wir die Orbiten mit nur einem Element weglassen, erhalten wir eine Zerlegung von σ als Produkt paarweise disjunkter Zykeln. Die Eindeutigkeit ist aus der Interpretation der Faktoren als Orbiten klar. □

Die obige Zerlegung bezeichnet man als die *Zykelnotation* für $\sigma \in \mathfrak{S}_n$ und lässt dabei das Symbol $\circ$ meist weg. Um die Zykelnotation einer durch eine Wertetabelle gegenenen Permutation $\sigma \in \mathfrak{S}_n$ abzulesen, muß man die Menge $M = \{1,\dots,n\}$ in Orbiten unter $\langle\sigma\rangle$ zerlegen. Dazu kann man einen gerichteten Graphen zeichnen, dessen Ecken die Punkte aus M sind und dessen Kanten die Wirkung von σ angeben; die Zykel sind dann diejenigen Zusammenhangskomponenten des Graphen, die aus mehr als einer Ecke bestehen: Für

$$\sigma \;=\; \begin{pmatrix} 1&2&3&4&5&6&7\\ 2&3&4&1&6&5&7 \end{pmatrix} \;\in\; \mathfrak{S}_7$$

liest man aus dem Graphen in Beispiel 6.11 die Zykelnotation $\sigma = (1234)(56)$ ab.

Unsere obigen Rechenregeln für Zykel liefern sofort entsprechende Regeln für Permutationen in Zykelnotation. Z.B. erhält man aus der Zerlegung von Zykeln als Produkt von (nicht notwendig disjunkten) Transpositionen sofort eine Zerlegung beliebiger Permutationen als ein Produkt von Transpositionen; daher wird $\mathfrak{S}_n$ von Transpositionen erzeugt. Für die Konjugation von Permutationen gilt:

Lemma 7.6. *Für ein Produkt von Zykeln*

$$\sigma \;=\; (i_{11}\dots i_{1k_1})(i_{21}\dots i_{2k_2})\dots(i_{r1}\dots i_{rk_r}) \;\in\; \mathfrak{S}_n$$

ist das Konjugierte mit einer Permutation $\tau \in \mathfrak{S}_n$ gegeben durch

$$\tau\sigma\tau^{-1} \;=\; (j_{11}\dots j_{1k_1})(j_{21}\dots j_{2k_2})\dots(j_{r1}\dots j_{rk_r}) \quad \textit{mit} \quad j_{\mu\nu} \;=\; \tau(i_{\mu\nu}).$$

Beweis. Folgt direkt aus der Konjugationsformel für Zykel in Lemma 7.4 und der Tatsache, dass $\mathfrak{S}_n \to \mathfrak{S}_n, \sigma \mapsto \tau\sigma\tau^{-1}$ ein Gruppenhomomorphismus ist (alternativ kann man natürlich auch direkt denselben Beweis wie in Lemma 7.4 nutzen). □

Definition 7.7. Der *Zykeltyp* von $\sigma \in \mathfrak{S}_n$ ist das Tupel $(k_1, \ldots, k_s) \in \mathbb{N}^s$ der Längen in der Zerlegung

$$\sigma \;=\; (i_{11} \ldots i_{1k_1})(i_{21} \ldots i_{2k_2}) \ldots (i_{s1} \ldots i_{sk_s})$$

als Produkt disjunkter Zykel, wobei wir folgende Konventionen machen:

- Wir ordnen die Zykel gemäß absteigender Länge $k_1 \geq k_2 \geq \cdots \geq k_s$ an.
- Wir fügen triviale Zykel der Länge Eins hinzu, sodass $k_1 + \cdots + k_s = n$ wird.

Die letzte Konvention sorgt dafür, dass Zykeltypen der Permutationen $\sigma \in \mathfrak{S}_n$ genau Zerlegungen

$$n \;=\; k_1 + k_2 + \cdots + k_s \quad \text{mit natürlichen Zahlen} \quad k_1 \geq k_2 \geq \cdots \geq k_s \geq 1$$

sind. Solche Zerlegungen bezeichnet man auch als *Partitionen* von n. Wir erhalten:

Korollar 7.8. *Sei $n \in \mathbb{N}$.*

a) Die Konjugationsklassen in $\mathfrak{S}_n$ entsprechen bijektiv den Partitionen von n mittels

$$\text{Konjugationsklasse von } \sigma \quad \mapsto \quad \text{Zykeltyp von } \sigma$$

b) Für $\sigma \in \mathfrak{S}_n$ vom Zykeltyp $(k_1, \ldots, k_s)$ gilt $\operatorname{ord}(\sigma) = \operatorname{kgV}(k_1, \ldots, k_s)$.

Beweis. Teil a) folgt unmittelbar aus Lemma 7.6. Teil b) folgt aus der Zerlegung als Produkt

$$\sigma \;=\; \sigma_1 \circ \cdots \circ \sigma_s \quad \text{paarweise disjunkter Zykel} \quad \sigma_\nu = (i_{\nu 1} i_{\nu 2} \ldots i_{\nu k_\nu}).$$

Denn wegen der paarweisen Disjunktheit kommutieren die Zykel miteinander, für die Potenzen von σ ist also

$$\sigma^k \;=\; \sigma_1^k \circ \cdots \circ \sigma_s^k$$

Erneut wegen der paarweisen Disjunktheit der Zykel liest man ab, dass $\sigma^k = id$ ist genau dann, wenn $\sigma_1^k = \cdots = \sigma_s^k = id$ ist. Dies ist aber genau dann der Fall, wenn k durch $\operatorname{ord}(\sigma_\nu) = k_\nu$ teilbar ist für alle $\nu \in \{1, \ldots, s\}$. □

Beispiel 7.9. In $\mathfrak{S}_4$ gibt es genau fünf Konjugationsklassen:

- Der Zykeltyp $(1,1,1,1)$ entspricht der Konjugationsklasse von $\sigma = id$.
- Der Zykeltyp $(2,1,1)$ entspricht der Konjugationsklasse von $\sigma = (12)$.
- Der Zykeltyp $(2,2)$ entspricht der Konjugationsklasse von $\sigma = (12)(34)$.
- Der Zykeltyp $(3,1)$ entspricht der Konjugationsklasse von $\sigma = (123)$.
- Der Zykeltyp (4) entspricht der Konjugationsklasse von $\sigma = (1234)$.

Übungsaufgabe: Wieviele Elemente liegen jeweils in diesen Konjugationsklassen?

Zum Schluß dieses Kapitels wollen wir uns noch kurz der *alternierenden Gruppe* zuwenden, also dem Kern $\mathfrak{A}_n := \ker(sgn)$ des aus der linearen Algebra bekannten Homomorphismus

$$sgn: \quad \mathfrak{S}_n \longrightarrow \{\pm 1\}, \quad \sigma \mapsto \prod_{1\le i<j\le n} \frac{\sigma(j)-\sigma(i)}{j-i}.$$

Dass durch die obige Formel tatsächlich ein Homomorphismus definiert wird, haben wir uns bereits in der linearen Algebra überlegt; dort haben wir auch gesehen, dass Transpositionen σ das Signum $sgn\sigma = -1$ besitzen. Hieraus folgt für das Signum von Zykeln

$$sgn(i_1 \dots i_k) \;=\; (-1)^{k-1}$$

sodass wir aus der Zykelnotation einer Permutation auch sofort ihr Signum ablesen können. Während die symmetrische Gruppe von Transpositionen erzeugt wird, gilt für die alternierende Gruppe:

Lemma 7.10. *Die Untergruppe $\mathfrak{A}_n = \ker(sgn) \le \mathfrak{S}_n$ wird von den 3-Zykeln erzeugt.*

Beweis. Alle 3-Zykel haben das Signum 1 und liegen somit in $\mathfrak{A}_n$. Wir müssen umgekehrt zeigen, dass jedes Element $\sigma \in \mathfrak{A}_n$ ein Produkt von 3-Zykeln ist. Hierzu schreiben wir σ zunächst als Produkt von Transpositionen; wegen $sgn\sigma = 1$ ist dabei eine gerade Anzahl von Transpositionen nötig. Es genügt daher zu zeigen, dass das Produkt von je zwei Transpositionen sich als ein Produkt von 3-Zykeln schreiben lässt. Dazu seien zwei Transpositionen $(ij),(kl) \in \mathfrak{S}_n$ gegeben, wobei wir im Fall $|\{i,j\}\cap\{k,l\}| = 1$ oBdA $i = k$ annehmen dürfen, da die Indices in jeder der beiden Transpositionen bei Bedarf vertauscht werden können. Wegen

$$(ij)(kl) \;=\; \begin{cases} 1 & \text{für } \{i,j\} = \{k,l\}, \\ (klj) & \text{für } i = k \text{ und } j \ne l, \\ (ikj)(ikl) & \text{für } \{i,j\}\cap\{k,l\} = \varnothing. \end{cases}$$

folgt dann die Behauptung. □

Die alternierende Gruppe $\mathfrak{A}_n$ ist für $n = 1,2$ trivial und wird für $n = 3,4$ in den Übungsgruppen eingehender betrachtet. In allen übrigen Fällen ist die alternierende Gruppe die normale Hülle eines beliebigen 3-Zykels:

Lemma 7.11. *Für $n \ge 5$ sind alle 3-Zykel in $\mathfrak{A}_n$ zueinander konjugiert.*

Beweis. Gemäß Korollar 7.8 gibt es für je zwei 3-Zykel $(i_1i_2i_3),(j_1j_2j_3) \in \mathfrak{S}_n$ ein Element $\tau \in \mathfrak{S}_n$ mit

$$\tau \circ (i_1i_2i_3) \circ \tau^{-1} \;=\; (j_1j_2j_3).$$

Wir müssen zeigen, dass man hierbei im Fall $n \ge 5$ sogar $\tau \in \mathfrak{A}_n$ wählen kann. Dazu wählen wir

$$i_4, i_5 \;\in\; \{1,\dots,n\} \setminus \{i_1,i_2,i_3\}.$$

und ersetzen τ durch

$$\sigma := \begin{cases} \tau \circ (i_4 i_5) & \text{falls } sgn\tau = -1, \\ \tau & \text{falls } sgn\tau = +1, \end{cases}$$

Dann gilt $\sigma \in \mathfrak{A}_n$ und es ist immer noch $\sigma \circ (i_1 i_2 i_3) \circ \sigma^{-1} = (j_1 j_2 j_3)$. □

Der Homomorphismus $sgn : \mathfrak{S}_n \longrightarrow \{\pm 1\}$ hat es uns erlaubt, die symmetrische Gruppe in zwei kleinere Teile zu zerlegen: Den Normalteiler $\mathfrak{A}_n \trianglelefteq \mathfrak{S}_n$ sowie die Quotientengruppe $\mathfrak{S}_n/\mathfrak{A}_n \simeq \{\pm 1\}$. Aus dem obigen Resultat erhalten wir, dass sich die alternierende Gruppe nicht mehr weiter auf derartige Weise zerlegen lässt; dazu zunächst ein allgemeiner Begriff:

Definition 7.12. Eine Gruppe G heißt *einfach*, wenn gilt:

$$N \trianglelefteq G \quad \Longrightarrow \quad N = \{1\} \text{ oder } N = G$$

Der Name kommt daher, dass sich jede Gruppe in gewisser Weise zusammensetzen lässt aus einfachen Gruppen, die somit die elementaren Bestandteile aller Gruppen darstellen; wir werden das später für endliche Gruppen im Satz von Jordan-Hölder präzisieren. Der Name sollte nicht darüber hinwegtäuschen, dass einfache Gruppen recht kompliziert sein können! Es gilt:

Satz 7.13. *Für $n \geq 5$ ist die alternierende Gruppe $\mathfrak{A}_n$ einfach.*

Beweis. Nach Lemma 7.10 und 7.11 müssen wir nur zeigen, dass jeder von der trivialen Untergruppe verschiedene Normalteiler $N \trianglelefteq \mathfrak{A}_n$ einen 3-Zykel enthält. Sei dazu $\sigma \in \mathfrak{A}_n$ mit $\sigma \neq id$. Wir finden einen 3-Zykel in dem Normalteiler ausgehend von der Zerlegung

$$\sigma \;=\; \sigma_1 \sigma_2 \cdots \sigma_s$$

in paarweise disjunkte Zykel $\sigma_1, \ldots, \sigma_s$ der Länge $k := k_1 \geq l := k_2 \geq \cdots \geq k_s$ wie folgt:

- Falls $k > 3$ ist, schreibe $\sigma_1 = (i_1 \ldots i_k)$ und setze $\tau = (i_3 i_2 i_1) \in \mathfrak{A}_n$. Wir erhalten dann
$$N \;\ni\; \sigma^{-1} \cdot \tau\sigma\tau^{-1} \;=\; (i_k \ldots i_1) \cdot (i_3 i_1 i_2 i_4 \ldots i_k) \;=\; (i_2 i_3 i_k).$$
- Falls $k = l = 3$ ist, schreibe $\sigma_1 = (i_1 i_2 i_3)$ und $\sigma_2 = (i_4 i_5 i_6)$. Mit $\tau = (i_4 i_2 i_1) \in \mathfrak{A}_4$ reduzieren wir auf den vorigen Fall mittels
$$N \;\ni\; \sigma^{-1} \cdot \tau\sigma\tau^{-1} \;=\; (i_3 i_2 i_1)(i_6 i_5 i_4) \cdot (i_4 i_1 i_3)(i_2 i_5 i_6) \;=\; (i_1 i_2 i_4 i_3 i_6).$$
- Falls $k = 3$ und $l \leq 2$ ist, schreibe $\sigma_1 = (i_1 i_2 i_3)$. Dann ist $N \ni \sigma_1^2 = (i_1 i_3 i_2)$.
- Falls $k = l = 2$ ist, schreibe $\sigma_1 = (i_1 i_2)$ und $\sigma_2 = (i_3 i_4)$. Mit $\tau = (i_3 i_2 i_1)$ berechnet man dann
$$N \;\ni\; \sigma^{-1} \cdot \tau\sigma\tau^{-1} \;=\; (i_1 i_2)(i_3 i_4) \cdot (i_3 i_1)(i_2 i_4) \;=\; (i_1 i_4)(i_2 i_3).$$

Wähle nun $i_5 \in \{1,\dots,n\} \setminus \{i_1,\dots,i_4\}$, was wegen $n \geq 5$ geht. Für $\mu = (i_5 i_4 i_1)$ folgt

$$N \ni \mu(i_1 i_4)(i_2 i_3)\mu^{-1} = (i_5 i_1)(i_2 i_3)$$

und somit erhalten wir auch hier $N \ni (i_1 i_4)(i_2 i_3)\cdot(i_5 i_1)(i_2 i_3) = (i_1 i_5 i_4)$. □

8 Die Sätze von Sylow

Sei G eine endliche Gruppe der Ordnung n. Der Satz von Lagrange besagt, dass dann die Ordnung jeder Untergruppe ein Teiler von n sein muß. Es liegt die Frage nahe, ob umgekehrt zu jedem Teiler $d \mid n$ eine Untergruppe $H \leq G$ mit $|H| = d$ existiert. Falls G eine *abelsche* Gruppe ist, ist dies in der Tat der Fall, da dann

$$G \simeq \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}$$

isomorph zu einem Produkt zyklischer Gruppen ist, wie wir im Struktursatz in der linearen Algebra gesehen haben. Für *nichtabelsche* Gruppen G gilt die Umkehrung des Satzes von Lagrange jedoch im Allgemeinen nicht:

Beispiel 8.1. Die alternierende Gruppe $G = \mathfrak{A}_4$ hat die Ordnung $|G| = 12$, in den Übungsaufgaben werden wir aber sehen, dass sie *keine* Untergruppe der Ordnung 6 besitzt! Allgemeiner existiert auch für $n > 4$ in der alternierenden Gruppe $\mathfrak{A}_n$ keine Untergruppe $H \leq \mathfrak{A}_n$ vom Index

$$[\mathfrak{A}_n : H] = \frac{|\mathfrak{A}_n|}{|H|} = 2,$$

denn Untergruppen vom Index zwei sind immer Normalteiler (Übungsaufgabe).

Die Situation sieht allerdings besser aus, wenn wir lediglich Untergruppen von Primpotenzordnung betrachten:

Definition 8.2. Sei p eine Primzahl.

a) Eine *p-Gruppe* ist eine endliche Gruppe, deren Ordnung eine Potenz von p ist.

b) Eine *p-Untergruppe* einer Gruppe ist eine Untergruppe, die eine p-Gruppe ist.

c) Eine *p-Sylowuntergruppe* oder kurz *p-Sylowgruppe* einer endlichen Gruppe G ist eine Untergruppe $H \leq G$, deren Ordnung die maximale p-Potenz ist, die die Ordnung von G teilt:

$$|H| = p^k \quad \text{für} \quad |G| = p^k m \quad \text{mit} \quad p \nmid m.$$

Die p-Sylowgruppen sind also genau die p-Untergruppen $H \leq G$ mit $p \nmid [G:H]$. Der erste Satz von Sylow zeigt die Existenz von p-Sylowgruppen und allgemeiner auch von p-Untergruppen kleinerer Ordnung:

Satz 8.3 (Erster Satz von Sylow). *Sei G eine endliche Gruppe, und sei $p^k \mid |G|$ ein Primzahlpotenzteiler der Gruppenordnung. Dann existiert eine Untergruppe $H \leq G$ mit*

$$|H| \;=\; p^k$$

Beweis. Wir schließen per Induktion über die Gruppenordnung und betrachten dazu das Zentrum

$$Z(G) \;\coloneqq\; \{z \in G \mid \forall g \in G :\; gz = gz\} \trianglelefteq G.$$

Dies ist eine abelsche Untergruppe. Wir unterscheiden nun zwei Fälle:

Fall 1: Wenn p die Ordnung $|Z(G)|$ teilt, gibt es eine Untergruppe $N \leq Z(G)$ der Ordnung $|N| = p$, weil die Umkehrung des Satzes von Lagrange im Fall abelscher Gruppen ja korrekt ist. Nun ist N als Untergruppe des Zentrums insbesondere ein Normalteiler von G, wir können also die Quotientengruppe G/N betrachten. Dabei gilt $p^{k-1} \mid |G/N|$ und somit können wir per Induktion eine Untergruppe $\overline{H} \leq G/N$ von der Ordnung $|\overline{H}| = p^{k-1}$ finden. Sei

$$H \;\coloneqq\; f^{-1}(\overline{H}) \;\leq\; G$$

ihr Urbild unter dem Quotientenhomomorphismus $f : G \twoheadrightarrow G/N$. Dann gilt $N \leq H$, und wir erhalten einen Epimorphismus

$$f|_H : \quad H \;\twoheadrightarrow\; \overline{H} \quad \text{mit} \quad \ker(f|_H) \;=\; N.$$

Somit folgt $|H| = |N| \cdot |\overline{H}| = p \cdot p^{k-1} = p^k$ und wir sind fertig.

Fall 2: Sei nun p kein Teiler der Ordnung $|Z(G)|$. Wir betrachten in diesem Fall die Operation der Gruppe G auf sich selbst durch Konjugation. Es sei $R \subseteq G$ ein Repräsentantensystem für die Bahnen dieser Operation, also eine Teilmenge, die aus jeder Konjugationsklasse genau ein Element enthält. Sei $R^* := R \setminus Z(G)$, dann lautet die Bahnformel

$$|G| \;=\; |Z(G)| + \sum_{x \in R^*} |x^G| \quad \text{mit} \quad |x^G| \;=\; [G : Z_G(x)]$$

für den Zentralisator $Z_G(x) = \{g \in G \mid gx = xg\} \leq G$. Wegen $p \mid |G|$ und $p \nmid |Z(G)|$ muß ein $x \in R^*$ existieren mit

$$p \nmid [G : Z_G(x)].$$

Da p^k ein Teiler der Gruppenordnung $|G| = [G : Z_G(x)] \cdot |Z_G(x)|$ ist, muß also p^k die Ordnung des Zentralisators $Z_G(x)$ teilen. Aber für den Zentralisator gilt $Z_G(x) \neq G$ wegen $x \notin Z(G)$. Per Induktion über die Gruppenordnung hat $Z_G(x)$ folglich eine Untergruppe der Ordnung p^k und somit folgt die Behauptung. □

Der erste Satz von Sylow ist lediglich eine Existenzaussage. Im Allgemeinen sind p-Sylowuntergruppen nicht eindeutig, beispielsweise besitzt die symmetrische Gruppe $G = \mathfrak{S}_3$ zwar genau drei verschiedene 2-Sylowgruppen, nämlich die von je einer Transposition erzeugten Untergruppen

$$\langle(12)\rangle, \langle(13)\rangle, \langle(23)\rangle \;\leq\; \mathfrak{S}_3.$$

Somit müssen Sylowgruppen keine Normalteiler sein. Für jede p-Sylowgruppe sind natürlich auch alle ihre Konjugierten wieder p-Sylowgruppen; der zweite Satz von Sylow zeigt, dass man auf diese Weise alle p-Sylowgruppen erhält:

Satz 8.4 (Zweiter Satz von Sylow). *Sei G eine endliche Gruppe und p prim.*

a) Jede p-Untergruppe von G ist in einer p-Sylowgruppe von G enthalten.

b) Je zwei p-Sylowuntergruppen von G sind zueinander konjugiert.

Beweis. Wir fixieren eine beliebige p-Sylowuntergruppe $H \leq G$. Sei $U \leq G$ eine beliebige weitere p-Untergruppe. Wir betrachten dann die Gruppenoperation von U auf der Menge G/H durch Linkstranslation:

$$U \times G/H \;\longrightarrow\; G/H, \quad (u, gH) \;\mapsto\; ugH.$$

Die Bahnformel besagt

$$|G/H| \;=\; \sum_{gH \in R} |U|/|\mathrm{Stab}_U(gH)|,$$

wobei $R \subseteq G/H$ ein Repräsentantensystem für die Bahnen ist. Wegen $p \nmid |G/H|$ existiert somit ein $gH \in R$ mit

$$p \;\nmid\; |U|/|\mathrm{Stab}_U(gH)|.$$

Da U eine p-Gruppe ist, muß dann $\mathrm{Stab}_U(gH) = U$ sein. Also ist $ugH = gH$ und somit

$$g^{-1}ug \;\in\; H \quad \text{für alle} \quad u \;\in\; U$$

d.h. es ist $g^{-}Ug \subseteq H$ wie in $a)$ behauptet. Falls U sogar eine p-Sylowgruppe von G ist, gilt in der vorigen Inklusion sogar Gleichheit, da dann $|g^{-1}Ug| = |U| = |H|$ ist; somit folgt auch $b)$. □

Wir haben oben bereits bemerkt, dass Sylowuntergruppen im Allgemeinen keine Normalteiler sein müssen. Aus dem zweiten Satz von Sylow erhalten wir genauer:

Korollar 8.5. *Für p-Sylowgruppen $N \leq G$ sind äquivalent:*

a) N ist ein Normalteiler in G.

b) N ist die einzige p-Sylowgruppe von G.

c) Es ist $N \;=\; \{g \in G \mid \exists k \in \mathbb{N}_0 : \mathrm{ord}(g) = p^k\}$.

Beweis. Sei $N \leq G$ eine p-Sylowgruppe. Per Definition ist N ein Normalteiler in G genau dann, wenn $gNg^{-1} = N$ für alle $g \in G$ ist. Nach dem zweiten Satz von Sylow sind alle p-Sylowgruppen konjugiert zueinander, daher ist die Normalität äquivalent dazu, dass N die einzige p-Sylowgruppe ist. Somit sind $a)$ und $b)$ äquivalent. Für die Äquivalenz mit $c)$ beachte man, dass die Teilmenge

$$\{g \in G \mid \exists k \in \mathbb{N}_0 : \mathrm{ord}(g) = p^k\} \subseteq G$$

genau die Vereinigung aller p-Sylowgruppen von G ist: Denn jede p-Sylowgruppe ist eine p-Gruppe, also nach dem Satz von Lagrange enthalten in der angegebenen Teilmenge; umgekehrt erzeugt jedes Element dieser Teilmenge eine p-Untergruppe, ist also nach dem zweiten Satz von Sylow in einer p-Sylowgruppe enthalten. □

Der dritte Satz von Sylow gibt eine gewisse Information über die Anzahl $n_p(G)$ der p-Sylowuntergruppen einer endlichen Gruppe G:

Satz 8.6 (Dritter Satz von Sylow). *Sei G eine endliche Gruppe, und sei $n_p(G)$ die Anzahl ihrer p-Sylowgruppen. Dann gilt:*

a) $n_p(G) \equiv 1 \mod p$.

b) $n_p(G)$ *ist ein Teiler von* $|G|$.

Beweis. Sei $Syl_p(G)$ die Menge aller p-Sylowgruppen in G. Auf dieser operiert G durch Konjugation

$$G \times Syl_p(G) \longrightarrow Syl_p(G), \quad (g,H) \mapsto gHg^{-1}$$

und nach dem zweiten Satz von Sylow ist diese Operation transitiv, d.h. $Syl_p(G)$ besteht aus nur einem G-Orbit. Sei $U \leq G$ eine beliebige p-Sylowuntergruppe. Ihr Stabilisator bezüglich der Konjugation ist der Normalisator

$$N_G(U) := \{g \in G \mid gUg^{-1} = U\},$$

und $G/N_G(U) \to Syl_p(G), g \mapsto gUg^{-1}$ ist bijektiv. Also ist $n_p(G) = |Syl_p(G)|$ ein Teiler der Gruppenordnung und somit ist $b)$ gezeigt. Zum Beweis der Kongruenz in $a)$ betrachten wir die Einschränkung der vorigen Operation zu einer Operation der Gruppe U, also

$$U \times Syl_p(G) \longrightarrow Syl_p(G), \quad (u,H) \mapsto uHu^{-1}$$

Die Bahnformel besagt

$$n_p(G) = \sum_{H \in R} [U : \mathrm{Stab}_U(H)] \quad \text{mit} \quad \mathrm{Stab}_U(H) = U \cap N_G(H),$$

wobei $R \subseteq Syl_p(G)$ ein Repräsentantensystem der Bahnen ist. Da U eine p-Gruppe ist, folgt

$$n_p(G) \equiv |\mathrm{Fix}(U)| \mod p$$

für die Menge der Fixpunkte

$$\mathrm{Fix}(U) := \{H \in Syl_p(G) \mid \mathrm{Stab}_U(H) = U\}.$$

Wir wollen zeigen, dass $\mathrm{Fix}(U)$ lediglich ein einziges Element, nämlich $H = U$, enthält. Für $H \in \mathrm{Fix}(U)$ gilt

$$\mathrm{Stab}_U(H) = U \cap N_G(H) \overset{!}{=} U \quad \Longrightarrow \quad U \leq N_G(H).$$

Damit ist U ebenso wie H auch eine p-Sylowuntergruppe des Normalisators $N_G(H)$; da nach dem zweiten Satz von Sylow je zwei Sylowgruppen in einer gegebenen Gruppe zueinander konjugiert sind, folgt

$$U = gHg^{-1} \quad \text{für ein} \quad g \in N_G(H).$$

Aber per Definition von $N_G(H)$ ist dann $U = H$ und wir sind fertig. □

Wir wissen von der Diskussion zyklischer Gruppen, dass jede Gruppe G von Primzahlordnung $|G| = p$ isomorph zu $\mathbb{Z}/p\mathbb{Z}$ ist. Als Anwendungsbeispiel für die Sätze von Sylow betrachten wir Gruppen, deren Ordnung ein Produkt von zwei verschiedenen Primzahlen ist:

Korollar 8.7. *Jede Gruppe G der Ordnung $|G| = pq$ für zwei Primzahlen $p > q$ hat eine Präsentation*

$$G \simeq \langle x, y \mid x^p = y^q = 1, yxy^{-1} = x^k \rangle \quad \textit{für ein } k \in \mathbb{Z} \textit{ mit } p \mid (k^q - 1).$$

Insbesondere gilt:

a) Im Fall $q = 2$ ist G zyklisch oder $G \simeq D_n$.

b) Im Fall $q \nmid (p-1)$ ist G zyklisch.

Beweis. Für die Anzahl $n_p(G)$ der p-Sylowgruppen in G gilt nach dem dritten Satz von Sylow:

- $n_p(G)$ ist ein Teiler von $|G| = pq$, also $n_p(G) \in \{1, p, q, pq\}$.
- $n_p(G) \equiv 1 \mod p$, somit bleibt von obigen vier Möglichkeiten nur $n_p(G) = 1$.

Es gibt also genau eine p-Sylowgruppe $P \trianglelefteq G$, und nach Korollar 8.5 ist diese dann sogar ein Normalteiler. Nach dem ersten Satz von Sylow können wir außerdem eine Untergruppe $Q \leq G$ mit $|Q| = q$ finden (diese muß kein Normalteiler sein). Dann gilt

$$|P \cap Q| = 1,$$

da die linke Seite nach dem Satz von Lagrange ein gemeinsamer Teiler von p und q ist wegen $P \cap Q \leq P$ und $P \cap Q \leq Q$. Für die als punktweises Produkt gebildete Teilmenge

$$P \cdot Q := \{ g \cdot h \in G \mid g \in P, h \in Q \} \subseteq G$$

folgt

$$|P \cdot Q| = \frac{|P||Q|}{|P \cap Q|} = pq = |G|$$

und somit $P \cdot Q = G$. Als Gruppen von Primzahlordnung sind P und Q zyklisch, wir können also Elemente $a, b \in G$ mit $a^p = b^q = 1$ finden, sodass gilt:

$$P = \{a^m \mid n \in \mathbb{Z}\},$$
$$Q = \{b^n \mid n \in \mathbb{Z}\}.$$

Da $P \trianglelefteq G$ ein Normalteiler ist, gilt $bPb^{-1} = P$ und für den Erzeuger $a \in P$ muß daher

$$bab^{-1} = a^k \quad \text{für ein} \quad k \in \mathbb{Z}$$

gelten. Hieraus folgt induktiv

$$b^i ab^{-i} = a^{k^i} \quad \text{für} \quad i = 1,2,\ldots$$

speziell $i = q$ also $p \mid (k^q - 1)$. Wir betrachten nun den Homomorphismus

$$f: \quad \left\langle x,y \mid x^p = y^q = 1, yxy^{-1} = x^k \right\rangle \twoheadrightarrow G \quad \text{mit} \quad \begin{cases} f(x) = a, \\ f(y) = b. \end{cases}$$

Dieser ist surjektiv wegen $P \cdot Q = G$. Er ist dann auch injektiv, wie man durch Zählen von Elementen sieht: Durch Benutzen der Relationen sieht man, dass sich jedes Element der durch obige Präsentation definierten Gruppe als $x^m y^n$ mit $1 \leq m \leq p$ und $1 \leq n \leq q$ schreiben lässt.

In der obigen Präsentation der Gruppe ist nur die Restklasse $[k] \in \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ relevant. Im Fall $q = 2$ ist

$$p \mid (k^2 - 1) = (k-1)(k+1) \quad \Longrightarrow \quad p \mid (k-1) \text{ oder } p \mid (k+1)$$

und wir dürfen daher in diesem Fall oBdA $k \in \{\pm 1\}$ annehmen und erhalten somit entweder eine zyklische Gruppe oder eine Diedergruppe wie in a) behauptet. Für b) sei

$$d := \operatorname{ord}_{\mathbb{F}_p^\times}([k]) = \min\{i \in \mathbb{N} \mid [k]^i = [1] \in \mathbb{F}_p^\times\}$$

die Ordnung von $[k]$ in der multiplikativen Gruppe $\mathbb{F}_p^\times = (\mathbb{F}_p, \cdot)$. Dann gilt:

- d teilt q, da nach Voraussetzung $k^q \equiv 1 \bmod p$ gilt.
- d teilt $|\mathbb{F}_p^\times| = p - 1$ nach dem kleinen Satz von Fermat.

Im Fall $q \nmid (p-1)$ folgt $d < q$. Dann ist $b^d \neq 1$ ein Erzeuger der zyklischen Gruppe

$$Q = \{b^i \mid i = 0,1,\ldots,q-1\},$$

denn eine zyklische Gruppe von Primzahlordnung wird von jedem nichttrivialen Element der Gruppe erzeugt. Wenn wir in unserer ursprünglichen Präsentation den Erzeuger b durch b^d ersetzen, wird dabei k durch k^d ersetzt. Da $[k]^d = [1] \in \mathbb{F}_p$ ist und für die Präsentation der Gruppe nur diese Restklasse eine Rolle spielt, dürfen wir dann $k = 1$ annehmen und erhalten somit, dass G abelsch ist. Abelsche Gruppen der Ordnung pq sind aber zyklisch und somit folgt b). □

In den Übungsaufgaben haben wir durch Betrachten des Zentrums gesehen, dass jede Gruppe G der Ordnung $|G| = p^2$ für eine Primzahl p abelsch ist. Wir kennen also jetzt alle Gruppen, deren Ordnung ein Produkt von zwei Primzahlen ist!

Zum Schluß wollen wir uns noch ein Beispiel dafür ansehen, wie man aus den Sätzen von Sylow folgern kann, dass Gruppen gewisser Ordnungen nichttriviale Normalteiler besitzen (weitere Beispiele werden wir in den Übungen sehen):

Lemma 8.8. *Sei $|G| = pqr$ mit Primzahlen $p > q > r$. Dann ist G nicht einfach.*

Beweis. Sei $n_p := n_p(G)$ die Anzahl der p-Sylowgruppen, analog für n_q, n_r. Je zwei verschiedene Sylowgruppen von Primzahlordnung (nicht Primpotenzordnung) schneiden sich nur im trivialen Element. Durch Zählen der Elemente finden wir daher in G genau

- $n_p \cdot (p-1)$ Elemente der Ordnung p,
- $n_q \cdot (q-1)$ Elemente der Ordnung q,
- $n_r \cdot (r-1)$ Elemente der Ordnung r.

Wenn G eine einfache Gruppe wäre, dann müssten die drei Zahlen n_p, n_q, n_r alle > 1 sein wegen Korollar 8.5. Nach dem dritten Satz von Sylow erhalten wir dann wegen unserer Annahme $p > q > r$:

- $n_p \equiv 1 \bmod p$ und $n_p \mid qr \quad \Longrightarrow \quad n_p = qr$
- $n_q \equiv 1 \bmod q$ und $n_q \mid pr \quad \Longrightarrow \quad n_q \geq p$.
- $n_r \equiv 1 \bmod r$ und $n_r \mid qr \quad \Longrightarrow \quad n_r \geq q$.

Wir hätten dann in G insgesamt

$$qr(p-1) + p(q-1) + q(r-1) + 1 \;>\; qr(p-1) + r(q-1) + r + 1 \;=\; |G| + 1$$

Elemente, ein Widerspruch! Also muß G einfach sein. □

9 Kompositionsreihen

Um eine Gruppe G zu verstehen, kann man diese manchmal in "kleinere Teile" zerlegen: Wenn die Gruppe einen nichttrivialen Normalteiler $N \trianglelefteq G$ hat, kann man zuerst die Untergruppe N und den Quotient $Q = G/N$ studieren und aus der exakten Sequenz

$$1 \longrightarrow N \longrightarrow G \longrightarrow Q \longrightarrow 1$$

Rückschlüsse über die gesamte Gruppe ziehen. Wir sagen auch, die Gruppe G sei eine *Extension* von Q mit N. Im Allgemeinen ist der mittlere Term der Sequenz durch die Angabe der beiden äußeren Terme noch nicht eindeutig bestimmt:

Beispiel 9.1. Die beiden Gruppen $G = \mathbb{Z}/4\mathbb{Z}$ und $H = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ sind nicht zueinander isomorph. Beide sind aber Extensionen derselben Gruppen: Wir haben exakte Sequenzen

$$0 \longrightarrow \mathbb{Z}/2\mathbb{Z} \xrightarrow{g} G \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow 0$$

$$0 \longrightarrow \mathbb{Z}/2\mathbb{Z} \xrightarrow{h} H \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow 0$$

mit $g(x \bmod 2) := (2x \bmod 4) \in \mathbb{Z}/4\mathbb{Z}$ und $h(x) := (x,0) \in \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Auch wenn der mittlere Term einer kurzen exakten Sequenz durch die Angabe der äußeren Terme noch nicht eindeutig bestimmt ist, bildet die Untersuchung von Normalteilern und Quotienten ein wichtiges Hilfsmittel für das allgemeine Studium von Gruppen. Man kann dies iterieren: Wenn $N \trianglelefteq G$ noch zu kompliziert ist, kann man Normalteiler in $G_1 := N$ suchen usw. Dies führt auf folgenden Begriff:

Definition 9.2. Eine *Subnormalreihe* einer Gruppe G ist eine echt absteigende Folge von Untergruppen

$$G = G_0 > G_1 > \cdots > G_m = \{1\} \quad \text{mit} \quad G_{i+1} \trianglelefteq G_i \quad \text{für alle } i.$$

Wir nennen die Zahl m die *Länge* und die Quotientengruppen G_i/G_{i+1} die *Faktoren* der Subnormalreihe. Um auszudrücken, dass jeder Term ein echter Normalteiler des jeweils vorigen Terms ist, schreiben wir auch

$$G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_m = \{1\}.$$

Man beachte, dass die Untergruppen in einer Subnormalreihe nur Normalteiler in der jeweils vorigen Untergruppe sein müssen; wenn sie sogar Normalteiler in G sind, spricht man von einer *Normalreihe*. Eine weitere Subnormalreihe

$$G = H_0 \triangleright H_1 \triangleright \cdots \triangleright H_n = \{1\}$$

heißt eine *Verfeinerung* der zu Beginn genannten Subnormalreihe, wenn sie aus ihr durch Hinzufügen weiterer Untergruppen entsteht, wenn es also eine monotone Funktion $\sigma : \{1,\dots,m-1\} \longrightarrow \{1,\dots,n-1\}$ gibt mit $G_i = H_{\sigma(i)}$ für alle i. Im Fall $n > m$ nennen wir die Verfeinerung auch eine *echte* Verfeinerung.

Beispiel 9.3. Jede Gruppe $G \neq \{1\}$ hat die triviale Subnormalreihe

$$G = G_0 \triangleright G_1 = \{1\}.$$

Diese hat eine echte Verfeinerung genau dann, wenn es einen Normalteiler $N \trianglelefteq G$ mit $N \neq \{1\}$ und $N \neq G$ gibt, also wenn die Gruppe G nicht einfach ist:

Definition 9.4. Eine Gruppe G heißt *einfach*, wenn gilt:

$$N \trianglelefteq G \quad \Longrightarrow \quad N = \{1\} \text{ oder } N = G$$

Beispiel 9.5. Es gilt:

a) Die Gruppe $G = \mathfrak{S}_n$ ist nicht einfach, sie hat die Subnormalreihe $\mathfrak{S}_n \triangleright \mathfrak{A}_n \triangleright \{1\}$.

b) Die Gruppe $G = \mathfrak{A}_n$ ist für $n > 4$ einfach, wie wir in Satz 7.13 gesehen haben.

c) Sei K ein Körper. Für $\mu_n(K) \neq \{1\}$ ist die Gruppe $G = \mathrm{SL}_n(K)$ ist nicht einfach, denn

$$G \triangleright Z(G) \triangleright \{1\} \quad \text{mit} \quad Z(G) = \left\{ \begin{pmatrix} a & & \\ & \ddots & \\ & & a \end{pmatrix} \;\middle|\; a \in K,\, a^n = 1 \right\} \simeq \mu_n(K).$$

Falls K mehr als drei Elemente enthält, ist aber

$$\mathrm{PSL}_n(K) := \mathrm{SL}_n(K)/\mu_n(K)$$

eine einfache Gruppe, sie heißt die *projektive lineare Gruppe* (siehe Übungen).

Bemerkung 9.6. Die Klassifikation aller *endlichen* einfachen Gruppen gehört zu den bahnbrechenden Erfolgen des letzten Jahrhunderts. Sie hat viele Mathematiker bis über die 1980er Jahre hinaus beschäftigt, der Beweis erstreckt sich über viele Zeitschriftenartikel. Bis auf Isomorphie gibt es genau folgende endliche einfache Gruppen:

a) $G = \mathbb{Z}/p\mathbb{Z}$ für eine Primzahl p.

b) $G = \mathfrak{A}_n$ für eine natürliche Zahl $n > 4$.

c) Die *einfachen Gruppen vom Lie-Typ*. Diese sind Matrixgruppen über endlichen Körpern K, beispielsweise die Gruppen $G = \mathrm{PSL}_n(K)$.

d) Die 27 *sporadischen Gruppen*, darunter das *Monster* mit etwa $8 \cdot 10^{53}$ Elementen!

Für mehr Informationen siehe Wilson, *The finite simple groups*, Springer GTM 251.

Kehren wir zurück zur Frage, wie man eine gegebene Gruppe durch sukzessive Verfeinerung von Subnormalreihen in "kleinste Bestandteile" zerlegen kann. Die kleinsten Bestandteile werden dabei einfache Gruppen sein. Zunächst eine einfache Vorbemerkung:

Lemma 9.7. *Für Subnormalreihen $G = G_0 > \cdots > G_m = \{1\}$ sind äquivalent:*

a) Die Subnormalreihe hat keine echte Verfeinerung.

b) Alle Faktoren G_i/G_{i+1} der Subnormalreihe sind einfach.

Beweis. Betrachte den Epimorphismus $p_i : G_i \twoheadrightarrow \overline{G}_i := G_i/G_{i+1}$. Aus der Definition von Quotienten und Normalteilern erhält man unmittelbar, dass die im folgenden Diagramm gezeigten Abbildungen

$$\left\{\text{Normalteiler } N \trianglelefteq G_i \text{ mit } G_{i+1} \trianglelefteq N\right\} \underset{\overline{N} \mapsto N = p_i^{-1}(\overline{N})}{\overset{N \mapsto \overline{N} = p_i(N)}{\rightleftarrows}} \left\{\text{Normalteiler } \overline{N} \trianglelefteq \overline{G}_i\right\}$$

zueinander inverse Bijektionen sind. Dabei gilt

$$G_{i+1} \neq N \neq G_i \quad \Longleftrightarrow \quad \{1\} \neq \overline{N} \neq G_i/G_{i+1}$$

und hieraus folgt unmittelbar die Behauptung. □

Die gesuchte Zerlegung einer gegebenen Gruppe in ihre "kleinsten Bestandteile" nimmt damit die folgende Form an:

Definition 9.8. Eine *Kompositionsreihe* einer Gruppe ist eine Subnormalreihe, die sich nicht weiter verfeinern lässt, in der also alle Faktoren einfache Gruppen sind; man nennt diese Faktoren dann auch die *Kompositionsfaktoren* der Reihe.

Beispiel 9.9. Es gilt:

a) Die Gruppe $G = (\mathbb{Z}, +)$ hat keine Kompositionsreihe: Denn der letzte von Null verschiedene Term einer solchen wäre einfach, es gibt jedoch keine einfachen Untergruppen von $\mathbb{Z}$. Für jede Folge von Primzahlen $p_0, p_1, p_2, \ldots$ haben wir eine *unendliche* echt absteigende Folge

$$G_0 := G \triangleright G_1 \triangleright G_2 \triangleright \cdots$$

von Normalteilern $G_i := p_0 \cdots p_i \mathbb{Z}$ mit einfachen Quotienten $G_i/G_{i+1} \simeq \mathbb{Z}/p_{i+1}\mathbb{Z}$.

b) Sei K ein Körper. Die spezielle lineare Gruppe $G = \mathrm{SL}_2(K)$ besitzt dann die Normalreihe

$$G = G_0 = \mathrm{SL}_2(K) > G_1 = \{\pm 1\} > G_2 = \{1\}$$

mit den Faktoren

$$G_0/G_1 = \mathrm{PSL}_2(K) \quad \text{und} \quad G_1/G_2 = \{\pm 1\}.$$

Für $|K| > 3$ ist die projektive lineare Gruppe $\mathrm{PSL}_2(K)$ einfach nach Beispiel 9.5, wir haben in diesem Fall also eine Kompositionsreihe gefunden.

c) Jede *endliche* Gruppe $G \neq \{1\}$ hat eine Kompositionsreihe: Denn wir können die triviale Normalreihe sukzessive zu Subnormalreihen verfeinern; da endliche Gruppen nur endlich viele Untergruppen haben, muß das Verfahren nach endlich vielen Schritten terminieren und wir haben dann eine Kompositionsreihe.

d) Im Fall ihrer Existenz sind Kompositionsreihen im Allgemeinen nicht eindeutig bestimmt: Für $G = \mathbb{Z}/6\mathbb{Z}$ haben wir die beiden Kompositionsreihen

$$G_0 = \mathbb{Z}/6\mathbb{Z} \triangleright G_1 = 2\mathbb{Z}/6\mathbb{Z} \triangleright G_2 = \{0\},$$
$$H_0 = \mathbb{Z}/6\mathbb{Z} \triangleright H_1 = 3\mathbb{Z}/6\mathbb{Z} \triangleright H_2 = \{0\}.$$

Die zugehörigen Kompositionsfaktoren sind

$$G_i/G_{i+1} \simeq \begin{cases} \mathbb{Z}/2\mathbb{Z} & \text{für } i = 0, \\ \mathbb{Z}/3\mathbb{Z} & \text{für } i = 1, \end{cases} \quad \text{und} \quad H_i/H_{i+1} \simeq \begin{cases} \mathbb{Z}/3\mathbb{Z} & \text{für } i = 0, \\ \mathbb{Z}/2\mathbb{Z} & \text{für } i = 1. \end{cases}$$

Man beachte, dass die Faktoren der beiden Kompositionsreihen im letzten Beispiel bis auf die Reihenfolge übereinstimmen! Dies führt auf folgende

Definition 9.10. Sei G eine Gruppe. Zwei Subnormalreihen

$$G = G_0 \rhd G_1 \rhd G_2 \rhd \cdots \rhd G_m = \{0\}$$
$$G = H_0 \rhd H_1 \rhd H_2 \rhd \cdots \rhd H_n = \{0\}$$

heißen zueinander *äquivalent*, wenn $m = n$ ist und wenn eine Permutation $\sigma \in \mathfrak{S}_n$ existiert mit

$$G_i/G_{i+1} \simeq H_{\sigma(i)}/H_{\sigma(i)+1} \quad \text{für} \quad i = 1,\ldots,n.$$

Wir wollen zeigen, dass je zwei Kompositionsreihen einer gegebenen Gruppe G zueinander äquivalent sind. Als Vorbereitung vergleichen wir zunächst nur zwei Normalteiler von verschiedenen Untergruppen:

Lemma 9.11 (Schmetterlingslemma). *Seien $A, B \leq G$ beliebige Untergruppen mit Normalteilern*

$$A_1 \trianglelefteq A \quad \textit{und} \quad B_1 \trianglelefteq B.$$

Dann gilt

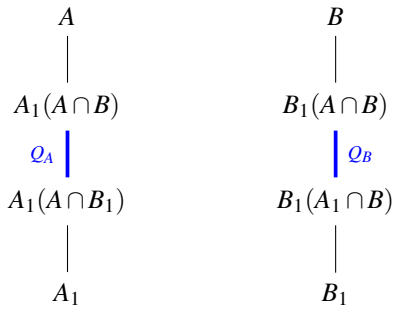
$$A_1(A \cap B)/A_1(A \cap B_1) \simeq B_1(A \cap B)/B_1(A_1 \cap B).$$

Beweis. Wir können jede der Ketten $A \rhd A_1$ und $B \rhd B_1$ benutzen, um die jeweils andere zu verfeinern: Es ist

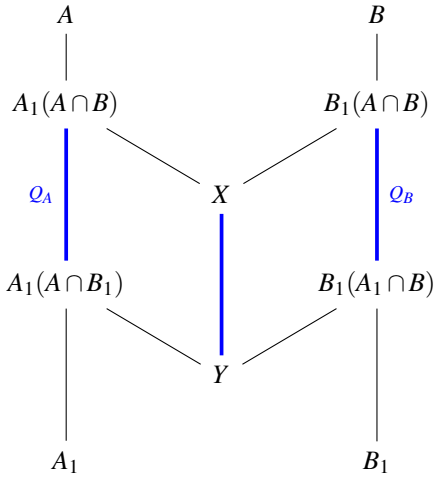
$$A \geq A \cap B \geq A \cap B_1 \geq \{1\},$$
$$B \geq A \cap B \geq A_1 \cap B \geq \{1\},$$

und indem wir diese Ketten mit A_1 bzw. B_1 multiplizieren, erhalten wir die in dem folgenden Hasse-Diagramm gezeigten Verfeinerungen. Man beachte, dass in dem Diagramm jeweils nur die unteren beiden Inklusionen Normalteiler sind, denn im Allgemeinen muß $A \cap B$ weder in A noch in B normal sein.

Wir interessieren uns für die Quotienten Q_A und Q_B zu den mittleren, in blau gezeichneten Inklusionen von Normalteilern:



Man beachte, dass es im Allgemeinen keine natürliche Abbildung zwischen den Gruppen $A_1(A\cap B)$ und $B_1(A\cap B)$ gibt. Um die beiden Quotienten miteinander zu vergleichen, betrachten wir gemeinsame Untergruppen X und Y wie im folgenden Diagramm:



Eine naheliegende Wahl ist $X = A\cap B$. Der erste Isomorphiesatz sagt uns dann, wie wir Y wählen sollten, um die Kürzungsregel für Quotienten anzuwenden; allerdings sind zunächst zwei Wahlen denkbar, denn:

- Es ist $Q_A \simeq X/Y_1$ für $Y_1 := (A_1(A\cap B_1))\cap(A\cap B)$.
- Es ist $Q_B \simeq X/Y_2$ für $Y_2 := (B_1(A_1\cap B))\cap(A\cap B)$.

Zum Glück kann man sich leicht überlegen, dass

$$Y_1 \;=\; (A\cap B_1)(A_1\cap B) \;=\; Y_2$$

ist (Übungsaufgabe). Damit ist das Schmetterlingslemma bewiesen; wenn man im Hasse-Diagramm $A_1\cap Y$ und $B_1\cap Y$ ergänzt, versteht man auch den Namen. □

Der Vergleich zweier beliebiger Subnormalreihen ist jetzt nur noch eine Frage der richtigen Buchhaltung:

Satz 9.12 (Satz von Jordan-Hölder-Schreier). *Je zwei Subnormalenreihen einer beliebigen Gruppe lassen sich derart verfeinern, dass die Verfeinerungen der beiden Reihen zueinander äquivalent sind.*

Beweis. Seien zwei Subnormalreihen

$$G = G_0 \triangleright G_1 \triangleright G_2 \triangleright \cdots \triangleright G_m = \{0\}$$
$$G = H_0 \triangleright H_1 \triangleright H_2 \triangleright \cdots \triangleright H_n = \{0\}$$

der Länge m und n gegeben. Für jedes feste $i \in \{1,\ldots,m\}$ betrachten wir in G_i die Folge

$$G_i = G_i \cap H_0 \trianglerighteq G_i \cap H_1 \trianglerighteq G_i \cap H_2 \trianglerighteq \cdots \trianglerighteq G_i \cap H_n = \{1\},$$

wobei jeder Term ein Normalteiler des jeweils vorigen Terms ist. Multiplikation mit dem Normalteiler $G_{i+1} \trianglelefteq G_i$ liefert die Folge

$$G_i = (G_i \cap H_0)G_{i+1} \trianglerighteq (G_i \cap H_1)G_{i+1} \trianglerighteq \cdots \trianglerighteq (G_i \cap H_n)G_{i+1} = G_{i+1},$$

wobei wiederum jeder Term ein Normalteiler des jeweils vorigen Terms ist. Wir haben so den i-ten Schritt der ersten Subnormalreihe durch zusätzliche n Schritte verfeinert. Wenn wir dies für alle i machen, erhalten wir eine Verfeinerung der ersten Subnormalreihe mit insgesamt mn Schritten (wobei ausnahmsweise die Inklusionen nicht als strikt vorausgesetzt werden). Ebenso können wir die Schritte der zweiten Subnormalreihe verfeinern zu

$$H_j = (G_0 \cap H_j)H_{j+1} \trianglerighteq (G_1 \cap H_j)H_{j+1} \trianglerighteq \cdots \trianglerighteq (G_m \cap H_j)H_{j+1} = H_{j+1}.$$

Wir wollen die Faktoren dieser beiden verfeinerten Subnormalreihen miteinander vergleichen:

- Der j-te Verfeinerungsschritt im i-ten Schritt der ersten Normalreihe liefert den Faktor
$$G_{ij} := (G_i \cap H_j)G_{i+1}/(G_i \cap H_{j+1})G_{i+1}.$$
- Der i-te Verfeinerungsschritt im j-ten Schritt der zweiten Normalreihe liefert den Faktor
$$H_{ji} := (G_i \cap H_j)H_{j+1}/(G_{i+1} \cap H_j)H_{j+1}.$$

Nach dem Schmetterlingslemma mit

$$A_1 := G_{i+1} \trianglelefteq A := G_i$$
$$B_1 := H_{j+1} \trianglelefteq B := H_j$$

folgt daher die Behauptung. □

Korollar 9.13. *Je zwei Kompositionsreihen einer Gruppe sind äquivalent.*

Beweis. Kompositionsreihen haben per Definition keine echte Verfeinerung. □

Falls G eine Kompositionsreihe besitzt, sind daher die in einer beliebigen solchen Kompositionsreihe auftretenden Faktoren bis auf die Reihenfolge eindeutig. Wir bezeichnen sie auch als die *Kompositionsfaktoren der Gruppe G*.

Bemerkung 9.14. Nicht jede Anordnung der Kompositionsfaktoren einer Gruppe wird durch eine geeignete Kompositionsreihe realisiert: Z.B. kann man zeigen, dass die Gruppe $G = \mathfrak{S}_n$ für $n > 4$ nur *einen* Normalteiler hat, nämlich $\mathfrak{A}_n$. Ihre *einzige* Kompositionsreihe ist somit

$$G_0 \;=\; \mathfrak{S}_n \rhd G_1 \;=\; \mathfrak{A}_n \rhd G_2 \;=\; \{1\} \quad \text{mit} \quad G_i/G_{i+1} \;\simeq\; \begin{cases} \{\pm 1\} & \text{für } i = 0, \\ \mathfrak{A}_n & \text{für } i = 1. \end{cases}$$

Für die Reihenfolge der Kompositionsfaktoren gibt es hier keine Wahl.

Nach den abelschen Gruppen sind die einfachsten Gruppen diejenigen, welche sich als sukzessive Extensionen von abelschen Gruppen konstruieren lassen. In der Galoistheorie wird später die Frage nach der Lösbarkeit von Gleichungen durch Radikale zu solchen Gruppen führen, daher der folgende Name:

Definition 9.15. Eine Gruppe G heißt *auflösbar*, wenn sie eine Subnormalreihe

$$G \;=\; G_0 \rhd G_1 \rhd \cdots \rhd G_n \;=\; \{1\}$$

besitzt mit der Eigenschaft, dass alle Faktoren G_i/G_{i+1} abelsche Gruppen sind.

Beispiel 9.16. Es gilt:

a) Jede abelsche Gruppe ist auflösbar.

b) Eine einfache Gruppe ist auflösbar nur dann, wenn sie abelsch ist.

c) Für $n \geq 3$ ist die Diedergruppe D_n auflösbar, denn wir haben eine kurze exakte Sequenz
$$1 \longrightarrow \mu_3(\mathbb{C}) \longrightarrow D_3 \longrightarrow \{\pm 1\} \longrightarrow 1$$

d) Sei K ein Körper. Dann ist die Gruppe der oberen Dreiecksmatrizen
$$G \;=\; \left\{ \left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) \mid b \in K, a, d \in K^\times \right\}$$
auflösbar: Denn die in ihr liegenden unipotenten Matrizen bilden einen abelschen Normalteiler
$$U \;=\; \left\{ \left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right) \mid b \in K \right\} \trianglelefteq G$$
und der Quotient $G/U \simeq K^\times \times K^\times$ ist ebenfalls abelsch (Übungsaufgabe).

Lemma 9.17. *Jede p-Gruppe ist auflösbar.*

Beweis. Sei G eine p-Gruppe. Aus den Übungen wissen wir, dass $Z(G) \neq \{1\}$ ist, es gilt somit

$$|G/Z(G)| \ < \ |G|.$$

Dabei ist $G/Z(G)$ ebenfalls eine p-Gruppe. Per Induktion über die Gruppenordnung dürfen wir daher annehmen, dass der Quotient $G/Z(G)$ auflösbar ist. Aber $Z(G)$ ist als abelsche Gruppe ebenfalls auflösbar. In der exakten Sequenz

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

sind also die äußeren beiden Terme auflösbar. Dann ist G auflösbar (Übung). □

Tatsächlich erfüllen p-Gruppen sogar eine viel stärkere Eigenschaft, es handelt sich hierbei um sogenannte nilpotente Gruppen; dazu in den Übungen mehr. Die Klasse der auflösbaren Gruppen ist sehr viel größer, als es die bisherigen Beispiele vermuten lassen: Der berühmte *Satz von Feit und Thompson* (1962/63) besagt, dass jede endliche Gruppe ungerader Ordnung auflösbar ist. Der Beweis ist trotz diverser späterer Vereinfachungen leider noch immer lang und technisch.

Um die Auflösbarkeit einer Gruppe zu prüfen, müssen wir nicht alle möglichen Subnormalreihen betrachten. Es gibt ein einfaches Kriterium, das auf der folgenden allgemeinen Konstruktion von Normalteilern beruht:

Definition 9.18. Sei G eine Gruppe. Der *Kommutator von zwei Elementen* $a, b \in G$ ist definiert als

$$[a,b] \ := \ a^{-1}b^{-1}ab \ \in \ G.$$

Für Untergruppen $A, B \leq G$ setzen wir

$$[A,B] \ := \ \big\langle [a,b] \in G \mid a \in A, b \in B \big\rangle \ \leq \ G$$

Man beachte, dass die Menge aller Kommutatoren im Allgemeinen keine Gruppe bildet (man denke an die Situation für freie Gruppen); in der Definition von $[A,B]$ darf der Übergang von dieser Menge zu der davon erzeugten Untergruppe nicht vergessen werden. Die Untergruppe

$$G' \ := \ [G,G]$$

heißt die *Kommutatorgruppe* oder *derivierte Gruppe* von G.

Lemma 9.19. *Sei G eine Gruppe.*

a) Die derivierte Gruppe $G' \trianglelefteq G$ ist ein Normalteiler.

b) Der Quotient $G^{ab} := G/G'$ ist eine abelsche Gruppe.

c) Für jede abelsche Gruppe H ist $\mathrm{Hom}(G,H) \simeq \mathrm{Hom}(G^{ab},H)$.

Beweis. Folgt direkt aus den Definitionen. □

Der Quotient G^{ab} ist nach dem Lemma die größte abelsche Quotientengruppe und wird daher auch als die *Abelisierung von G* bezeichnet. Ebenso kann man die derivierte Gruppe $G' = [G,G]$ als kleinsten Normalteiler mit abelschem Quotienten ansehen. Allgemeiner definieren wir die i-te derivierte Gruppe $G^{(i)} \trianglelefteq G$ für $i \in \mathbb{N}_0$ induktiv durch

$$G^{(0)} := G \quad \text{und} \quad G^{(i+1)} := [G^{(i)}, G^{(i)}],$$

also $G^{(1)} = G'$, $G^{(2)} = G''$ usw. Wir nennen

$$G = G^{(0)} \trianglerighteq G^{(1)} \trianglerighteq G^{(2)} \trianglerighteq \cdots$$

die *derivierte Reihe* von G. Alle ihre Terme sind charakteristische Untergruppen und damit insbesondere Normalteiler in G. Die Auflösbarkeit einer Gruppe lässt sich einfach an ihrer derivierten Reihe ablesen:

Proposition 9.20. *Eine Gruppe G ist auflösbar genau dann, wenn ihre derivierte Reihe nach endlich vielen Schritten endet, d.h. wenn gilt:*

$$G^{(n)} = 1 \quad \textit{für alle genügend großen } n \in \mathbb{N}.$$

Beweis. Wenn die derivierte Reihe nach endlich vielen Schritten abbricht, ist es eine Normalreihe im Sinne unserer Definition. Die Faktoren dieser Normalreihe sind per Definition

$$G^{(i)}/G^{(i+1)} = G^{(i)}/[G^{(i)}, G^{(i)}] = (G^{(i)})^{ab}$$

und somit abelsch, also ist dann G auflösbar. Ist umgekehrt G auflösbar, so wähle man eine Subnormalreihe

$$G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_n = \{1\}$$

mit abelschen Faktoren. Wir zeigen induktiv, dass dann $G^{(i)} \leq G_i$ für alle i gilt:

Für $i = 0$ ist dies trivial. Angenommen, die Behauptung sei für ein $i \in \mathbb{N}_0$ gezeigt, es gelte also

$$G^{(i)} \leq G_i.$$

Da G_i/G_{i+1} abelsch ist, faktorisiert der Homomorphismus $G^{(i)} \to G_i \to G_i/G_{i+1}$ über die Abelisierung

$$(G^{(i)})^{ab} = G^{(i)}/G^{(i+1)}$$

Es folgt $G^{(i+1)} \leq G_{i+1}$ wie gewünscht. Ebenso wie die gewählte Subnormalreihe bricht also auch die derivierte Reihe nach endlich vielen Schritten ab. □

Kapitel II
Ringe und Polynome

Zusammenfassung In diesem Kapitel diskutieren wir einige Grundbegriffe über Ringe, insbesondere Polynomringe. In faktoriellen Ringen hat jedes Element eine eindeutige Primfaktorzerlegung; der Satz von Gauß zeigt, dass Polynomringe über beliebigen faktoriellen Ringen wieder faktoriell sind. Dies liefert Kriterien für die Irreduzibilität von Polynomen, die später in der Galoistheorie für die Beschreibung endlicher Körpererweiterungen nützlich sein werden.

1 Grundbegriffe

Wir erinnern uns aus der linearen Algebra an den Begriff eines Ringes:

Definition 1.1. Ein *Ring* ist ein Tupel $(R,+,\cdot)$ bestehend aus einer Menge R und zwei Verknüpfungen

$$+: \quad R\times R \longrightarrow R \qquad \text{und} \qquad \cdot: \quad R\times R \longrightarrow R,$$

sodass gilt:

a) $(R,+)$ ist eine *abelsche Gruppe* mit neutralem Element $0 \in R$.

b) $(R,\ \cdot\ )$ ist ein *Monoid*, d.h.

- die Multiplikation ist assoziativ: $a\cdot(b\cdot c) = (a\cdot b)\cdot c$ für alle $a,b,c \in R$.
- es gibt ein Element $1 \in R$ mit der Eigenschaft $1\cdot a = a\cdot 1 = a$ für alle $a \in R$.

c) Es gilt das *Distributivgesetz*: Für alle $a,b,c \in R$ ist

$$(a+b)\cdot c \ = \ a\cdot c + b\cdot c, \quad a\cdot(b+c) \ = \ a\cdot b + a\cdot c.$$

Der Ring R heißt *kommutativ*, wenn außerdem $a\cdot b = b\cdot a$ für alle $a,b \in R$ gilt.

Beim Distributivgesetz haben wir auf der rechten Seite jeweils keine Klammern gesetzt: Wir verwenden die übliche Konvention, dass das Multiplikationszeichen stärker bindet als das Additionszeichen. Wir schreiben $-a$ für das additive Inverse von $a \in R$. Aus den Ringaxiomen folgert man leicht die üblichen Rechenregeln wie z.B.

$$0 \cdot a \;=\; a \cdot 0 \;=\; 0, \qquad (-a) \cdot b \;=\; -(a \cdot b), \qquad (-a) \cdot (-b) \;=\; a \cdot b,$$

Wegen der Assoziativität der Multiplikation kann man Klammern um mehrfache Produkte weglassen, auch das Verknüpfungssymbol $\cdot$ lassen wir häufig weg und schreiben kurz $abc = a \cdot (b \cdot c) = (a \cdot b) \cdot c$. In jedem beliebigen Ring R bildet die Menge

$$R^\times \;:=\; \{r \in R \mid \exists s \in R : \; rs = sr = 1\}$$

der multiplikativ invertierbaren Elemente des Ringes eine Gruppe bezüglich der Multiplikation, wir nennen diese die *Einheitengruppe* und ihre Elemente *Einheiten* von R. Wir bezeichnen R als *Schiefkörper*, wenn

$$R^\times = R \setminus \{0\}$$

ist, wenn also die Einheiten des Ringes genau die von Null verschiedenen Elemente sind. Kommutative Schiefkörper bezeichnet man als *Körper*. Ein Element $a \in R$ heißt *Nullteiler*, wenn es ein $b \in R \setminus \{0\}$ gibt mit $ab = 0$ oder $ba = 0$. Schiefkörper haben offenbar die Eigenschaft, dass in ihnen das Nullelement der einzige Nullteiler ist. Unter einem *Integritätsring* verstehen wir einen kommutativen Ring R, welcher diese letzte Eigenschaft besitzt, also

$$ab \neq 0 \quad \text{für alle} \quad a, b \in R \setminus \{0\}$$

erfüllt. In Integritätsringen darf man kürzen: Aus $ac = bc$ mit $c \neq 0$ folgt $a = b$.

Beispiel 1.2. Es gilt:

a) $R = \{0\}$ ist ein Ring, der sogenannte *Nullring*: Der einzige Ring mit $0 = 1$.

b) $R = \mathbb{Z}$ ist ein Integritätsring mit der Einheitengruppe $\mathbb{Z}^\times = \{\pm 1\}$.

c) $R = \mathbb{Q}, \mathbb{R}, \mathbb{C}$ sind Körper. Die Hamiltonschen Quaternionen $\mathbb{H}$ bilden einen Schiefkörper. Wir erinnern kurz an die Konstruktion dieses Schiefkörpers: Als reeller Vektorraum ist

$$\mathbb{H} \;=\; \mathbb{R} \oplus \mathbb{R}i \oplus \mathbb{R}j \oplus \mathbb{R}k$$

ein vierdimensionaler Vektorraum mit der Basis $1, i, j, k$. Die Multiplikation ist definiert durch $\mathbb{R}$-bilineare Ausdehnung der Verknüfung auf den Basisvektoren, welche gegeben ist durch die Forderung, dass 1 das Einselement sein soll und dass gilt:

$$i^2 = j^2 = k^2 = -1, \quad ij = k = -ji, \quad jk = i = -kj, \quad ki = j = -ik.$$

d) $R = \mathbb{Z}/n\mathbb{Z}$ ist ein kommutativer Ring mit der repräsentantenweise definierten Addition und Multiplikation

$$[a]+[b] \;\coloneqq\; [a+b], \qquad [a]\cdot[b] \;\coloneqq\; [a\cdot b]$$

von Restklassen $[a],[b] \in \mathbb{Z}/n\mathbb{Z}$. In der linearen Algebra haben wir uns überlegt, dass

$$(\mathbb{Z}/n\mathbb{Z})^\times \;=\; \big\{\, [a] \in \mathbb{Z}/n\mathbb{Z} \mid \mathrm{ggT}(a,n) = 1 \big\}$$

ist und dass gilt:

$$\mathbb{Z}/n\mathbb{Z} \text{ Integritätsring} \iff \mathbb{Z}/n\mathbb{Z} \text{ Körper} \iff n = p \text{ Primzahl}$$

Für Primzahlen p bezeichnen wir den so erhaltenen Körper auch mit $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

e) Für jeden Ring S bildet die Menge $R = \mathrm{Mat}_{n\times n}(S)$ der $n \times n$ Matrizen über S einen Ring bezüglich der Addition und Multiplikation von Matrizen. Für $n > 1$ ist dieser Matrizenring nicht kommutativ. Seine Einheitengruppe ist die allgemeine lineare Gruppe

$$\mathrm{GL}_n(R) \;\coloneqq\; \big\{ A \;\in\; \mathrm{Mat}_{n\times n}(S) \mid \exists B \;\in\; \mathrm{Mat}_{n\times n}(S) : AB = BA = \mathbf{1} \big\}.$$

f) Sei I eine Indexmenge, und für jedes $i \in I$ sei ein Ring R_i gegeben. Dann ist die Produktmenge

$$R \;=\; \prod_{i\in I} R_i$$

ein Ring bezüglich der komponentenweisen Addition und Multiplikation. Für die Indexmenge $I = \{1,\dots,n\}$ schreiben wir kurz

$$R \;=\; \prod_{i=1}^{n} R_i \;=\; R_1 \times \cdots \times R_n.$$

Produkte von Ringen haben viele Nullteiler, z.B. ist $(1,0)\cdot(0,1) = (0,0)$ in $R\times R$.

In der Gruppentheorie kam dem Begriff einer Untergruppe eine wichtige Bedeutung zu. Das Analogon für Ringe sieht so aus:

Definition 1.3. Ein *Teilring* eines Ringes S ist eine Teilmenge $R \subseteq S$, die sowohl eine additive Untergruppe als auch ein multiplikatives Untermonoid ist, also eine nichtleere Teilmenge $R \subseteq S$ mit der Eigenschaft:

$$\forall\, a,b \in R: \quad a-b \in R, \quad ab \in R.$$

In diesem Fall bildet offenbar R selber wieder einen Ring bezüglich der Addition und Multiplikation von S. Wir sagen auch, dass $R \subseteq S$ eine *Ringerweiterung* sei.

Beispielsweise sind $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{H}$ Ringerweiterungen. Eine wichtige Quelle für Ringerweiterungen sind Polynomringe, die wir schon aus der linearen Algebra kennen:

Definition 1.4. Sei R ein kommutativer Ring. Wir definieren den *Polynomring* $R[x]$ in der Variable x als die Menge

$$R[x] \coloneqq \left\{ (a_k)_{k\in\mathbb{N}_0} \in R^{\mathbb{N}_0} \mid \exists n \in \mathbb{N}_0 \, \forall k > n \; a_k = 0 \right\}$$

der endlichen Folgen von Elementen in R. Die Folgen sollte man als Folgen von Koeffizienten ansehen: Für $f = (a_k)_{k\in\mathbb{N}_0} \in R$ mit $a_k = 0$ für alle $k > n$ schreiben wir suggestiver

$$f(x) \;=\; a_0 + a_1 x + \cdots + a_n x^n \;=\; \sum_{k=0}^{n} a_k x^k$$

wobei nicht vergessen werden darf, dass x hier nur eine formale Variable darstellt und kein Element von R. Die Summe und das Produkt von Polynomen

$$f \;=\; (a_i)_{i\in\mathbb{N}_0} \quad \text{und} \quad g \;=\; (b_j)_{j\in\mathbb{N}_0} \quad \text{in} \quad R[x]$$

definieren wir durch

$$\begin{aligned} f+g &\coloneqq (c_k)_{k\in\mathbb{N}_0} && \text{mit} \quad c_k \;=\; a_k + b_k, \\ f\cdot g &\coloneqq (d_k)_{k\in\mathbb{N}_0} && \text{mit} \quad d_k \;=\; \sum_{i+j=k} a_i b_j. \end{aligned}$$

Man prüft leicht nach, dass diese Definition $(R[x], +, \cdot)$ zu einem kommutativen Ring macht. In Polynomschreibweise mit den Potenzen einer formalen Variablen x liefern die obigen Formeln natürlich genau die gewohnten Formeln. Wir erhalten eine Ringerweiterung $R \subset R[x]$, indem wir Elemente $r \in R$ auffassen als Polynome von der Form

$$f(x) \;=\; r + 0\cdot x + 0\cdot x^2 + \cdots$$

Unter dem *Nullpolynom* verstehen wir das Nullelement des Ringes $R[x]$, also das Polynom, dessen Koeffizienten alle Null sind. Der *Grad* von Polynomen ist definiert durch

$$\deg(f) \;\coloneqq\; \begin{cases} n & \text{für } f(x) = \sum_{k=0}^{n} a_k x^k \text{ mit } a_n \neq 0, \\ -\infty & \text{für das Nullpolynom } f(x) = 0. \end{cases}$$

Im ersten Fall nennen wir a_n auch den *Leitkoeffizienten* von f und bezeichnen das Polynom als *normiert*, wenn sei Leitkoeffizient 1 ist.

Bemerkung 1.5. In dem Polynom $f = a_0 + a_1 x + \cdots + a_n x^n \in R[x]$ ist x eine formale Variable. Wenn wir für die Variable konkrete Ringelemente einsetzen, erhalten wir konkrete Werte

$$f(r) \;\coloneqq\; a_0 + a_1 r + \cdots + a_n r^n \;\in\; R \quad \text{für} \quad r \;\in\; R.$$

Ein Ringelement $r \in R$ heißt eine *Nullstelle* von $f \in R[x]$, falls $f(r) = 0$ ist. Die Abbildung

$$R \;\longrightarrow\; R, \quad r \;\mapsto\; f(r)$$

heißt die *Polynomfunktion* zum Polynom f. Der Grund für die Unterscheidung von Polynomen und Polynomfunktionen wird klar, wenn man das vom Nullpolynom verschiedene Polynom

$$f(x) \;=\; x^p - x \;\in\; \mathbb{F}_p[x]$$

für p prim betrachtet: Seine Polynomfunktion ist die Nullfunktion!

Bemerkung 1.6. Für das Rechnen mit Polynomen über Ringen gilt:

a) $\deg(f+g) \leq \max\{\deg(f), \deg(g)\}$, mit Gleichheit im Fall $\deg(f) \neq \deg(g)$.

b) $\deg(f \cdot g) \leq \deg(f) + \deg(g)$, mit Gleichheit für Integritätsringe R.

c) Der Polynomring $R[x]$ ist ein Integritätsring genau dann, wenn R es ist.

d) Durch Polynome $g(x) = a_0 + a_1 x + \cdots + a_d x^d \in R[x]$, die eine Einheit $a_d \in R^\times$ als Leitkoeffizient haben, kann man auf eindeutige Weise mit Rest dividieren: Für jedes $f \in R[x]$ existieren eindeutige $q, r \in R[x]$ mit

$$f \;=\; qg + r \quad \text{und} \quad \deg(r) \;<\; d.$$

Beweis. Genauso wie für Polynome über Körpern (siehe lineare Algebra). □

2 Homomorphismen und Ideale

Ähnlich wie im Fall von Gruppen wollen wir auch im Fall von Ringen Abbildungen betrachten, welche die Ringstruktur erhalten:

Definition 2.1. Ein *Ringhomomorphismus* ist eine Abbildung $\varphi : R \to S$ zwischen zwei Ringen, die ein Homomorphismus sowohl von additiven Gruppen als auch von multiplikativen Monoiden ist, also für alle $a, b \in R$ die folgenden Eigenschaften erfüllt:

a) Es ist $\varphi(a+b) = \varphi(a) + \varphi(b)$ für alle $a, b \in R$.

b) Es ist $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$ für alle $a, b \in R$, und $\varphi(1) = 1$.

Wir bezeichnen mit $\mathrm{Hom}(R, S)$ die Menge aller solcher Ringhomomorphismen.

Bemerkung 2.2. Die Abbildung $\varphi : \mathbb{Z} \longrightarrow \mathbb{Z}, n \mapsto 2n$ ist *kein* Ringhomomorphismus im Sinn der obigen Definition, weil sie das Einselement nicht auf das Einselement abbildet. Für jeden Ring R gibt es genau einen Homomorphismus $\varphi : \mathbb{Z} \longrightarrow R$ von Ringen, dieser ist gegeben durch

$$\varphi(n) \;=\; n \cdot 1 \;:=\; 1 + \cdots + 1 \;\in\; R \quad \text{für} \quad n \;\in\; \mathbb{Z}.$$

Denn dieselbe Aussage für Homomorphismen additiver Gruppen mit $\varphi(1) = 1$ ist klar; man rechnet dann direkt nach, dass der auf diese Weise erhaltene eindeutige Gruppenhomomorphismus ein Ringhomomorphismus ist.

Die Bedeutung von Polynomringen für die Untersuchung kommutativer Ringe erklärt sich daraus, dass man für ihre Variablen nicht nur Elemente des gegebenen Ringes, sondern auch Elemente von Ringerweiterungen einsetzen kann. Wir wollen dies gleich für Polynome in mehreren Variablen betrachten:

Definition 2.3. Wir definieren rekursiv

$$R[x_1,\dots,x_n] \;:=\; \big(R[x_1,\dots,x_{n-1}]\big)[x_n]$$

für $n>1$. Die Elemente dieses Polynomringes in mehreren Variablen schreiben wir als endliche Summen

$$f(x_1,\dots,x_n) \;=\; \sum_{I\in\mathbb{N}^n} a_I x^I \quad \text{mit Koeffizienten} \quad a_I \,\in\, R,$$

wobei wir die Multiindexnotation $x^I := x_1^{i_1}\cdots x_n^{i_n}$ für $I=(i_1,\dots,i_n)$ benutzen. Für induktive Argumente ist es oft praktisch, für die Monome bzw. die Multiexponenten die *lexikographische Ordnung* zu verwenden, diese ist definiert durch

$$\begin{aligned} x_1^{i_1}\cdots x_n^{i_n} \;\succ\; x_1^{j_1}\cdots x_n^{j_n} \quad &:\Longleftrightarrow \quad (i_1,\dots,i_n) \;\succ\; (j_1,\dots,j_n) \\ &:\Longleftrightarrow \quad \exists k:\; i_\nu = j_\nu \text{ für alle } \nu<k, \text{ aber } i_k > j_k. \end{aligned}$$

Wir können so beispielsweise den *Multigrad* eines Polynoms in $x_1,\dots,x_n$ definieren durch

$$\deg(f) \;:=\; \max\{I \mid a_I\neq 0\} \;\in\; \mathbb{N}_0^n \quad \text{für} \quad f(x_1,\dots,x_n) \;=\; \sum_I a_I x^I \;\neq\; 0,$$

wobei das Maximum bezüglich der lexikographischen Ordnung genommen wird.

Satz 2.4 (Universelle Eigenschaft von Polynomringen). *Es sei $\varphi : R \longrightarrow S$ ein Homomorphismus von kommutativen Ringen, und es seien Elemente $s_1,\dots,s_n \in S$ gegeben. Dann gibt es genau einen Ringhomomorphismus*

$$\Phi: \quad R[x_1,\dots,x_n] \;\longrightarrow\; S$$

mit folgenden beiden Eigenschaften:

a) Auf dem Teilring $R\subset R[x_1,\dots,x_n]$ ist $\Phi|_R=\varphi$.

b) Das Polynom $x_i\in R[x_1,\dots,x_n]$ wird abgebildet auf $\Phi(x_i)=s_i$ für $i=1,\dots,n$.

Beweis. Wenn ein solcher Ringhomomorphismus existiert, dann muß nach $a)$, $b)$ offenbar

$$\Phi\Big(\sum_I a_I x^I\Big) \;=\; \sum_I \varphi(a_I)\cdot s_1^{i_1}\cdots s_n^{i_n}$$

gelten. Umgekehrt definiert diese Formel einen Ringhomomorphismus. □

Falls $\varphi : R \hookrightarrow S$ die Inklusion eines Teilringes ist und die Inklusionsabbildung aus dem Kontext klar ist, bezeichnen wir den obigen Ringhomomorphismus kurz mit

$$R[x_1,\ldots,x_n] \longrightarrow S, \quad f(x_1,\ldots,x_n) \mapsto f(s_1,\ldots,s_n).$$

Wir wollen nun einen etwas genaueren Blick auf Ringhomomorphismen werfen und insbesondere ein Analogen des Homomorphiesatzes aus der Gruppentheorie formulieren. Die Begriffe *Mono-*, *Epi-* und *Isomorphismus* definieren wir im Fall von Ringhomomorphismen genauso wie für Gruppenhomomorphismen, dasselbe gilt für den *Kern* und das *Bild*

$$\ker(\varphi) := \{a \in R \mid \varphi(a) = 0\} \quad \text{und} \quad \operatorname{im}(\varphi) := \{f(a) \in S \mid a \in R\}.$$

Direkt aus der Definition sieht man, dass das Bild $\operatorname{im}(\varphi) \subseteq S$ ein Teilring ist. Der Kern $\ker(\varphi) \subseteq R$ ist allerdings *kein* Teilring, außer im trivialen Fall $S = \{0\}$; es handelt sich hierbei um ein Ideal:

Definition 2.5. Sei R ein Ring. Eine additive Untergruppe $I \subseteq R$ heißt

a) ein *Linksideal*, wenn $r \cdot a \in I$ ist für alle $a \in I$ und alle $r \in R$.

b) ein *Rechtsideal*, wenn $a \cdot r \in I$ ist für alle $a \in I$ und alle $r \in R$.

c) ein *Ideal*, wenn sie sowohl ein Links- als auch ein Rechtsideal ist.

Die Ideale $I = \{0\}$ und $I = R$ heißen das *Nullideal* und das *Einsideal*. Allgemeiner bezeichnen wir für je endlich viele Ringelemente $a_1,\ldots,a_n$ mit $(a_1,\ldots,a_n) \subseteq R$ das kleinste diese Elemente enthaltende Ideal und bezeichnen dieses als das von den gegebenen Elementen *erzeugte Ideal*, im Fall $n = 1$ auch als ein *Hauptideal*. In kommutativen Ringen ist

$$\begin{aligned}(a_1,\ldots,a_n) &= a_1R + \cdots + a_nR \\ &= \{a_1r_1 + \cdots + a_nr_n \mid r_1,\ldots,r_n \in R\},\end{aligned}$$

in nicht-kommutativen Ringen ist die Beschreibung auch für Hauptideale etwas komplizierter, wird aber für uns im Folgenden keine Rolle spielen. Die folgende Aussage zeigt, dass Ideale genau das ringtheoretische Pendant zu Normalteilern in der Gruppentheorie sind:

Proposition 2.6. *Sei R ein Ring. Für additive Untergruppen $I \subseteq R$ sind äquivalent:*

a) $I = \ker(\varphi)$ ist der Kern eines Ringhomomorphismus $\varphi : R \to S$.

b) $I \subseteq R$ ist ein Ideal.

c) Die additive Gruppe R/I trägt eine Ringstruktur, sodass

$$p: \quad R \longrightarrow R/I, \quad a \mapsto a+I \quad \textit{ein Ringhomomorphismus ist.}$$

Beweis. Wenn $I = \ker(\varphi)$ ist, gilt für beliebige $r \in R$, $a \in I$ auch $r \cdot a \in I$ und $a \cdot r \in I$ wegen

$$\varphi(r \cdot a) \;=\; \varphi(r) \cdot \varphi(a) \;=\; \varphi(r) \cdot 0 \;=\; 0 \quad \text{und analog} \quad \varphi(a \cdot r) \;=\; 0.$$

Also ist $I \subseteq R$ ein Ideal. Wenn letzteres gilt, wird auf der additiven Gruppe R/I durch

$$\cdot : \quad R/I \times R/I \;\longrightarrow\; R/I, \quad (a+I) \cdot (b+I) \;:=\; (ab+I)$$

eine Verknüpfung wohldefiniert: Denn seien $a, a' \in R$ mit $a+I = a'+I$ und $b, b' \in R$ mit $b+I = b'+I$ verschiedene Repräsentanten für dieselben Nebenklassen, dann gilt:

- $(a'-a)b' \in I$, weil $a'-a \in I$ und I ein Rechtsideal ist.
- $a(b'-b) \in I$, weil $b'-b \in I$ und I ein Linksideal ist.

Es folgt $a'b' - ab = (a'-a)b' + a(b'-b) \in I$ und somit ist $ab+I = a'b'+I$ wie gewünscht. Die so definierte Multiplikation definiert offenbar eine Ringstruktur auf der Gruppe R/I, und zwar die einzige Ringstruktur, sodass

$$p : \quad R \;\longrightarrow\; R/I, \quad r \;\mapsto\; r+I$$

ein Ringhomomorphismus ist. Ist umgekehrt p ein Ringhomomorphismus, dann ist die Untergruppe $I = \ker(p)$ natürlich der Kern eines Ringhomomorphismus. □

Wie in der Gruppentheorie ist ein Ringhomomorphismus injektiv genau dann, wenn sein Kern trivial ist. Beispielsweise ist jeder Ringhomomorphismus von einem Körper in einen beliebigen anderen Ring injektiv, denn es gilt:

Lemma 2.7. *Ein kommutativer Ring $R \neq \{0\}$ ist ein Körper genau dann, wenn er kein vom Nullideal verschiedenes echtes Ideal besitzt.*

Beweis. Angenommen, der kommutative Ring R hat kein von Null verschiedenes echtes Ideal. Für jedes $a \in R \setminus \{0\}$ muß dann das davon erzeugte Ideal $aR = R$ sein, also folgt $ab = 1$ für ein Element $b \in R$ und somit ist $R^\times = R \setminus \{0\}$; also ist R ein Körper. Die Umkehrung folgt analog. □

Bei der Konstruktion von Isomorphismen von Gruppen kam eine zentrale Rolle dem Homomorphiesatz zu. Dasselbe gilt auch in der Ringtheorie:

Satz 2.8 (Homomorphiesatz). *Jeder Ringhomomorphismus $\varphi : R \to S$ induziert einen Isomorphismus*

$$\overline{\varphi} : \quad R/I \;\xrightarrow{\sim}\; \operatorname{im}(\varphi) \quad \textit{mit} \quad I \;:=\; \ker(\varphi).$$

Beweis. Wie im Homomorphiesatz für Gruppen. □

Beispiel 2.9. Nach der universellen Eigenschaft von Polynomringen können wir in reelle Polynome die komplexe Zahl $i \in \mathbb{C}$ einsetzen und erhalten auf diese Weise einen Ringhomomorphismus

$$\varphi: \quad R = \mathbb{R}[x] \longrightarrow \mathbb{C}, \quad f(x) \mapsto f(i).$$

Dieser Homomorphismus ist surjektiv, da er das Polynom $f(x) = a + bx$ auf die komplexe Zahl $a + ib$ abbildet. Sein Kern besteht per Definition aus allen reellen Polynomen, die als komplexe Polynome eine Nullstelle im Punkt i besitzen. Wegen

$$\overline{f(z)} = f(\bar{z}) \quad \text{für reelle Polynome } f(x) \in \mathbb{R}[x] \text{ und } z \in \mathbb{C}$$

ist aber mit jeder komplexen Nullstelle eines reellen Polynoms auch ihr komplex Konjugiertes eine Nullstelle. Somit gilt:

$$\begin{aligned} f \in \ker(\varphi) &\iff f(i) = 0 \\ &\iff f(i) = f(-i) = 0 \\ &\iff f(x) = (x-i)(x+i)q(x) \text{ für ein } q(x) \in \mathbb{R}[x] \end{aligned}$$

wobei wir im letzten Schritt Polynomdivision durch $g(x) = (x-i)(x+i) = x^2+1$ verwendet haben. Der Kern ist also das Hauptideal

$$\ker(\varphi) = (x^2+1) \subseteq \mathbb{R}[x]$$

und wir erhalten nach dem Homomorphiesatz eine Beschreibung des Körpers $\mathbb{C}$ als Quotientenring

$$\mathbb{R}[x]/(x^2+1) \xrightarrow{\sim} \mathbb{C}.$$

3 Primideale und maximale Ideale

Wir werden später ähnlich wie im vorigen Beispiel Erweiterungen von Körpern als Quotienten von Polynomringen schreiben. Die Frage, wann der Quotient ein Körper ist, führt auf den folgenden Begriff:

Definition 3.1. Sei R ein kommutativer Ring. Ein Ideal $I \subseteq R$ mit $I \neq R$ heißt

a) ein *Primideal*, wenn für alle $a, b \in R$ gilt: Aus $ab \in I$ folgt $a \in I$ oder $b \in I$.

b) ein *maximales Ideal*, wenn es kein Ideal $J \subseteq R$ gibt mit $I \subsetneq J \subsetneq R$.

Wir erhalten das folgende Kriterium:

Proposition 3.2. *Sei R ein kommutativer Ring und $I \subseteq R$ ein Ideal.*

a) R/I ist ein Integritätsring genau dann, wenn I ein Primideal ist.

b) R/I ist ein Körper genau dann, wenn I ein maximales Ideal ist.

Beweis. Sei $I \subseteq R$ ein Ideal, und sei $p : R \to R/I$ die Quotientenabbildung. Dann gilt

$$x \in I \quad \Longleftrightarrow \quad p(x) = 0 \in R/I$$

Für $x \in \{a, b, ab\}$ mit $a, b \in R$ folgt aus den Definitionen und aus $p(ab) = p(a)p(b)$ sofort die Äquivalenz der beiden Aussagen in Teil a). Für Teil b) beachte man, dass die im folgenden Diagramm gezeigten Abbildungen

$$\left\{ \text{Ideale } J \subseteq R \text{ mit } I \subseteq J \right\} \underset{\bar{J} \mapsto p^{-1}(\bar{J})}{\overset{J \mapsto p(J)}{\rightleftarrows}} \left\{ \text{Ideale } \bar{J} \subset R/I \right\}$$

zueinander inverse Bijektionen sind. Für $I \neq R$ ist dabei $R/I \neq \{0\}$. Somit erhalten wir die Äquivalenz

$$I \subsetneq R \text{ ist maximal} \quad \Longleftrightarrow \quad (0) \subsetneq R/I \text{ ist maximal} \quad \Longleftrightarrow \quad R/I \text{ ist ein Körper}$$

wie behauptet. □

Beispiel 3.3. Es gilt:

a) Nach der vorigen Proposition ist jedes maximale Ideal prim. Die Umkehrung gilt nicht: In Integritätsringen ist das Nullideal prim, aber nicht maximal.

b) In $R = \mathbb{Z}$ sind die maximalen Ideale genau die Ideale (p) mit Primzahlen p. Das einzige weitere Primideal ist das Nullideal.

c) In $R = \mathbb{Q}[x_1, \ldots, x_n]$ haben wir eine echt aufsteigende Kette von Primidealen

$$(0) \subsetneq (x_1) \subsetneq (x_1, x_2) \subsetneq \cdots \subsetneq (x_1, \ldots, x_n).$$

Von diesen kann also höchstens das letzte ein maximales Ideal sein. Dass es tatsächlich eines ist, sieht man anhand der vorigen Proposition: Denn für den Epimomorphismus

$$\varphi : \quad R = \mathbb{Q}[x_1, \ldots, x_n] \twoheadrightarrow \mathbb{Q}, \quad f(x_1, \ldots, x_n) \mapsto f(0, \ldots, 0)$$

gilt $(x_1, \ldots, x_n) \subseteq \ker(\varphi)$, nach dem Homomorphiesatz faktorisiert er somit über einen Epimorphismus

$$\overline{\varphi} : \quad \mathbb{Q}[x_1, \ldots, x_n]/(x_1, \ldots, x_n) \twoheadrightarrow \mathbb{Q}$$

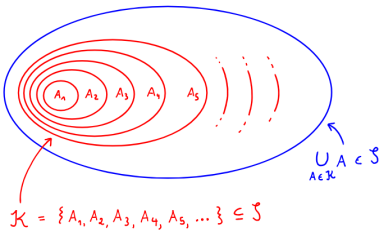
und man prüft leicht nach, dass letzterer sogar ein Isomorphismus ist.

Jeder Ring hat mindestens ein maximales Ideal und damit einen Homomorphismus in einen Körper. Um dies allgemein zu zeigen, brauchen wir etwas Mengenlehre ähnlich wie für die Existenz von Basen in unendlichdimensionalen Vektorräumen in der linearen Algebra:

Proposition 3.4. *Jeder Ring $R \neq \{0\}$ besitzt ein maximales Ideal.*

Beweis. Wir erinnern uns an das Lemma von Zorn, das in der Mengenlehre die Existenz maximaler Elemente kontrolliert:

- Sei $(\mathscr{S}, \preceq)$ eine partiell geordnete Menge.
- Eine *Kette in* $\mathscr{S}$ ist eine total geordnete Teilmenge $\mathscr{K} \subseteq \mathscr{S}$.
- Eine *obere Schranke von* $\mathscr{K}$ *in* $\mathscr{S}$ ist ein $S \in \mathscr{S}$ mit $K \preceq S$ für alle $K \in \mathscr{K}$.
- Ein Element $S \in \mathscr{S}$ heißt *maximal*, wenn kein $S' \in \mathscr{S}$ existiert mit $S \preceq S'$, $S \neq S'$.



Das Lemma von Zorn besagt:

Wenn in $\mathscr{S}$ jede Kette eine obere Schranke hat, gibt es ein maximales $S \in \mathscr{S}$.

Wir verwenden dies im Folgenden für die durch die Inklusion gegebene partielle Ordnung auf der Menge

$$\mathscr{S} := \{I \subsetneq R \mid I \neq R \text{ ist ein Ideal von } R\}$$

der echten Ideale von R. Um das Lemma von Zorn auf diese Menge anwenden zu können, müssen wir zeigen, dass für jede Kette $\mathscr{K} \subseteq \mathscr{S}$ von echten Idealen auch die Vereinigung

$$I := \bigcup_{K \in \mathscr{K}} K \subseteq R$$

ein echtes Ideal ist. Dies sieht man wie folgt:

- Zunächst ist I ein Ideal von R: Seien $a_1, a_2 \in I$. Per Definition gibt es $K_i \in \mathscr{K}$ mit $a_i \in K_i$. Wegen der Ketteneigenschaft von $\mathscr{K}$ können wir nach Umnumerieren annehmen, dass $K_1 \subseteq K := K_2$ ist. Dann ist also $a_1, a_2 \in K$, und weil $K \subseteq R$ ein Ideal ist, folgt
$$a_1 + r a_2 \in K \subseteq I \quad \text{für alle} \quad r \in R.$$
- Zudem ist $I \subsetneq R$ ein echtes Ideal: Denn im Fall $I = R$ wäre $1 \in I$. Per Definition der Vereinigung gäbe es dann ein $K \in \mathscr{K}$ mit $1 \in K$, im Widerspruch zu $K \neq R$.

Somit ist das Lemma von Zorn anwendbar und liefert ein maximales Ideal. □

4 Quotientenkörper

Aus dem Ring der ganzen Zahlen erhält man den Körper der rationalen Zahlen durch Bilden von Brüchen. Allgemeiner kann man so vorgehen:

Definition 4.1. Sei R ein kommutativer Ring und $S \subseteq R$ ein Untermonoid, also eine Teilmenge mit

$$1 \in S \quad \text{und} \quad a \cdot b \in S \quad \text{für alle} \quad a, b \in S.$$

Wir nennen $S \subseteq R$ auch eine *multiplikative Teilmenge*. Sei $S^{-1}R := (R \times S)/\sim$ für die Äquivalenzrelation $\sim$ definiert durch

$$(r_1, s_1) \sim (r_2, s_2) \quad :\Longleftrightarrow \quad \exists s \in S : \; s \cdot (r_1 s_2 - r_2 s_1) = 0$$

Dass es sich hierbei um eine Äquivalenzrelation handelt, rechnet man sofort nach; der Vorfaktor $s \in S$ wird wegen möglicher Nullteiler benötigt und kann im Fall von Integritätsringen weggelassen werden. Wir schreiben die Äquivalenzklassen eines Paares $(r,s) \in R \times S$ formal als

$$\frac{r}{s} := \big[(r,s) \text{ modulo } \sim\big] \in S^{-1}R$$

und definieren auf der Menge solcher Brüche die Addition und Multiplikation durch die Formeln

$$\frac{r_1}{s_1} + \frac{r_2}{s_2} := \frac{r_1 s_2 + r_2 s_1}{s_1 s_2} \quad \text{und} \quad \frac{r_1}{s_1} \cdot \frac{r_2}{s_2} := \frac{r_1 r_2}{s_1 s_2}.$$

Man rechnet leicht nach, dass diese Addition und Multiplikation wohldefiniert sind und $S^{-1}R$ zu einem Ring machen. Wir bezeichnen diesen Ring als die *Lokalisierung* des kommutativen Ringes R an der Teilmenge $S \subseteq R$.

Beispiel 4.2. Es gilt:

a) Für Integritätsringe R ist $R \setminus \{0\}$ ein Untermonoid. Die Lokalisierung an diesem ist ein Körper, wir nennen ihn den *Quotientenkörper* von R und bezeichnen ihn mit
$$\operatorname{Quot}(R) := S^{-1}R \quad \text{für} \quad S = R \setminus \{0\}.$$

b) Sei $R = \mathbb{Z}$ und $S = \{p^n \mid n \in \mathbb{N}_0\}$ für eine Primzahl p. Die Lokalisierung an S ist hier
$$\mathbb{Z}[1/p] := \Big\{a/p^n \in \mathbb{Q} \mid a \in \mathbb{Z}, n \in \mathbb{N}_0\Big\} \subset \mathbb{Q}.$$

c) Sei $R = \mathbb{Z}$ und $S = \{s \in \mathbb{Z} \mid p \nmid s\}$ für eine Primzahl p. Die Lokalisierung an S ist hier
$$\mathbb{Z}_{(p)} := \Big\{a/b \in \mathbb{Q} \mid a, b \in \mathbb{Z}, p \nmid b\Big\} \subset \mathbb{Q}.$$

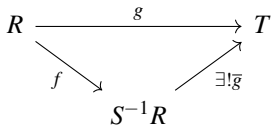
Die Lokalisierung $S^{-1}R$ lässt sich durch die folgende universelle Eigenschaft charakterisieren:

Satz 4.3. *Sei R ein kommutativer Ring und $S \subset R$ eine multiplikative Teilmenge.*

a) Die Lokalisierungsabbildung $f : R \longrightarrow S^{-1}R, a \mapsto \frac{a}{1}$ ist ein Homomorphismus von Ringen mit

$$f(S) \subseteq (S^{-1}R)^\times$$

b) Jeder Homomorphismus $g : R \longrightarrow T$ in einen Ring T mit $g(S) \subseteq T^\times$ faktorisiert eindeutig über diese Lokalisierungsabbildung wie in dem folgenden Diagramm gezeigt:



Beweis. Übungsaufgabe. □

Wir werden hier nur Quotientenkörper benötigen; die allgemeine Lokalisierung an beliebigen multiplikativen Teilmengen erlaubt es, gezielt nur einzelne Primideale eines Ringes zu betrachten:

Übung 4.4. Man zeige, dass die Lokalisierungsabbildung $R \longrightarrow S^{-1}R$ zueinander inverse Bijektionen

$$\left\{ \text{Primideale } I \subseteq R \text{ mit } I \cap S = \varnothing \right\} \rightleftarrows \left\{ \text{Primideale } J \subset S^{-1}R \right\}$$

induziert, und bestimme alle Primideale der Ringe $\mathbb{Z}[1/p]$ und $\mathbb{Z}_{(p)}$.

5 Faktorielle Ringe und das Lemma von Gauss

Im Folgenden sei stets R ein Integritätsring. In der linearen Algebra haben wir uns bereits mit den Grundbegriffen der Teilbarkeitstheorie beschäftigt:

Definition 5.1. Seien $a, b \in R$.

- b heißt ein *Teiler* von a, wenn $a = bc$ für ein $c \in R$ ist. Wir schreiben dann $b \mid a$.
- b heißt *assoziiert* zu a, wenn $a = bc$ für ein $c \in R^\times$ ist. Wir schreiben dann $b \sim a$.

Für die von den Elementen erzeugten Hauptideale gilt offenbar:

$$\begin{aligned} b \mid a &\iff bR \supseteq aR \\ b \sim a &\iff bR = aR \end{aligned}$$

Der Begriff einer Primzahl lässt sich auf zwei verschiedene Arten verallgemeinern:

Definition 5.2. Ein Element $p \in R$ mit $p \notin R^\times \cup \{0\}$ heißt

a) *prim*, wenn aus $p \mid ab$ folgt, dass $p \mid a$ oder $p \mid b$ ist.

b) *irreduzibel*, wenn aus $p = ab$ folgt, dass $a \in R^\times$ oder $b \in R^\times$ ist.

Aus der Definition folgt sofort, dass jedes Primelement irreduzibel ist. Allerdings gilt die Umkehrung im Allgemeinen nicht! Wir interessieren uns im Folgenden für Ringe, in denen jedes Element eine Primfaktorzerlegung besitzt:

Definition 5.3. Ein *faktorieller Ring* ist ein Integritätsring R, in dem es für jedes Element $a \in R \setminus (R^\times \cup \{0\})$ eine Zerlegung

$$a \;=\; p_1 \cdots p_n$$

mit Primelementen $p_1, \ldots, p_n \in R$ gibt. Die Primelemente müssen dabei natürlich nicht paarweise verschieden sein, Mehrfachnennungen sind erlaubt. In der Praxis wählt man meist ein Repräsentantensystem $\mathscr{P} \subset R$ für die Primelemente modulo Assoziiertheit und schreibt

$$a \;=\; u \cdot \prod_{p \in \mathscr{P}} p^{m_p}$$

mit einer Einheit $u \in R^\times$ und Exponenten $m_p \in \mathbb{N}_0$, die fast alle Null sind.

Aus der Definition von Primelementen folgt, dass eine solche Zerlegung im Falle ihrer Existenz im Wesentlichen eindeutig ist:

Proposition 5.4. *Sei R ein Integritätsring, und es seien $m_p, n_p \in \mathbb{N}_0$ (fast alle Null) und $u, v \in R^\times$ mit*

$$u \cdot \prod_{p \in \mathscr{P}} p^{m_p} \;=\; v \cdot \prod_{p \in \mathscr{P}} p^{n_p}$$

gegeben. Dann ist $u = v$ und für alle Primelemente $p \in \mathscr{P}$ gilt $m_p = n_p$.

Beweis. Auf beiden Seiten kommen nur endlich viele Primelemente mit positiven Exponenten vor. Es reicht daher zu zeigen: Sind $p_1, \ldots, p_m, q_1, \ldots, q_n$ Primelemente mit

$$p_1 \cdots p_m \;\sim\; q_1 \cdots q_n,$$

dann ist $m = n$, und es gibt eine Permutation $\sigma \in \mathfrak{S}_n$ mit $q_i \sim p_{\sigma(i)}$ für $i \in \{1, \ldots, n\}$.

Wir verwenden Induktion über $\max\{m, n\}$. Da p_m ein Primelement ist, folgt aus der Teilbarkeit $p_m \mid q_1 \cdots q_n$ die Existens eines Index i mit $p_m \mid q_i$. Aber q_i ist als Primelement insbesondere irreduzibel, also ist $p_m \sim q_i$. Wir dürfen dabei durch Umnumerieren der Indices $i = n$ annehmen. Durch Kürzen des Elementes p_m folgt dann $p_1 \cdots p_{m-1} \sim q_1 \cdots q_{n-1}$ und damit per Induktion die Behauptung. □

Insbesondere können wir in jedem faktoriellen Ring R für beliebige Elemente mit der Primfaktorzerlegung

$$a_i \;=\; u_i \cdot \prod_{p\in\mathscr{P}} p^{m_p(a_i)}$$

ihren *größten gemeinsamen Teiler* und ihr *kleinstes gemeinsames Vielfaches* wie gewohnt definieren durch

$$\mathrm{ggT}(a_1,\ldots,a_n) \;:=\; \prod_{p\in\mathscr{P}} p^{m_p} \qquad \text{mit} \quad m_p \;:=\; \min\{m_p(a_i) \mid 1\le i\le n\},$$

$$\mathrm{kgV}(a_1,\ldots,a_n) \;:=\; \prod_{p\in\mathscr{P}} p^{n_p} \qquad \text{mit} \quad n_p \;:=\; \max\{m_p(a_i) \mid 1\le i\le n\}.$$

Man beachte, dass diese bis auf Multiplikation mit Einheiten nicht von der Wahl des Repräsentantensystems $\mathscr{P}$ abhängen. Wir sehen sie als Elemente von $K^\times/R^\times$ an.

Die *Eindeutigkeit* der Primfaktorzerlegung haben wir direkt aus der Definition eines Primelementes erhalten. Die Frage nach der *Existenz* einer solchen Zerlegung ist heikler: In der Regel ist es einfacher, die Existenz einer Zerlegung als Produkt von irreduziblen Elemente zu zeigen. Die folgende Charakterisierung faktorieller Ringen macht klar, was dann noch fehlt:

Satz 5.5. *Ein Integritätsring R ist faktoriell genau dann, wenn er folgende beiden Eigenschaften besitzt:*

a) Jedes $a \in R\setminus(R^\times\cup\{0\})$ ist ein Produkt irreduzibler Elemente.

b) Jedes irreduzible Element $q \in R$ ist ein Primelement.

Beweis. Aus $a)$ und $b)$ folgt trivialerweise, dass R faktoriell ist. Ist umgekehrt R faktoriell, so besitzt jede von Null verschiedene nicht-Einheit eine Zerlegung als ein Produkt von Primelementen; da Primelemente irreduzibel sind, gilt dann $a)$. Zudem hat dann jedes irreduzible Element $q \in R$ eine Zerlegung als Produkt $q = p_1\cdots p_n$ von Primelementen $p_i \in R$. Wegen der Irreduzibilität muß dabei $n = 1$ sein, also ist q prim und somit gilt auch $b)$. □

Beispiel 5.6. In dem Ring

$$\mathbb{Z}[\sqrt{-5}] \;:=\; \{a+ib\sqrt{5}\in\mathbb{C} \mid a,b\in\mathbb{Z}\}$$

besitzt jedes Element eine Zerlegung als Produkt irreduzibler Elemente, wie man beispielsweise durch Betrachten des Absolutbetrags von Elementen sieht; aber der Ring R ist *nicht* faktoriell, denn man kann sich überlegen, dass in der folgenden Zerlegung

$$(1+i\sqrt{5})\cdot(1-i\sqrt{5}) \;=\; 2\cdot 3$$

alle vier Faktoren irreduzibel und paarweise nicht-assoziiert sind. Dies zeigt nach dem obigen Satz auch, dass keiner der irreduziblen Faktoren ein Primelement ist.

Beispiel 5.7. In der linearen Algebra haben wir gesehen:

a) Jeder Hauptidealring ist faktoriell. Insbesondere ist für jeden Körper K auch der Polynomring $K[x]$ ein faktorieller Ring.

b) Die Polynomringe $\mathbb{Z}[x]$ und $K[x,y]$ sind keine Hauptidealringe, beispielsweise sind die Ideale
$$(2,x) \subseteq \mathbb{Z}[x] \quad \text{und} \quad (x,y) \subseteq K[x,y]$$
keine Hauptideale. Aber wir werden sehen, dass $\mathbb{Z}[x]$ und $K[x,y]$ faktoriell sind!

Allgemeiner wollen wir uns überlegen, dass für jeden faktoriellen Ring R auch der Polynomring $R[x]$ faktoriell ist. Die Idee ist es, statt Polynomen über dem Ring R zunächst solche über dem Quotientenkörper $K = \mathrm{Quot}(R)$ zu betrachten. Bei der Diskussion von Irreduzibilität ist dabei etwas Vorsicht geboten: Beispielsweise ist das Polynom

$$\begin{aligned} f(x) &= 4x+6 && \text{irreduzibel in } \mathbb{Q}[x] \\ &= 2\cdot(2x+3) && \text{reduzibel in } \mathbb{Z}[x] \end{aligned}$$

Wir machen daher die folgende

Definition 5.8. Sei R ein faktorieller Ring. Ein Polynom $f(x) = \sum_{k=0}^{n} a_k x^k \in R[x]$ heißt *primitiv*, wenn gilt:
$$\mathrm{ggT}(a_0,\ldots,a_n) = 1.$$

Jedes von Null verschiedene Polynom ist bis auf einen konstanten Faktor primitiv:

Lemma 5.9. *Sei R faktoriell mit Quotientenkörper K. Dann besitzt jedes von Null verschiedene Polynom $f(x) \in K[x] \setminus \{0\}$ eine bis auf Multiplikation mit Elementen von $R^\times$ eindeutige Zerlegung*

$$f(x) = c(f)\cdot f^*(x)$$

mit einem Skalar $c(f) \in K^\times$ und einem primitiven Polynom $f^* \in R[x]$.

Beweis. Die Existenz reduziert man durch Multiplikation mit einem gemeinsamen Nenner der Koeffizienten auf den Fall $f \in R[x] \setminus \{0\}$. Sei also $f(x) = \sum_{k=0}^{n} a_k x^k$ mit Koeffizienten $a_k \in R$, dann folgt

$$f(x) = c(f)\cdot f^*(x) \quad \text{mit} \quad c(f) = \mathrm{ggT}(a_0,\ldots,a_n) \quad \text{und} \quad f^*(x) = \sum_{k=0}^{n} a_k^* x^k$$

wobei die $a_k^* \in R$ definiert sind durch $a_k = c(f)\cdot a_k^*$. Per Konstruktion ist $f^*(x) \in R[x]$ primitiv und somit ist die Existenz der gewünschten Zerlegung gezeigt. Umgekehrt überlegt man sich leicht, dass die so gefundene Zerlegung bis auf Multiplikation mit Einheiten in $R^\times$ die einzig mögliche Art ist, $f(x)$ als Produkt eines Skalars und eines primitiven Polynoms zu schreiben. □

Definition 5.10. Wir nennen $c(f) \in K^\times/R^\times$ den *Inhalt* des Polynoms $f \in K[x]\setminus\{0\}$.

Man beachte, dass wir den Inhalt bezüglich eines festen faktoriellen Ringes R definiert haben, wir sollten also genauer $c(f) = c_R(f)$ schreiben. Meist ist aber der faktorielle Ring R aus dem Kontext klar, so wählt man für $K = \mathbb{Q}$ meist $R = \mathbb{Z}$ und berechnet z.B.

$$f(x) \;=\; 2x^3 - \tfrac{4}{3}x^2 + 6x + \tfrac{4}{5} \;=\; \tfrac{2}{15}\cdot\big(15x^3 - 10x^2 + 45x + 6\big) \quad\Longrightarrow\quad c(f) \;=\; \tfrac{2}{15}$$

Die zentrale Aussage für die Untersuchung der Irreduzibilität ist, dass sich der Inhalt von Polynomen multiplikativ verhält:

Lemma 5.11 (Gauß'sches Lemma). *Sei R ein faktorieller Ring und $K = \mathrm{Quot}(R)$, dann gilt*

$$c(fg) \;=\; c(f)\cdot c(g) \quad \textit{für alle} \quad f,g \;\in\; K[x]\setminus\{0\}.$$

Beweis. Nach dem vorigen Lemma können wir $f(x) = a\cdot f^*(x)$ und $g(x) = b\cdot g^*(x)$ mit $a,b \in K^\times$ und primitiven $f^*(x), g^*(x) \in R[x]$ schreiben. Da der Inhalt offenbar multiplikativ bezüglich der Reskalierung mit beliebigen Konstanten $a,b \in K^\times$ ist, erhalten wir

$$\begin{aligned} c(f) &= a\cdot c(f^*),\\ c(g) &= b\cdot c(g^*),\\ c(fg) &= ab\cdot c(f^*g^*). \end{aligned}$$

Dabei ist $c(f^*) = c(g^*) = 1$, zu zeigen bleibt daher nur $c(f^*g^*) = 1$: Wir müssen nachprüfen, dass das Produkt von zwei primitiven Polynomen primitiv ist. Dazu schreiben wir

$$f^*(x) \;=\; \sum_{k=0}^{m} a_k x^k \quad\text{und}\quad g^*(x) \;=\; \sum_{l=0}^{n} b_l x^l$$

Im Fall $c(f^*g^*) \neq 1$ gäbe es ein Primelement $p \in R$ mit $p \mid c(f^*g^*)$. Da f^* und g^* per Definition primitive Polynome sind, sind nicht alle ihre Koeffizienten durch p teilbar. Sei

$$k_0 \;:=\; \max\{k :\; p\nmid a_k\} \quad\text{und}\quad l_0 \;:=\; \max\{l :\; p\nmid b_l\}.$$

In dem Polynom

$$fg \;=\; \sum_{\nu=0}^{m+n} c_\nu x^\nu \;\in\; R[x]$$

wäre dann für $\nu_0 := k_0 + l_0$ der Koeffizient

$$\begin{aligned} c_{\nu_0} &= \sum_{k+l=\nu_0} a_k b_l \\ &= a_{k_0} b_{l_0} + \sum_{k>k_0} a_k b_{\nu_0 - l} + \sum_{l>l_0} a_{\nu_0 - l} b_l \\ &\equiv a_{k_0} b_{l_0} \mod p \end{aligned}$$

nicht durch p teilbar, ein Widerspruch zur Annahme $p \mid c(f^* g^*)$. □

Insbesondere macht es für die Teilbarkeit von Polynomen in $R[x]$ durch *primitive* Polynome keinen Unterschied, ob wir diese Teilbarkeit in dem Polynomring $R[x]$ oder in $K[x]$ betrachten:

Korollar 5.12. *Sei R faktoriell, $K = \mathrm{Quot}(R)$ und $f \in R[x]$. Für primitive $g \in R[x]$ sind dann äquivalent:*

a) Es ist g ein Teiler von f in $K[x]$.

b) Es ist g ein Teiler von f in $R[x]$.

Beweis. Aus $b)$ folgt sofort $a)$. Wenn umgekehrt $a)$ gilt, ist $f = gh$ mit $h \in K[x]$. Dann ist aber

$$\begin{aligned} c(f) &= c(g)c(h) && \text{nach dem Lemma von Gauss} \\ &= c(h) && \text{weil } g \text{ primitiv ist} \end{aligned}$$

Wegen $f \in R[x]$ folgt $c(h) \in R$ und damit $h = c(h) \cdot h^* \in R[x]$, also gilt $b)$. □

Damit haben wir insbesondere die Frage nach irreduziblen Elementen in $R[x]$ unter vollständiger Kontrolle:

Korollar 5.13. *Sei R faktoriell und $K = \mathrm{Quot}(R)$. Für $f(x) \in R[x]$ mit $\deg(f) > 0$ sind äquivalent:*

a) $f(x)$ ist irreduzibel in $R[x]$.

b) $f(x)$ ist irreduzibel in $K[x]$ und primitiv in $R[x]$.

Beweis. Ein Polynom in $R[x]$ ist reduzibel genau dann, wenn es ein Produkt $f = gh$ von Polynomen

$$g, h \in R[x] \quad \text{mit} \quad g, h \notin R[x]^\times = R^\times$$

ist. Dabei gibt es zwei Fälle, je nachdem ob einer der Faktoren g, h ein Polynom vom Grad Null ist oder beide Faktoren Polynome von echt positivem Grad sind. Es gilt:

$$\begin{aligned} f \text{ nicht primitiv} &\iff \exists g \in R, h \in R[x] : \ f = gh \text{ und } g, h \notin R^\times \\ f \text{ reduzibel in } K[x] &\iff \exists g, h \in R[x] : \ f = gh \text{ und } \deg(g), \deg(h) > 0 \end{aligned}$$

Die einzige Implikation, die nicht direkt aus den Definitionen folgt, ist $\Longrightarrow$ in der zweiten Äquivalenz. Diese folgt aus dem vorigen Korollar: Denn wenn f reduzibel in $K[x]$ ist, dann besitzt f einen echten Teiler $g \in K[x]$. Aber dann ist das primitive Polynom $g^* \in R[x]$ ein echter Teiler von f in $R[x]$ nach Korollar 5.12. □

Korollar 5.14. *Für jeden faktoriellen Ring R ist der Polynomring $R[x]$ faktoriell.*

Beweis. Wir nutzen die Charakterisierung faktorieller Ringe aus Satz 5.5. Da $K[x]$ als Hauptidealring faktoriell ist, können wir jedes $f \in R[x] \subseteq K[x]$ schreiben als endliches Produkt

$$f(x) \;=\; p_1(x)\cdots p_n(x) \quad \text{mit irreduziblen} \quad p_i(x) \;\in\; K[x].$$

Dies liefert eine Zerlegung

$$f(x) \;=\; c(f)\cdot p_1^*(x)\cdots p_n^*(x),$$

wobei die Polynome $p_i(x) \in R[x]$ nach Korollar 5.13 irreduzibel in $R[x]$ sind und der Inhalt $c(f) \in R$ in dem faktoriellen Ring R in irreduzible Faktoren zerfällt. Dies liefert die gewünschte Zerlegung in irreduzible Faktoren in $R[x]$.

Dass in $R[x]$ jedes irreduzible Element prim ist, folgt aus der analogen Aussage in $K[x]$: Nach Korollar 5.13 sind irreduzible Elemente in $R[x]$ primitiv, und nach Korollar 5.12 lässt sich die Teilbarkeit durch primitive Polynome in $K[x]$ testen. □

Induktiv erhält man, dass für jeden faktoriellen Ring R und beliebiges $n \in \mathbb{N}$ die Polynomringe $R[x_1,\ldots,x_n]$ faktoriell sind. Wir werden uns in der Galoistheorie vor allem für Polynomringe in einer Variablen über Körpern interessieren, von diesen wußten wir schon aus der linearen Algebra, dass sie faktoriell sind. Das Lemma von Gauß ist aber auch hier nützlich, um Irreduzibilität zu prüfen:

Satz 5.15 (Eisenstein-Kriterium). *Sei $K = \mathrm{Quot}(R)$ für einen faktoriellen Ring R, und sei*

$$f(x) \;=\; \sum_{k=0}^{n} a_k x^k \;\in\; R[x]$$

ein primitives Polynom über diesem Ring. Es gebe ein Primelement $p \in R$, sodass gilt:

- $p \nmid a_n$,
- $p^2 \nmid a_0$,
- $p \mid a_i$ *für alle* $i \in \{0,\ldots,n-1\}$.

Dann ist das Polynom $f(x)$ irreduzibel in $R[x]$ und somit auch in $K[x]$.

Beweis. Wäre f reduzibel in $K[x]$, dann nach dem Lemma von Gauß auch in $R[x]$, es wäre also

$$f(x) \;=\; g(x)h(x) \quad \text{für geeignete} \quad g(x),h(x) \;\in\; R[x] \quad \text{mit} \quad \deg(g),\deg(h) \;>\; 0.$$

Für die durch Reduktion der Koeffizienten modulo p erhaltenen Polynome über dem Körper $\overline{R} := R/pR$ wäre dann

$$\overline{a}_n x^n \;=\; \overline{f}(x) \;=\; \overline{g}(x)\cdot\overline{h}(x) \quad \text{in} \quad \overline{R}[x].$$

Da $\overline{R}[x]$ faktoriell ist, würde $\overline{g}(x) \sim x^d$ und $\overline{h}(x) \sim x^e$ mit $d+e=n$ folgen. Es wäre also

$$\begin{aligned} g(x) \;&=\; \sum_{k=0}^{d} b_k x^k && \text{mit} \quad p \mid b_k \quad \text{für alle} \quad k < d, \\ h(x) \;&=\; \sum_{l=0}^{e} c_l x^l && \text{mit} \quad p \mid c_l \quad \text{für alle} \quad l < e. \end{aligned}$$

Insbesondere wäre $p^2 \mid b_0 c_0 = a_0$ im Widerspruch zur Annahme. □

Primitive Polynome, die die Teilbarkeitsbedingungen im Eisenstein-Kriterium für ein Primelement p erfüllen, nennt man *Eisenstein-Polynome* bezüglich p. Wir haben also gezeigt, dass Eisenstein-Polynome irreduzibel sind. Zum Abschluß noch einige einfache Beispiele:

Beispiel 5.16. Es gilt:

a) Das Polynom
$$f(x) \;=\; 3x^7 - 4x^3 + 10x - 6 \;\in\; \mathbb{Q}[x]$$
ist irreduzibel als Eisenstein-Polynom bezüglich $p = 2$.

b) Manchmal ist das Eisenstein-Kriterium nicht direkt anwendbar, aber nach einer geeigneten Variablensubstitution: Das Polynom
$$f(x) \;:=\; \frac{x^p - 1}{x - 1} \;=\; x^{p-1} + x^{p-2} + \cdots + x + 1 \;\in\; \mathbb{Q}[x]$$
ist kein Eisenstein-Polynom, egal bezüglich welcher Primzahl. Für p prim ist jedoch
$$f(x+1) \;=\; \frac{(x+1)^p - 1}{x} \;=\; x^{p-1} + \tbinom{p}{p-1} x^{p-2} + \cdots + \tbinom{p}{2} x + \tbinom{p}{1}$$
Eisenstein bezüglich p, also irreduzibel. Damit ist auch $f(x) \in \mathbb{Q}[x]$ irreduzibel.

c) Der obige Trick einer Variablensubstitution ist nicht immer anwendbar: Es gibt irreduzible Polynome $f(x) \in \mathbb{Z}[x]$ mit der Eigenschaft, dass $f(x+a)$ *kein* Eisenstein-Polynom ist, egal bezüglich welcher Primzahl p wir arbeiten und wie wir $a \in \mathbb{Z}$ wählen. Man kann sogar $\deg(f) \in \{2,3\}$ wählen (siehe Übungen).

Die wesentliche Idee im Beweis des Eisenstein-Kriteriums war die Reduktion von ganzzahligen Polynomen modulo geeigneter Primzahlen. Diese liefert auch ein weiteres Irreduzibilitätskriterium:

Lemma 5.17. *Sei R ein faktorieller Ring, und sei $f(x) \in R[x]$ ein Polynom, dessen Reduktion*

$$\overline{f}(x) \ \in \ (R/pR)[x] \quad \textit{modulo einem Primelement } p \in R$$

irreduzibel ist mit $\deg(\overline{f}) = \deg(f)$. *Dann ist das Polynom $f(x)$ irreduzibel in $R[x]$.*

Beweis. Aus $f(x) = g(x)h(x)$ folgt $\overline{f}(x) = \overline{g}(x)\overline{h}(x)$. □

Beispiel 5.18. Für alle ungeraden $a, b \in \mathbb{Z}$ ist

$$f(x) = x^5 + ax^2 + b \in \mathbb{Z}[x]$$

irreduzibel: Denn durch Reduktion modulo $p = 2$ erhält man das Polynom

$$\overline{f}(x) = x^5 + x^2 + 1 \ \in \ \mathbb{F}_2[x],$$

und man prüft leicht nach, dass dieses keine echten Teiler in $\mathbb{F}_2[x]$ besitzt; denn es besitzt in $\mathbb{F}_2$ offenbar keine Nullstelle und ist auch durch das einzige irreduzible quadratische Polynom $x^2 + x + 1 \in \mathbb{F}_2[x]$ nicht teilbar. Man beachte, dass hier das Eisenstein-Kriterium ohne weitere Information über a, b nicht anwendbar ist!

Leider greift auch das obige Kriterium nicht immer: Es gibt irreduzible primitive Polynome $f(x) \in \mathbb{Z}[x]$, deren Reduktion modulo jeder Primzahl p reduzibel wird, dies ist beispielsweise für

$$f(x) \ = \ x^4 - 10x^2 + 1$$

der Fall (Übungsaufgabe). Die Faktorisierung von Polynomen in $\mathbb{Z}[x]$ ist aber selbst bei Versagen aller obigen Methoden nur eine Frage der Geduld und kann von einem Computer erledigt werden. Wir begnügen uns hier mit dem folgenden Algorithmus von Kronecker:

Bemerkung 5.19. Sei $f \in \mathbb{Z}[x]$. Wenn f reduzibel ist, gibt es Polynome $g, h \in \mathbb{Z}[x]$ mit

$$f \ = \ gh \quad \text{und} \quad 1 \ \leq \ \deg(g) \ \leq \ d \ := \ \lfloor \deg(f)/2 \rfloor.$$

Ein Polynom vom Grad $\leq d$ ist aber durch seine Werte an $d+1$ verschiedenen Stellen bereits eindeutig festgelegt; daher finden wir alle Möglichkeiten für $g \mid f$ wie folgt:

- Berechne $f(i)$ für $d+1$ verschiedene Stellen $i \in \mathbb{Z}$.
- An jeder dieser Stellen muß $g(i)$ einer der endlich vielen Teiler von $f(i)$ sein.
- Wir erhalten insgesamt endlich viele Möglichkeiten für $g \in \mathbb{Z}[x]$. Für jedes dieser Polynome prüfe man per Polynomdivision, ob $g \mid f$ ist.

Kapitel III
Körper und Galoistheorie

Zusammenfassung In diesem Kapitel untersuchen wir die Struktur von Körpern und ihren Erweiterungen. Wir lernen den Begriff von algebraischen Erweiterungen kennen; die Adjunktion von Nullstellen von Polynomen liefert den algebraischen Abschluß und Zerfällungskörper. Wir betrachten dann Galoiserweiterungen und zeigen den Hauptsatz der Galoistheorie, der alle Zwischenköroer einer gegebenen Galoiserweiterung mittels Gruppentheorie beschreibt.

1 Endliche und algebraische Erweiterungen

In diesem Kapitel wollen wir uns etwas ausführlicher mit der Struktur von Körpern und Körpererweiterungen beschäftigen. Die einfachsten möglichen Körper sind die sogenannten *Primkörper*

$$K = \mathbb{Q} \quad \text{und} \quad K = \mathbb{F}_p \quad \text{für Primzahlen } p.$$

Ringhomomorphismen zwischen Körpern heißen *Körperhomomorphismen*. Sie sind immer injektiv, da Körper keine von Null verschiedenen echten Ideale haben. Unter einem *Teilkörper* eines Körpers L verstehen wir einen Teilring $K \subseteq L$, der selber ein Körper ist. Wir nennen dann L einen *Erweiterungskörper* des Körpers K und bezeichnen $K \subseteq L$ als *Körpererweiterung*. Wenn eine Verwechslung mit Quotienten ausgeschlossen ist, schreibt man statt der Inklusion auch L/K. Es gilt:

Lemma 1.1. *Jeder Körper K enthält einen eindeutigen kleinsten Teilkörper. Dieser ist isomorph zu genau einem der oben genannten Primkörper $\mathbb{Q}$ oder $\mathbb{F}_p$.*

Beweis. Der Kern des eindeutigen Ringhomomorphismus $\varphi : \mathbb{Z} \to K$ ist ein Ideal in $\mathbb{Z}$. Somit gibt es nur zwei Möglichkeiten:

a) $\ker(\varphi) = (p)$ für eine Primzahl p. Dann ist $\mathbb{F}_p \hookrightarrow K$.

b) $\ker(\varphi) = (0)$. Dann setzt sich φ fort zu einem Monomorphismus $\varphi : \mathbb{Q} \hookrightarrow K$. □

Man beachte, dass wir die Körpereigenschaft von K nur für die Fortsetzung in b) benutzt haben, der Rest bleibt für Integritätsringe gültig. Die *Charakteristik* eines Integritätsringes R ist definiert durch

$$\operatorname{char}(R) := \begin{cases} p & \text{für } \mathbb{F}_p \subseteq R, \\ 0 & \text{für } \mathbb{Z} \subseteq R. \end{cases}$$

Definition 1.2. Sei L/K eine Körpererweiterung. Dann bildet L insbesondere einen Vektorraum über dem Körper K. Wir definieren den *Grad* der Körpererweiterung durch

$$[L:K] := \dim_K(L) \in \mathbb{N} \cup \{\infty\}.$$

Die Körpererweiterung heißt *endlich*, wenn $[L:K] < \infty$ ist, andernfalls *unendlich*.

Beispiel 1.3. Es gilt:

a) $[\mathbb{C}:\mathbb{R}] = 2$.

b) $[\mathbb{Q}(\sqrt{2}):\mathbb{Q}] = 2$ für den Körper $\mathbb{Q}(\sqrt{2}) := \{a + b\sqrt{2} \in \mathbb{R} \mid a,b \in \mathbb{Q}\}$.

c) $[\mathbb{R}:\mathbb{Q}] = \infty$ aus mengentheoretischen Gründen, da $\mathbb{R}$ nicht abzählbar ist.

d) $[K(x):K] = \infty$ für den Körper

$$K(X) := \operatorname{Quot}(K[X]) = \left\{\tfrac{f}{g} \mid f,g \in K[x], g \neq 0\right\}$$

der rationalen Funktionen über einem beliebigen Körper K (Übungsaufgabe).

Satz 1.4 (Gradsatz). *Seien $K \subseteq L \subseteq M$ Körpererweiterungen. Dann gilt*

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

Beweis. Wir nehmen zunächst an, dass M/L und L/K endliche Erweiterungen sind; seien dann

- $\alpha_1, \ldots, \alpha_m \in L$ eine Basis von L als Vektorraum über K,
- $\beta_1, \ldots, \beta_n \in M$ eine Basis von M als Vektorraum über L.

Wir zeigen, dass die Produkte

$$\gamma_{ij} := \alpha_i \beta_j \quad \text{für} \quad 1 \leq i \leq m \quad \text{und} \quad 1 \leq j \leq n$$

eine Basis von M als Vektorraum über K bilden. Zunächst prüfen wir die lineare Unabhängigkeit der gegebenen Elemente über dem Körper K nach. Seien $c_{ij} \in K$ gegeben mit

$$\sum_{i,j} c_{ij} \gamma_{ij} = 0.$$

Indem wir die Doppelsumme in zwei separate Summationen zerlegen und $\gamma_{ij} = \alpha_i \beta_j$ einsetzen, erhalten wir

$$\sum_{j=1}^{n} a_j \beta_j \;=\; 0 \quad \text{mit} \quad a_j \;:=\; \sum_{i=1}^{m} c_{ij} \alpha_i \;\in\; L.$$

Weil $\beta_1, \ldots, \beta_n$ linear unabhängig über L sind, folgt $a_j = 0$ für alle j. Aus dieser letzten Gleichung und der lineare Unabhängigkeit der Elemente $\alpha_1, \ldots, \alpha_m$ über K erhalten wir dann $c_{ij} = 0$ für alle i, j. Damit haben wir gezeigt, dass die γ_{ij} linear unabhängig über K sind. Dass sie ein Erzeugendensystem von M als Vektorraum über K bilden, folgt ebenso: Da $\beta_1, \ldots, \beta_n$ ein Erzeugendensystem von M über L bilden, besitzt jedes $x \in M$ eine Darstellung

$$x \;=\; \sum_{j=1}^{n} a_j \beta_j \quad \text{mit Koeffizienten} \quad a_j \;\in\; L,$$

und da $\alpha_1, \ldots, \alpha_m$ eine Basis des Vektorraums L über K bilden, hat jedes a_j eine Darstellung

$$a_j \;=\; \sum_{i=1}^{n} c_{ij} \alpha_i \quad \text{mit Koeffizienten} \quad c_{ij} \;\in\; K.$$

Insgesamt erhalten wir somit eine Darstellung $x = \sum_{i,j} c_{ij} \gamma_{ij}$ wie gewünscht. □

Unter einem *Zwischenkörper* einer Körpererweiterung M/K verstehen wir einen Teilkörper $L \subset M$, welcher K enthält. Aus der Gradformel erhalten wir:

Korollar 1.5. *Wenn $[M : K]$ eine Primzahl ist, besitzt die Körpererweiterung M/K nur die trivialen Zwischenkörper $L = M$ und $L = K$.*

Beweis. Primzahlen haben keine echten Teiler. □

Zu jeder Menge von Elementen einer Körpererweiterung können wir den davon erzeugten Zwischenkörper betrachten. Zum Vergleich betrachten wir zunächst den analogen Begriff für Ringerweiterungen:

Definition 1.6. Sei $R \subseteq S$ eine Erweiterung kommutativer Ringe. Für $a_1, \ldots, a_n \in S$ liefert die universelle Eigenschaft von Polynomringen einen eindeutig bestimmten Ringhomomorphismus

$$\varphi : \quad R[x_1, \ldots, x_n] \;\longrightarrow\; S \quad \text{mit} \quad \begin{cases} \varphi(x_i) = a_i \text{ für } i = 1, \ldots, n, \\ \varphi|_R : R \hookrightarrow S \text{ ist die Inklusion.} \end{cases}$$

Die *von $a_1, \ldots, a_n \in S$ erzeugte Ringerweiterung von R* ist das Bild von φ, also der Teilring

$$\begin{aligned} R[a_1, \ldots, a_n] \;&:=\; \operatorname{im}(\varphi) \\ &=\; \big\{ f(a_1, \ldots, a_n) \in S \mid f \in R[x_1, \ldots, x_n] \big\} \;\subseteq\; S \end{aligned}$$

Wir sagen, dass der Ring $R[a_1,\ldots,a_n]$ aus R durch *Adjunktion* von $a_1,\ldots,a_n \in S$ hervorgeht. Man beachte: Die Notation sieht zwar aus wie für Polynomringe, aber im Gegensatz zu letzteren sind hier $a_1,\ldots,a_n$ keine formalen Variablen, sondern Elemente eines vorgegebenen Erweiterungsringes. Für beliebige Teilmengen $A \subseteq S$ setzen wir

$$R[A] \quad := \bigcup_{\substack{n\in\mathbb{N}\\ a_1,\ldots,a_n\in A}} R[a_1,\ldots,a_n] \quad \subseteq \quad S.$$

Offenbar ist dies der kleinste Teilring von S, der sowohl R als auch A enthält. Eine Ringerweiterung $R \subseteq S$ heißt *endlich erzeugt*, wenn es Elemente $a_1,\ldots,a_n \in S$ gibt mit

$$S \;=\; R[a_1,\ldots,a_n].$$

Für Körpererweiterungen wollen wir Elemente nicht nur in Polynome, sondern auch in rationale Funktionen einsetzen, sofern der Nenner dabei nicht Null wird:

Definition 1.7. Sei L/K eine Körpererweiterung. Für Teilmengen $A \subseteq L$ liefert die vorige Definition einen Teilring

$$K[A] \;\subseteq\; L.$$

Die *von der Teilmenge $A \subseteq L$ erzeugte Körpererweiterung von K* ist definiert als der Quotientenkörper

$$K(A) \;:=\; \mathrm{Quot}(K[A]) \;\subseteq\; L.$$

Dieser ist der kleinste die Teilmenge A enthaltende Zwischenkörper von L/K. Für endliche Mengen $A = \{a_1,\ldots,a_n\}$ lassen wir die Mengenklammern weg. Explizit ist

$$K(a_1,\ldots,a_n) \;=\; \left\{ \frac{f(a_1,\ldots,a_n)}{g(a_1,\ldots,a_n)} \;\in\; L \;\mid\; f,g \;\in\; K[x_1,\ldots,x_n],\; g(a_1,\ldots,a_n) \;\neq\; 0 \right\}$$

Wir bezeichnen diesen Körper als den aus K durch *Adjunktion* von $a_1,\ldots,a_n \in L$ hervorgehenden Körper. Eine Körpererweiterung L/K heißt *endlich erzeugt*, wenn es Elemente $a_1,\ldots,a_n \in L$ gibt mit

$$L \;=\; K(a_1,\ldots,a_n).$$

Der Fall $n = 1$ ist dabei von besonderer Bedeutung, der allgemeine Fall lässt sich induktiv mittels

$$K(a_1,\ldots,a_n) \;=\; (K(a_1,\ldots,a_{n-1}))(a_n)$$

darauf reduzieren. Für Körpererweiterungen, welche von einem Element erzeugt werden, hängen die obigen Begriffe wie folgt zusammen:

Satz 1.8. *Sei L/K eine Körpererweiterung. Für $a \in L$ sind äquivalent:*

a) Es ist $[K(a) : K] < \infty$.

b) Es gibt ein $g \in K[x] \setminus \{0\}$ mit $g(a) = 0$.

c) Es ist $K[a] = K(a)$.

Beweis. Wenn $a)$ gilt, setze $n = [K(a) : K] \in \mathbb{N}$. Die $n+1$ Elemente $1, a, a^2, \ldots, a^n$ müssen aus Dimensionsgründen linear abhängig über dem Körper K sein. Es gibt also eine Relation

$$c_0 + c_1 a + \cdots + c_n a^n \;=\; 0$$

mit $c_i \in K$ nicht alle Null, also gilt $b)$. Für die Äquivalenz von $b)$ und $c)$ betrachten wir den Ringhomomorphismus

$$\varphi: \quad K[x] \;\twoheadrightarrow\; K[a] \;\subseteq\; K(a), \quad g(x) \;\mapsto\; g(a).$$

Sein Kern $\ker(\varphi) \subseteq K[x]$ ist ein Ideal. Aus der linearen Algebra wissen wir, dass der Polynomring in einer Variablen über einem Körper ein Hauptidealring ist; es gibt also ein Polynom $f \in K[x]$ mit $\ker(\varphi) = (f)$. Der Homomorphiesatz liefert einen Isomorphismus

$$\overline{\varphi}: \quad K[x]/(f) \;\xrightarrow{\sim}\; K[a]$$

von Ringen. Da auf der rechten Seite ein Teilring eines Körpers steht, ist $K[x]/(f)$ ein Integritätsring $\neq \{0\}$. Somit gilt entweder $f = 0$, oder f ist ein irreduzibles Polynom in $K[x]$. Wir erhalten

$$\begin{aligned}
b) &\iff f \neq 0 && \text{wegen } \ker(\varphi) = (f)\\
&\iff f \text{ ist irreduzibel} && \text{nach obiger Dichotomie}\\
&\iff (f) \subseteq K[x] \text{ ist ein maximales Ideal} && \text{da } K[x] \text{ Hauptidealring}\\
&\iff K[a] \text{ ist ein Körper} && \text{wegen } K[a] \simeq K[x]/(f)\\
&\iff K[a] = K(a), \text{ d.h. } c) \text{ gilt} && \text{wegen } K(a) = \mathrm{Quot}(K[a])
\end{aligned}$$

Somit sind die Eigenschaften $b)$ und $c)$ zueinander äquivalent. Wenn sie erfüllt sind, gilt

$$[K(a) : K] \;=\; \dim_K K(a) \;=\; \dim_K K[a] \;=\; \dim_K K[x]/(f) \;<\; \infty,$$

genauer zeigt Division mit Rest durch das Polynom f vom Grad $n = \deg(f) \geq 0$, dass

$$1, x, x^2, \ldots, x^{n-1} \quad \text{eine Vektorraumbasis von} \quad K[x]/(f)$$

bilden und somit folgt auch $a)$. □

Definition 1.9. Sei L/K eine Körpererweiterung. Ein Element $a \in L$ heißt

a) *algebraisch über K*, wenn ein $g \in K[x] \setminus \{0\}$ existiert mit $g(a) = 0$.

b) *transzendent über K*, wenn es nicht algebraisch über K ist.

Wir erhalten damit eine vollständige Beschreibung aller Körpererweiterungen, die von einem Element erzeugt werden können:

Bemerkung 1.10. Sei L/K eine Körpererweiterung und $a \in L$.

a) Es ist $[K(a) : K] = \infty$ genau dann, wenn a transzendent über K ist. In diesem Fall ist
$$K(a) \simeq K(x) = \left\{ \tfrac{f}{g} \mid f, g \in K[x], g \neq 0 \right\}$$
isomorph zum Körper der rationalen Funktionen in einer Variablen x über K.

b) Es ist $[K(a) : K] < \infty$ genau dann, wenn a algebraisch über K ist. In diesem Fall ist
$$K(a) \simeq K[x]/(f)$$
isomorph zum Quotient des Polynomrings modulo dem von einem irreduziblen Polynom $f \in K[x]$ erzeugten Ideal. Wenn wir f als normiert voraussetzen, ist es eindeutig und wir nennen es das *Minimalpolynom* von a über K. Für $n = \deg(f)$ bilden die Elemente $1, a, a^2, \ldots, a^{n-1}$ eine Basis des Vektorraums $K(a)$ über K, insbesondere ist
$$\begin{aligned} [K(a) : K] &= \deg(f) \\ &= \min\{m \in \mathbb{N} \mid 1, a, a^2, \ldots, a^m \text{ sind linear abhängig über } K\} \end{aligned}$$
Für $g \in K[x]$ gilt die Äquivalenz:
$$g(a) = 0 \iff f \text{ teilt } g \text{ in } K[x]$$
Um nachzuweisen, dass ein $a \in L$ algebraisch über K ist, müssen wir nicht das genaue Minimalpolynom ausrechnen, wir müssen lediglich ein $g(x) \in K[x] \setminus \{0\}$ finden mit $g(a) = 0$. Dann gilt:

- Das Minimalpolynom $f(x)$ von a über K ist ein Teiler von $g(x)$. Insbesondere ist
$$[K(a) : K] = \deg(f) \leq \deg(g)$$
- Gleichheit gilt genau dann, wenn das Polynom $g(x)$ in $K[x]$ irreduzibel ist. In diesem Fall stimmt $g(x)$ bis auf Normieren mit dem Minimalpolynom überein.

Schauen wir uns einige einfache Beispiele an:

Beispiel 1.11. Es gilt:

a) Jedes $a \in K$ ist algebraisch über K mit Minimalpolynom $f(x) = x - a$.

b) Die Zahl $i \in \mathbb{C}$ ist algebraisch über $K = \mathbb{Q}$ mit Minimalpolynom $f(x) = x^2 + 1$.

c) Für jede Primzahl p und $n \in \mathbb{N}$ ist die Zahl $a = \sqrt[n]{p} \in \mathbb{R}$ algebraisch über $\mathbb{Q}$ mit Minimalpolynom

$$f(x) \;=\; x^n - p,$$

denn f hat die Nullstelle a und ist als Eisenstein-Polynom irreduzibel in $\mathbb{Q}[x]$; somit ist

$$\big[\mathbb{Q}(\sqrt[n]{p}) : \mathbb{Q}\big] \;=\; n.$$

d) Die Zahl $a = \sqrt{2 + \sqrt[3]{5}} \in \mathbb{R}$ ist algebraisch über $\mathbb{Q}$, denn sie ist eine Nullstelle des Polynoms

$$f(x) \;=\; (x^2 - 2)^3 - 5 \;=\; x^6 - 6x^4 + 12x^2 - 13.$$

Dieses Polynom ist sogar irreduzibel in $\mathbb{Q}[x]$, dies erfordert aber mehr Arbeit.

e) Mit der Menge aller Polynome in $\mathbb{Q}[x]$ ist auch die Menge der Nullstellen solcher Polynome abzählbar: Die meisten reellen Zahlen sind transzendent über $\mathbb{Q}$. Die Transzendenz einer konkreten Zahl zu zeigen, ist jedoch im Allgemeinen sehr schwierig. Bekannte Beispiele sind die Kreiszahl π und die Eulersche Zahl e.

Für Körpererweiterungen, die von endlich vielen Element erzeugt werden können, können wir die obigen Resultate induktiv anwenden. Wir benutzen dabei:

Lemma 1.12. *Seien $K \subseteq K' \subseteq L$ Körpererweiterungen. Für $a \in L$ gilt dann:*

$$\textit{a algebraisch über } K \quad \Longrightarrow \quad \textit{a algebraisch über } K'$$

Beweis. Ein Element $a \in L$ ist algebraisch über K genau dann, wenn ein von Null verschiedenes Polynom $g \in K[x] \setminus \{0\}$ existiert mit $g(a) = 0$. Wenn wir g als Element von $K'[x]$ betrachten, folgt hieraus, dass a auch algebraisch über K' ist. □

Die Verallgemeinerung von Satz 1.8 auf endlich erzeugte Körpererweiterungen können wir damit so formulieren:

Satz 1.13. *Sei L/K eine Körpererweiterung. Für $a_1, \ldots, a_n \in L$ sind äquivalent:*

a) Es ist $[K(a_1, \ldots, a_n) : K] < \infty$.

b) Die Elemente $a_1, \ldots, a_n$ sind algebraisch über K.

Beweis. Wenn $a)$ gilt, folgt aus $K(a_i) \subseteq K(a_1, \ldots, a_n)$

$$[K(a_i) : K] \;\leq\; [K(a_1, \ldots, a_n) : K] \;<\; \infty$$

und somit sind die a_i algebraisch über K, d.h. es gilt $b)$. Ist umgekehrt letzteres der Fall, dann wenden wir sukzessive das vorige Lemma an: Für jedes feste $i \geq 0$ ist

das Element a_{i+1} algebraisch über K, also nach dem vorigen Lemma erst recht über dem Zwischenkörper

$$K_i := K(a_1, \ldots, a_i).$$

Somit ist $d_i := [K_{i+1} : K_i] < \infty$ für alle i. Wir erhalten aus der aufsteigenden Kette von Erweiterungen

$$K = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_n = K(a_1, \ldots, a_n)$$

dann durch mehrfaches Anwenden des Gradsatzes $[K_n : K_0] = d_0 d_1 \cdots d_{n-1} < \infty$ und somit folgt die Endlichkeitsaussage $a)$. □

Wir haben zunächst Körpererweitungen betrachtet, welche von einem Element erzeugt werden, dann solche, die von endlich vielen Elementen erzeugt werden. Für beliebige Körpererweiterungen machen wir die folgende Definition:

Definition 1.14. Eine Körpererweiterung L/K heißt

a) *algebraisch*, falls jedes $a \in L$ algebraisch über K ist.

b) *transzendent*, falls sie nicht algebraisch ist.

Algebraische Körpererweiterungen müssen nicht endlich sein, sie sind aber immer Vereinigungen von endlichen Erweiterungen. Unsere letzte Verallgemeinerung der Sätze 1.8 und 1.13 sieht damit so aus:

Satz 1.15. *Für Körpererweiterungen L/K sind äquivalent:*

a) Die Erweiterung L/K ist algebraisch.

b) Es ist $L = K(A)$ für eine Menge $A \subseteq L$ von über K algebraischen Elementen.

c) Die Erweiterung L/K ist die Vereinigung ihrer endlichen Teilerweiterungen, d.h. es ist

$$L = \bigcup_{\substack{K \subseteq K' \subseteq L \\ [K':K] < \infty}} K'$$

wobei die Vereinigung über Zwischenkörper K' von L/K mit $[K' : K] < \infty$ läuft.

Beweis. Aus $a)$ folgt trivialerweise $b)$ mit $A = L$. Wenn $b)$ für ein geeignetes $A \subseteq L$ gilt, dann ist per Definition

$$L = K(A) := \bigcup_{\substack{n \in \mathbb{N} \\ a_1, \ldots, a_n \in A}} K(a_1, \ldots, a_n)$$

Die Erweiterungen $K(a_1, \ldots, a_n)/K$ mit algebraischen $a_1, \ldots, a_n$ sind nach Satz 1.13 endlich und es folgt $c)$. Wenn schließlich $c)$ gilt, ist jedes $a \in L$ enthalten in einer endlichen Erweiterung K'/K. Dann ist $[K(a) : K] \leq [K' : K] < \infty$ und somit ist a algebraisch über K, also folgt die Aussage $a)$. □

Korollar 1.16. *Für Körpererweiterungen L/K sind äquivalent:*

a) L/K ist eine endliche Erweiterung.

b) L/K ist algebraisch und endlich erzeugt.

Beweis. Aus b) folgt sofort a) nach Satz 1.13. Wenn umgekehrt a) gilt, dann ist L/K nach Satz 1.15 insbesondere algebraisch, und die endliche Erzeugtheit folgt sofort daraus, dass eine endliche Erweiterung keine unendlichen aufsteigenden Ketten von Zwischenkörpern enthalten kann. □

Bemerkung 1.17. Keine der zwei Eigenschaften *algebraisch* und *endlich erzeugt* folgt aus der anderen:

- Für $A = \{\sqrt[n]{2} \mid n \in \mathbb{N}\} \subseteq \mathbb{R}$ ist ist die Erweiterung $L = \mathbb{Q}(A)/\mathbb{Q}$ nicht endlich, denn
$$[L : \mathbb{Q}] \geq [\mathbb{Q}(\sqrt[n]{2}) : \mathbb{Q}] = n \quad \text{für alle} \quad n \in \mathbb{N}.$$
Sie ist aber algebraisch, da sie von den algebraischen Zahlen $\sqrt[n]{2}$ erzeugt wird, in der Tat ist
$$L = \bigcup_{n\in\mathbb{N}} \mathbb{Q}(\sqrt[n]{2}).$$
Nach dem obigen Korollar ist also die Erweiterung $L/\mathbb{Q}$ nicht endlich erzeugt.
- Sei $L = \mathbb{Q}(x)$ der Körper der rationalen Funktionen. Dann ist $L/\mathbb{Q}$ eine endlich erzeugte Körpererweiterung, aber nicht algebraisch: Es handelt sich hier um eine transzendente Körpererweiterung!

2 Algebraischer Abschluss eines Körpers

Wir wollen nun zu jedem Körper eine Körpererweiterung konstruieren, in der jedes Polynom von positivem Grad eine Nullstelle besitzt. Wir fangen bescheiden an und betrachten zunächst nur ein einzelnes Polynom:

Lemma 2.1 (Kronecker). *Sei K ein Körper und $f(x) \in K[x]$ mit $\deg(f) > 0$. Dann gibt es eine endliche Körpererweiterung L/K, in der das Polynom eine Nullstelle besitzt:*
$$f(a) = 0 \quad \textit{für ein} \quad a \in L.$$

Beweis. Das Polynom $f(x)$ ist ein Produkt irreduzibler Faktoren in $K[x]$; indem wir es durch einen dieser Faktoren ersetzen, dürfen wir oBdA annehmen, dass $f(x)$ in $K[x]$ irreduzibel ist. Dann ist der Quotientenring $L := K[x]/(f)$ ein Körper. Durch Zusammensetzen der Inklusion i und der Quotientenabbildung p erhalten wir einen Homomorphismus
$$K \xhookrightarrow{i} K[x] \xrightarrow{p} K[x]/(f) = L,$$

und dieser ist als Homomorphismus zwischen Körpern injektiv. Wir haben somit eine Körpererweiterung L/K. Sei $a := p(x) \in L$ die Restklasse von $x \in K[x]$. Für das Polynom

$$f(x) \;=\; \sum_{k=0}^{n} c_k x^k \quad \text{mit} \quad c_k \in K$$

gilt dann

$$f(a) \;=\; \sum_{k=0}^{n} c_k\, a^k \;=\; \sum_{k=0}^{n} c_k\, (p(x))^k \;=\; p\Big(\sum_{k=0}^{n} c_k x^k \Big) \;=\; p(f) \;=\; 0 \;\in\; L$$

und somit ist $a \in L$ eine Nullstelle des Polynoms $f(x) \in K[x]$. □

Wir wollen dieses Verfahren iterieren, um einen Erweiterungskörper zu finden, in dem *jedes* Polynom von positivem Grad eine Nullstelle hat. Dazu zunächst eine Vorbemerkung:

Lemma 2.2. *Sei K ein Körper. Dann sind äquivalent:*

a) Jedes Polynom $f(x) \in K[x]$ mit $\deg(f) > 0$ besitzt eine Nullstelle $a \in K$.

b) Jedes Polynom $f(x) \in K[x]$ mit $\deg(f) > 0$ zerfällt über K in Linearfaktoren, d.h.

$$f(x) \;=\; c \cdot \prod_{i=1}^{n} (x - a_i) \quad \textit{mit } n = \deg(f) \in \mathbb{N},\ \ c \in K^\times \textit{ und } a_1, \ldots, a_n \in K.$$

c) Die einzigen irreduziblen Polynome $f(x)$ in $K[x]$ sind die vom Grad $\deg(f) = 1$.

d) Der Körper K besitzt keine echten algebraischen Erweiterungskörper.

Beweis. Aus $a)$ folgt $b)$ durch Polynomdivision und Induktion über $\deg(f)$. Aus $b)$ folgt $c)$ trivialerweise. Angenommen, es gelte nun $c)$, und sei L/K eine algebraische Erweiterung. Für beliebiges $a \in L$ ist dann $K(a)/K$ eine endliche Erweiterung. Nach Bemerkung 1.10 ist

$$L \;\simeq\; K[x]/(f) \quad \text{für ein irreduzibles Polynom} \quad f(x) \;\in\; K[x].$$

Die Annahme $c)$ impliziert $\deg(f) = 1$ und somit folgt $L = K$, d.h. es gilt $d)$.

Zu zeigen bleibt, dass aus $d)$ auch $a)$ folgt. Wir argumentieren indirekt: Wenn $a)$ nicht gilt, gibt es ein irreduzibles Polynom $f(x) \in K[x]$ ohne Nullstellen in K. Die Lemma 2.1 liefert eine endliche Erweiterung L/K, in der $f(x)$ eine Nullstelle hat; insbesondere ist $L \neq K$ und damit gilt auch $d)$ nicht. □

Definition 2.3. Wir sagen, ein Körper sei K als *algebraisch abgeschlossen*, wenn er die äquivalenten Eigenschaften des vorigen Lemmas besitzt.

Z.B. besagt der aus der Analysis bekannte Fundamentalsatz der Algebra, dass der Körper $K = \mathbb{C}$ algebraisch abgeschlossen ist. Wir wollen zeigen, dass jeder Körper einen algebraisch abgeschlossenen Erweiterungskörper hat; dazu werden wir die Idee von Lemma 2.1 für Polynomringe in unendlich vielen Variablen betrachten:

Definition 2.4. Sei I eine Menge und $\mathfrak{X} = (X_i)_{i\in I}$ eine Familie von Variablen.

- Ein *Multiindex* ist eine Funktion $\nu : I \to \mathbb{N}_0$ mit $\nu(i) = 0$ für alle bis auf endlich viele i. Unter dem zugehörigen *Monom in den Variablen* $\mathfrak{X}$ verstehen wir das endliche formale Produkt
$$\mathfrak{X}^\nu := \prod_{i\in I} X_i^{\nu(i)}$$
- Ein *Polynom in* $\mathfrak{X}$ ist eine endliche formale Linearkombination der Form
$$P(\mathfrak{X}) = \sum_\nu a_\nu \mathfrak{X}^\nu$$
wobei die Summe über Multiindices läuft und die $c_\nu \in K$ fast alle Null sind.
- Die *Summe* und das *Produkt* von Polynomen definieren wir wie im Fall endlich vieler Variablen durch
$$\Big(\sum_\nu a_\nu \mathfrak{X}^\nu\Big) + \Big(\sum_\nu b_\nu \mathfrak{X}^\nu\Big) := \sum_\nu (a_\nu + b_\nu)\mathfrak{X}^\nu$$
$$\Big(\sum_\nu a_\nu \mathfrak{X}^\nu\Big) \cdot \Big(\sum_\mu b_\mu \mathfrak{X}^\mu\Big) := \sum_\lambda c_\lambda \mathfrak{X}^\lambda \quad \text{mit} \quad c_\lambda := \sum_{\nu+\mu=\lambda} a_\nu b_\mu$$
Man rechnet nach, dass die Menge aller solchen Polynome einen kommutativen Ring bildet. Wir bezeichnen ihn mit $K[\mathfrak{X}] = K\big[X_i \mid i \in I\big]$.

Wir können nun für alle Polynome zugleich Nullstellen konstruieren:

Proposition 2.5. *Jeder Körper K hat eine algebraische Erweiterung K'/K, sodass jedes Polynom $f(x) \in K[x]$ mit* $\deg(f) > 0$ *eine Nullstelle $a \in K'$ hat.*

Beweis. Wir wollen die Konstruktion in Lemma 2.1 für alle Polynome gleichzeitig durchführen. Da wir für jedes Polynom eine Nullstelle haben wollen, brauchen wir für jedes eine eigene Variable: Wir betrachten die Indexmenge
$$I := \big\{ f \in K[x] \mid \deg(f) > 0 \big\}$$
und bilden den sehr großen Polynomring
$$R := K[\mathfrak{X}] \quad \text{in den Variablen} \quad \mathfrak{X} := (X_f)_{f\in I}.$$
In Lemma 2.1 hatten wir in dem Ring $K[x]$ das Ideal $(f(x))$ ausgeteilt. In Analogie dazu betrachten wir das Ideal
$$\mathfrak{a} := \big(f(X_f) \mid f \in I\big) \subseteq R$$
erzeugt von allen Elementen $f(X_f) \in R$, welche man durch Einsetzen von $X_f \in R$ in das Polynom $f(x) \in K[x]$ erhält. Anders als in Lemma 2.1 ist dieses im Allgemeinen kein maximales Ideal. Wir zeigen aber, dass es ein echtes Ideal ist, also $\mathfrak{a} \notin R$ gilt:

Denn andernfalls wäre $1 \in \mathfrak{a}$. Per Definition des von einer Menge von Elementen erzeugten Ideals wäre dann 1 eine Linearkombination endlich vieler der Erzeuger des Ideals, also

$$1 \;=\; \sum_f g_f \cdot f(X_f) \quad \text{mit} \quad g_f \;\in\; R \;=\; K[\mathfrak{X}] \quad \text{fast alle Null.}$$

Indem wir Lemma 2.1 sukzessive auf die endlich vielen Polynome f mit $g_f \neq 0$ anwenden, erhalten wir eine endliche Erweiterung L/K mit der Eigenschaft, dass jedes dieser Polynome f eine Nullstelle $a_f \in L$ besitzt. Für alle f mit $g_f = 0$ wählen wir $a_f \in L$ beliebig. Der Einsetzungshomomorphismus

$$\Phi: \quad R \;=\; K[\mathfrak{X}] \;\longrightarrow\; L \quad \text{mit} \quad X_f \;\mapsto\; a_f \quad \text{für alle } f$$

macht aus der vorigen Darstellung des Einselementes

$$1 \;=\; \Phi(1) \;=\; \sum_f \Phi(g_f) \cdot \Phi(f(X_f)) \;=\; \sum_f \Phi(g_f) \cdot f(a_f) \;=\; 0,$$

was absurd ist. Also haben wir gezeigt, dass $\mathfrak{a} \neq R$ ein echtes Ideal ist.

Der Ring $R/\mathfrak{a}$ ist somit vom Nullring verschieden und hat nach dem Lemma von Zorn ein maximales Ideal. Das Urbild dieses maximalen Ideals liefert ein maximales Ideal

$$\mathfrak{m} \;\subseteq\; R \quad \text{mit} \quad \mathfrak{a} \;\subseteq\; \mathfrak{m}.$$

Wir betrachten nun den aus der Inklusion i und dem Quotientenhomomorphismus p zusammengesetzen Homomorphismus

$$K \;\xhookrightarrow{\;i\;}\; R \;\xrightarrow{\;p\;}\!\!\!\!\rightarrow\; K' \;:=\; R/\mathfrak{m}.$$

Dieser ist als Homomorphismus von Körpern injektiv, und wie in Lemma 2.1 sieht man, dass

$$f(a_f) \;=\; 0 \quad \text{für das Bild} \quad a_f \;:=\; p(X_f) \;\in\; L$$

von $X_f \in R$ gilt. Wir haben damit eine Körpererweiterung K'/K mit der gewünschten Nullstelleneigenschaft konstruiert. Aus der Konstruktion ist ferner klar, dass diese Erweiterung algebraisch ist: Denn R wird von den Variablen X_f mit $f \in I$ erzeugt, somit ist

$$K' = K(a_f \mid f \in I)$$

und $a_f \in K'$ ist als Nullstelle von $f \in K[x]$ algebraisch über K. Also wird K' über K von algebraischen Elementen erzeugt und ist somit nach Satz 1.15 eine algebraische Erweiterung. □

Satz 2.6. *Für jeden Körper K gibt es eine Körpererweiterung L/K, sodass gilt:*

a) L/K ist algebraisch, und

b) L ist algebraisch abgeschlossen.

Beweis. Nach der vorigen Proposition existiert eine algebraische Erweiterung K'/K, sodass jedes $f(x) \in K[x]$ mit $\deg(f) > 0$ eine Nullstelle in K' hat. Tatsächlich kann man zeigen, dass der so erhaltene Erweiterungskörper algebraisch abgeschlossen ist; dazu fehlen uns aber momentan noch einige Werkzeuge und wir gehen daher vorsichtiger vor. Durch sukzessives Anwenden der Proposition erhalten wir eine Kette algebraischer Erweiterungen

$$K = L_0 \subseteq K' = L_1 \subseteq L_2 \subseteq L_3 \subseteq \cdots$$

sodass jedes $f(x) \in L_n[x]$ mit $\deg(f) > 0$ eine Nullstelle in L_{n+1} hat. Als Vereinigung einer aufsteigenden Kette von Körpern ist dann

$$L := \bigcup_{n=0}^{\infty} L_n$$

wieder ein Körper, und als Vereinigung algebraischer Erweiterungen ist L/K eine algebraische Erweiterung. Der Körper L ist algebraisch abgeschlossen: Denn jedes Polynom $f(x) \in L[x]$ liegt in $L_n[x]$ für ein $n \in \mathbb{N}$ und besitzt im Fall $\deg(f) > 0$ somit eine Nullstelle $a \in L_{n+1} \subseteq L$. □

Definition 2.7. Sei K ein Körper. Wir bezeichnen einen Erweiterungskörper $L \supseteq K$ als einen *algebraischen Abschluß von K*, wenn er beide Eigenschaften aus dem vorigen Satz besitzt, d.h. wenn gilt:

a) L/K ist algebraisch, und

b) L ist algebraisch abgeschlossen.

Der Satz 2.6 besagt also, dass jeder Körper einen algebraischen Abschluß hat. Man beachte, dass diese Existenzaussage auf Proposition 2.5, also auf dem Lemma von Zorn beruht. Als nächstes wollen wir die Frage nach der Eindeutigkeit studieren und untersuchen hierzu zunächst allgemeiner Fortsetzungen von Homomorphismen zu algebraischen Körpererweiterungen.

3 Fortsetzungen von Homomorphismen

Um die Fortsetzungen von Homomorphismen zu algebraischen Erweiterungen zu verstehen, betrachten wir zunächst erneut Minimalpolynome. Für $f(x) \in K[x]$ und Homomorphismen $\sigma : K \hookrightarrow M$ sei

$$f^{\sigma}(x) \in M[x]$$

das Polynom, welches man durch Anwenden von σ auf die Koeffizienten von $f(x)$ erhält. Für die Fortsetzbarkeit von Körperhomomorphismen gilt dann das folgende Kriterium:

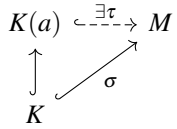
Lemma 3.1. *Sei L/K eine Körpererweiterung und $a \in L$ ein über K algebraisches Element mit Minimalpolynom $f \in K[x]$. Weiter sei ein Homomorphismus $\sigma : K \hookrightarrow M$ in einen Körper M gegeben. Dann hat man eine Bijektion*

$$\begin{aligned} \big\{ \text{Homomorphismen } \tau : K(a) \hookrightarrow M \text{ mit } \tau|_K = \sigma \big\} &\longrightarrow \big\{ c \in M \mid f^\sigma(c) = 0 \big\} \\ \tau &\mapsto \tau(a) \end{aligned}$$

zwischen der Menge der

a) Nullstellen $c \in M$ des Polynoms $f^\sigma(x) \in M[x]$,

b) Fortsetzungen von σ zu einem Homomorphismus $\tau : K(a) \hookrightarrow M$ mit $\tau|_K = \sigma$.



Beweis. Zunächst ist die Abbildung wohldefiniert: Sei $\tau : K(a) \hookrightarrow M$ mit $\tau|_K = \sigma$ und sei $c := \tau(a)$, dann gilt

$$\begin{aligned} f^\sigma(c) &= f^\tau(c) && \text{wegen } \tau|_K = \sigma \\ &= f^\tau(\tau(a)) && \text{wegen } c = \tau(a) \\ &= \tau(f(a)) && \text{da } \tau \text{ Homomorphismus} \\ &= \tau(0) && \text{wegen } f(a) = 0 \\ &= 0 && \text{da } \tau \text{ Homomorphismus} \end{aligned}$$

Um die Bijektivität der Abbildung einzusehen, erinnern wir uns daran, dass $f \in K[x]$ das Minimalpolynom von a über K ist. Der durch Auswerten von Polynomen an der Stelle a gegebene Homomorphismus induziert somit nach dem Homomorphiesatz für Ringe einen Isomorphismus

$$K[x]/(f) \xrightarrow{\sim} K(a), \quad g(x) \mapsto g(a)$$

Die universelle Eigenschaft von Quotientenringen liefert eine Bijektion zwischen der Menge der

- Homomorphismen $\tau : K(a) \longrightarrow M$,
- Homomorphismen $\tilde{\tau} : K[x] \longrightarrow M$ mit $f \in \ker(\tilde{\tau})$.

Nach der universellen Eigenschaft von Polynomringen ist der Homomorphismus $\tilde{\tau}$ eindeutig bestimmt durch seine Werte auf den konstanten Polynomen und das Bild

von x, also durch

$$\tilde{\tau}(x) \;=\; \tau(a) \;\in\; M,$$

$$\tilde{\tau}|_K \;=\; \tau|_K \;\in\; \mathrm{Hom}(K,M).$$

Für $\tau(a) = c$ und $\tau|_K = \sigma$ erhalten wir explizit $\tilde{\tau}(g(x)) = g^\sigma(c)$. Für den Kern folgt damit

$$f \;\in\; \ker(\tilde{\tau}) \quad\Longleftrightarrow\quad f^\sigma(c) \;=\; 0$$

Wir können die bisherige Diskussion im folgenden Diagramm zusammenfassen:

$$\begin{array}{ccc} K[x] & \xrightarrow{\;g(x)\mapsto g^\sigma(c)\;} & M \\ \big\downarrow & & \big\uparrow{\scriptstyle \exists\tau} \\ K[x]/(f) & \xrightarrow{\;\sim\;} & K(a) \end{array} \qquad\Longleftrightarrow\qquad f^\sigma(c) \;=\; 0$$

Dasselbe Diagramm zeigt, dass τ im Fall der Existenz eindeutig durch den Wert c bestimmt ist. Somit folgt die Behauptung. □

Korollar 3.2. *Sei a algebraisch über K mit Minimalpolynom $f \in K[x]$. Dann sind für Homomorphismen $\sigma : K \hookrightarrow M$ äquivalent:*

a) Es existiert ein $c \in M$ mit $f^\sigma(c) = 0$.

b) Es existiert ein Homomorphismus $\tau : K(a) \hookrightarrow M$ mit $\tau|_K = \sigma$.

Beweis. Die genannten Bedingungen besagen genau, dass die beiden in Lemma 3.1 betrachteten Mengen nicht-leer sind. □

Bemerkung 3.3. Die Fortsetzung $\tau : K(a) \hookrightarrow M$ mit $\tau|_K = \sigma$ ist im Allgemeinen nicht eindeutig bestimmt: Jede Nullstelle des Minimalpolynoms liefert eine andere Fortsetzung. Die Einbettung $\sigma : K = \mathbb{Q} \hookrightarrow M = \mathbb{C}$ lässt sich auf genau zwei Arten fortsetzen zu

$$L \;:=\; \mathbb{Q}[x]/(x^2+1) \;\hookrightarrow\; \mathbb{C},$$

die beiden Fortsetzungen sind gegeben durch $x \mapsto +i$ bzw. durch $x \mapsto -i$.

Falls M algebraisch abgeschlossen ist, dann ist die erste Bedingung des vorigen Korollars 3.2 immer erfüllt. Durch iterative Anwendung des Korollars erhalten wir für die Ausdehnung von Homomorphismen in algebraisch abgeschlossene Körper:

Satz 3.4. *Sei K'/K eine algebraische Körpererweiterung, und sei $\sigma : K \hookrightarrow M$ ein Homomorphismus in einen algebraisch abgeschlossenen Körper M. Dann gibt es einen Homomorphismus*

$$\sigma' : \quad K' \;\hookrightarrow\; M \qquad \textit{mit} \qquad \sigma'|_K \;=\; \sigma.$$

Beweis. Wir wenden das Lemma von Zorn an auf die Menge

$$\mathscr{S} := \left\{ (L,\tau) \mid K \subseteq L \subseteq K' \text{ Zwischenkörper und } \tau \in \mathrm{Hom}(L,M) \text{ mit } \tau|_K = \sigma \right\}$$

mit der partiellen Ordnung $\preceq$ definiert durch

$$(L_1,\sigma_1) \preceq (L_2,\sigma_2) \quad :\Longleftrightarrow \quad L_1 \subseteq L_2 \text{ und } \sigma_2|_{L_1} = \sigma_1.$$

Dass es sich hierbei um eine partielle Ordnung auf der Menge $\mathscr{S}$ handelt, folgt sofort aus der Definition. Um das Lemma von Zorn anwenden zu können, müssen wir für jede Kette $\mathscr{K} \subseteq \mathscr{S}$ eine obere Schranke $(L^*,\tau^*) \in \mathscr{S}$ finden. Wir betrachten dazu

$$L^* := \bigcup_{(L,\tau)\in\mathscr{K}} L \subseteq K'.$$

Diese Vereinigung ist offenbar ein Zwischenkörper der Erweiterung K'/K, da sie die Vereinigung einer aufsteigenden Kette von Zwischenkörpern ist. Wir definieren ferner

$$\tau^* : \quad L^* \hookrightarrow M, \quad x \mapsto \tau(x) \quad \text{für beliebiges } (L,\tau) \in \mathscr{K} \text{ mit } L \ni x.$$

Dies ist wohldefiniert, d.h. das Bild $\tau(x) \in M$ hängt nicht vom gewählten $(L,\tau) \in \mathscr{K}$ mit $L \ni x$ ab:

- Seien $(L_1,\tau_1),(L_2,\tau_2) \in \mathscr{K}$ mit $x \in L_1 \cap L_2$.
- Nach Umnumerieren ist oBdA $(L_1,\tau_1) \preceq (L_2,\tau_2)$, da $\mathscr{K}$ eine Kette ist.
- Per Definition von $\preceq$ erhalten wir dann $\tau_2(x) = (\tau_2|_{L_1})(x) = \tau_1(x)$.

Somit ist das Lemma von Zorn anwendbar und liefert ein bezüglich $\preceq$ maximales Element $(L,\tau) \in \mathscr{S}$. Wir wollen zeigen, dass $L = K'$ ist. Hierzu argumentieren wir indirekt und nehmen an, es wäre $K' \neq L$. Wir können dann ein $a \in K'$ mit $a \notin L$ wählen. Da K'/K eine algebraische Erweiterung ist, ist das Element a algebraisch über K und somit erst recht über L. Das Korollar 3.2 liefert dann eine Fortsetzung des Homomorphismus $\tau : L \hookrightarrow M$ zu einem Homomorphismus $L(a) \hookrightarrow M$. Dies steht aber im Widerspruch zur Maximalität von (L,τ). □

Die obige Anwendung des Lemmas von Zorn ist intuitiver als in Prop. 2.5. Wenn man ähnlich auch für 2.5 vorgehen möchte, muß man allerdings beachten, dass die algebraischen Erweiterungen von K keine Menge bilden, so wie es auch keine Menge aller Mengen gibt; im Gegensatz dazu haben wir es im obigen Beweis nur mit Zwischenkörpern einer festen Erweiterung zu tun, diese bilden natürlich eine Menge. Die für uns wichtigste Folgerung aus dem obigen Satz ist die Aussage, dass der algebraische Abschluß bis auf Isomorphie eindeutig bestimmt ist:

Korollar 3.5. *Sei K ein Körper. Für je zwei algebraische Abschlüsse $L_1, L_2 \supseteq K$ existiert ein Isomorphismus*

$$\tau : \quad L_1 \xrightarrow{\sim} L_2$$

mit $\tau \circ i_1 = i_2$ für die Inklusionsabbildungen $i_1 : K \hookrightarrow L_1$ und $i_2 : K \hookrightarrow L_2$.

Beweis. Aus Satz 3.4 für die algebraische Erweiterung L_1/K und den algebraisch abgeschlossenen Körper $M = L_2$ erhalten wir die Existenz eines Homomorphismus

$$\tau: \quad L_1 \longrightarrow L_2 \quad \text{mit} \quad \tau \circ i_1 = i_2.$$

Nun gilt:

- Mit L_1 ist auch das Bild $\tau(L_1) \simeq L_1$ algebraisch abgeschlossen.
- Da L_2/K algebraisch ist, ist erst recht $L_2/\tau(L_1)$ algebraisch.

Da algebraisch abgeschlossene Körper keine echten algebraischen Erweiterungen haben, folgt $L_2 = \tau(L_1)$, d.h. τ ist surjektiv. Aber injektiv ist τ als Homomorphismus von Körpern sowieso. □

Die obige Eindeutigkeitsaussage wird uns manchmal dazu verleiten, von *dem* algebraischen Abschluß $\overline{K}$ eines Körpers K zu sprechen. Dabei ist aber Vorsicht geboten: Das Korollar 3.5 besagt lediglich, dass ein Isomorphismus existiert, es gibt aber keine bevorzugte Wahl für diesen Isomorphismus; der algebraische Abschluß eines Körpers ist nur eindeutig bis auf *nicht-kanonischen* Isomorphismus. Wenn eine exakte Kontrolle von Homomorphismen eine Rolle spielt, sollte man daher von *einem* statt von *dem* algebraischen Abschluß sprechen und sich klar machen, dass dabei eine Wahl getroffen wird.

Definition 3.6. Ein *Homomorphismus* zwischen Erweiterungen L_1/K und L_2/K ist ein Homomorphismus $\sigma : L_1 \longrightarrow L_2$ von Körpern, sodass das folgende Diagramm kommutiert:

$$\begin{array}{ccc} L_1 & \xrightarrow{\ \sigma\ } & L_2 \\ \uparrow & & \uparrow \\ K & = & K \end{array}$$

Wir schreiben dann $\sigma|_K = id$. Wir nennen σ einen *Isomorphismus*, falls σ bijektiv ist. Ein *Automorphismus* einer Körpererweiterung L/K ist ein Isomorphismus der Erweiterung auf sich. Wir setzen

$$\begin{aligned} \mathrm{Hom}_K(L_1, L_2) &:= \big\{ \text{Homomorphismen } \sigma : L_1 \longrightarrow L_2 \text{ mit } \sigma_K = id \big\}, \\ \mathrm{Aut}(L/K) &:= \big\{ \text{Automorphismen } \sigma : L \longrightarrow L \text{ mit } \sigma_K = id \big\}. \end{aligned}$$

Der Begriff eines Endomorphismus ist für *algebraische* Eweiterungen unnötig:

Lemma 3.7. *Für jede algebraische Erweiterung L/K ist* $\mathrm{Hom}_K(L,L) = \mathrm{Aut}(L/K)$.

Beweis. Sei $\sigma \in \mathrm{Hom}_K(L,L)$. Als Homomorphismus von Körpern ist σ injektiv, zu zeigen bleibt die Surjektivität. Dazu sei ein Element $a \in L$ gegeben. Sei $f(x) \in K[x]$ sein Minimalpolynom. Dann bildet σ die endliche Menge $Z = \{c \in L \mid f(c) = 0\}$ in sich ab. Da jede injektive Abbildung einer endlichen Menge in sich surjektiv ist, folgt $\sigma(Z) = Z$. Insbesondere existiert wegen $a \in Z$ ein $c \in Z$ mit $a = \sigma(c)$. □

Die Verkettung von Automorphismen macht $\mathrm{Aut}(L/K)$ zu einer Gruppe. Diese Gruppen werden uns in der Galoistheorie genauer beschäftigen. Sie operieren in natürlicher Weise auf den Nullstellen von Polynomen:

Beispiel 3.8. Sei K ein Körper. Für $f(x) = x^2 - a \in K[x]$ irreduzibel betrachten wir den Erweiterungskörper

$$L \;=\; K[x]/(f).$$

Es gilt $L = K(\sqrt{a})$ mit $\sqrt{a} := (x \bmod f) \in L$. Da jedes $\tau \in \mathrm{Aut}(L/K)$ die Nullstellen des Polynoms

$$\begin{aligned} f(x) \;&=\; x^2 - a \;\in\; K[x] \\ &=\; (x+\sqrt{a})(x-\sqrt{a}) \;\in\; L[x] \end{aligned}$$

permutiert und durch seine Wirkung auf diesen schon eindeutig festgelegt ist, ist der einzige ggf. von der Identität verschiedene Automorphismus $\tau \in \mathrm{Aut}(L/K)$ gegeben durch $\tau(\sqrt{a}) = -\sqrt{a}$. Es folgt

$$\mathrm{Aut}(L/K) \;=\; \{id, \tau\} \;\simeq\; \begin{cases} \mathbb{Z}/2\mathbb{Z} & \text{für } \mathrm{char}(K) \neq 2, \\ 0 & \text{für } \mathrm{char}(K) = 2. \end{cases}$$

Die obige Argumentation verallgemeinert sich wie folgt, wenn wir die Nullstellen von Polynomen mittels Lemma 3.1 mit Körpereinbettungen identifizieren:

Lemma 3.9. *Sei L/K eine algebraische Erweiterung und $\overline{K}/K$ ein algebraischer Abschluß des Grundkörpers. Dann operiert die Automorphismengruppe* $\mathrm{Aut}(L/K)$ *frei auf der Menge* $\mathrm{Hom}_K(L,\overline{K})$ *mittels*

$$\mathrm{Aut}(L/K) \times \mathrm{Hom}_K(L,\overline{K}) \;\longrightarrow\; \mathrm{Hom}_K(L,\overline{K}), \quad (\sigma, i) \;\mapsto\; i \circ \sigma^{-1}$$

Insbesondere ist

$$|\mathrm{Aut}_K(L)| \;\leq\; |\mathrm{Hom}_K(L,\overline{K})|.$$

Beweis. Nach Satz 3.4 existiert eine Einbettung $i : L \hookrightarrow \overline{K}$ mit $i|_K = id$, die Menge $\mathrm{Hom}_K(L,\overline{K})$ ist also nicht leer. Da die Verkettung von Homomorphismen wieder ein Homomorphismus ist, gilt $i \circ \sigma^{-1} \in \mathrm{Hom}_K(L,\overline{K})$ für alle $\sigma \in \mathrm{Aut}(L,K)$. Die im Lemma angegebene Abbildung ist somit wohldefiniert, und man rechnet sofort nach, dass sie eine Gruppenoperation definiert. Für beliebiges $i \in \mathrm{Hom}_K(L,\overline{K})$ ist die Abbildung

$$\mathrm{Aut}_K(L) \;\hookrightarrow\; \mathrm{Hom}_K(L,\overline{K}), \quad \sigma \;\mapsto\; i \circ \sigma$$

injektiv, weil i injektiv ist; also ist der Stabilisator $\mathrm{Stab}_{\mathrm{Aut}_K(L)}(i) = \{id\} \leq \mathrm{Aut}_K(L)$ trivial und somit ist die Gruppenoperation frei. □

Als nächstes wollen wir solche Erweiterungen betrachten, für die in Lemma 3.9 Gleichheit $|\mathrm{Aut}_K(L)| = |\mathrm{Hom}_K(L,\overline{K})|$ gilt. Diese heißen *normale* Erweiterungen; grob gesagt handelt es sich dabei um Erweiterungen mit vielen Automorphismen und ihre Untersuchung ist ein zentrales Ziel der Galoistheorie.

4 Zerfällungskörper und normale Erweiterungen

Der algebraische Abschluß eines Körpers ist im Allgemeinen sehr groß. Wenn man sich nur für Nullstellen *einiger* Polynome interessiert, kommt man mit kleineren Erweiterungskörpern aus:

Definition 4.1. Sei K ein Körper. Ein *Zerfällungskörper* einer Menge $S \subseteq K[x]$ von Polynomen ist ein Erweiterungskörper $L \supseteq K$, der die folgenden zwei Eigenschaften besitzt:

a) Jedes nichtkonstante Polynom $f \in S$ zerfällt über L in Linearfaktoren.

b) Es ist $L = K(Z)$ für die Nullstellenmenge $Z = \{a \in L \mid \exists f \in S : f(a) = 0\}$.

Im Fall $S = \{f\}$ heißt L auch ein *Zerfällungskörper des Polynoms f über K*.

Zerfällungskörper sind insbesondere algebraisch über K, da sie nach b) von einer Menge algebraischer Elemente über K erzeugt werden. Ein Zerfällungskörper zu der Menge $S = K[x]$ ist nichts anderes als ein algebraischer Abschluß. Einige Beispiele von Zerfällungskörpern $L/\mathbb{Q}$ zu Polynomen $f(x) \in \mathbb{Q}[x]$:

$f(x)$	L
x^2+1	$\mathbb{Q}(i)$
x^n-1	$\mathbb{Q}(e^{2\pi i/n})$
x^3-2	$\mathbb{Q}(\sqrt[3]{2}, e^{2\pi i/3})$

Allgemeiner gibt es zu jeder Menge von Polynomen einen Zerfällungskörper, und dieser ist bis auf Isomorphie eindeutig:

Proposition 4.2. *Sei K ein Körper und $S \subseteq K[x]$. Dann gilt:*

a) Es gibt einen Zerfällungskörper L/K von S über K.

b) Je zwei solche sind als Erweiterungen von K zueinander isomorph.

Beweis. Für die Existenz wählen wir einen algebraischen Abschluß $\overline{K}/K$, dann hat der Teilkörper

$$L := K(Z) \subseteq \overline{K} \quad \text{erzeugt von} \quad Z := \{a \in \overline{K} \mid \exists f \in S : f(a) = 0\}$$

die für einen Zerfällungskörper geforderten Eigenschaften. Für die Eindeutigkeit seien L_1, L_2 zwei Zerfällungskörper von S über K. Wir wählen für jeden der beiden einen algebraischen Abschluß $\overline{L}_i \supseteq L_i$. Da die Erweiterung L_i/K algebraisch ist, ist dann $\overline{L}_i$ auch ein algebraischer Abschluß von K. Da je zwei algebraische Abschlüsse nach Korollar 3.5 isomorph sind, können wir einen Isomorphismus $\tau : \overline{L}_1 \to \overline{L}_2$ finden, sodass das folgende Diagramm kommutiert:

$$\begin{array}{ccc} \overline{L}_1 & \xrightarrow{\tau} & \overline{L}_2 \\ \uparrow & & \uparrow \\ L_1 & & L_2 \\ \uparrow & & \uparrow \\ K & = & K \end{array}$$

Wir wollen $\tau(L_1) = L_2$ zeigen. Per Definition von Zerfällungskörpern ist $L_i = K(Z_i)$ mit

$$Z_i \;:=\; \{a \in L_i \mid \exists f \in S\colon f(a) = 0\} \;=\; \{a \in \overline{L}_i \mid \exists f \in S\colon f(a) = 0\}.$$

Wir müssen daher nur $\tau(Z_1) = Z_2$ zeigen. Dazu betrachten wir für jedes feste $f \in S$ die Mengen

$$Z_i(f) \;:=\; \{a \in \overline{L}_i \mid f(a) \;=\; 0\}.$$

OBdA sei $f \in S$ normiert und

$$\begin{aligned} f(x) \;&=\; (x-a_1)\cdots(x-a_n) \quad \text{in} \quad \overline{L}_1[x] \\ &=\; (x-b_1)\cdots(x-b_n) \quad \text{in} \quad \overline{L}_2[x]. \end{aligned}$$

Wegen $f^\tau = f$ für $f \in K[x]$ folgt

$$\prod_{k=1}^{n}(x-\tau(a_k)) \;=\; f^\tau(x) \;=\; f(x) \;=\; \prod_{l=1}^{n}(x-b_l),$$

also $\tau(Z_1(f)) = \{\tau(a_1),\ldots,\tau(a_n)\} = \{b_1,\ldots,b_n\} = Z_2(f)$ wie gewünscht. □

Im Folgenden fixieren wir einen algebraischen Abschluß $\overline{K}/K$. Wir können dann Zerfällungskörper auf viele Arten charakterisieren:

Satz 4.3. *Sei L/K eine algebraische Erweiterung. Dann sind äquivalent:*

a) L ist Zerfällungskörper einer Teilmenge $S \subseteq K[x]$.

b) Es gibt eine Einbettung $i \in \mathrm{Hom}_K(L,\overline{K})$ mit $\tau(i(L)) = i(L)$ für alle $\tau \in \mathrm{Aut}(\overline{K}/K)$.

c) Die Operation in Lemma 3.9 ist transitiv, liefert also für festes $i \in \mathrm{Hom}_K(L,\overline{K})$ eine Bijektion

$$\mathrm{Aut}(L/K) \;\xrightarrow{\sim}\; \mathrm{Hom}_K(L,\overline{K}), \quad \sigma \;\mapsto\; i\circ\sigma.$$

d) Für jede Einbettung $i \in \mathrm{Hom}_K(L,\overline{K})$ gilt $\tau(i(L)) = i(L)$ für alle $\tau \in \mathrm{Aut}(\overline{K}/K)$.

e) Jedes irreduzible Polynom $f \in K[x]$ mit einer Nullstelle $a \in L$ zerfällt in $L[x]$ in Linearfaktoren:

$$f(x) \;=\; c\cdot\prod_{i=1}^{n}(x-a_i) \quad \textit{mit } c \in K^\times \textit{ und } a_1,\ldots,a_n \in L.$$

Beweis. Wenn $a)$ gilt, existiert wegen der Eindeutigkeit von Zerfällungskörpern ein Isomorphismus

$$i\colon \quad L \xrightarrow{\sim} K(Z) \subseteq \overline{K} \quad \text{für die Teilmenge} \quad Z = \{a \in \overline{K} \mid \exists f \in S : f(a) = 0\}.$$

Da jedes $\tau \in \mathrm{Aut}_K(\overline{K}/K)$ die Menge der Nullstellen jedes festen Polynoms $f \in K[x]$ bijektiv auf sich abbildet, gilt $\tau(Z) = Z$ und somit $\tau(i(L)) = i(L)$, also $b)$.

Sei nun eine Einbettung i wie in $b)$ gegeben. Nach dem Fortsetzungssatz 3.4 gibt es für jede weitere Einbettung $\rho \in \mathrm{Hom}_K(L,\overline{K})$ ein $\tau \in \mathrm{Hom}_K(\overline{K},\overline{K}) = \mathrm{Aut}(\overline{K}/K)$ mit $\rho = \tau \circ i$ wie im folgenden Diagramm angedeutet:

$$\begin{array}{ccc} \overline{K} & \overset{\exists\tau}{\dashrightarrow} & \overline{K} \\ {\scriptstyle i}\uparrow & \nearrow_{\rho} & \\ L & & \end{array}$$

Nach Annahme gilt $\rho(L) = \tau(i(L)) = i(L)$, also faktorisiert ρ über $i(L) \subseteq \overline{K}$ und wir erhalten

$$\rho \;=\; i \circ \sigma \quad \text{für ein} \quad \sigma \;\in\; \mathrm{Hom}_K(L,L) \;=\; \mathrm{Aut}_K(L)$$

wie in $c)$ gefordert. Man beachte, dass die Aussage $c)$ nicht von der Wahl von i abhängt: Wenn eine Gruppenoperation auf einer Menge transitiv ist, dann ist der Orbit jeden Elementes bereits die gesamte Menge. Wenn wir die Surjektivität in $c)$ auf

$$\tau \circ i \;\in\; \mathrm{Hom}_K(L,\overline{K}) \quad \text{für beliebige} \quad i \in \mathrm{Hom}_K(L,\overline{K}), \quad \tau \in \mathrm{Aut}_K(\overline{K})$$

anwenden, erhalten wir $d)$. Gelte nun $d)$. Sei $f \in K[x]$ irreduzibel mit $f(a) = 0$ für ein $a \in L$. Sei

$$f(x) \;=\; c \cdot \prod_{k=1}^{n} (x - a_k) \quad \text{mit } c \in K^\times \text{ und } a_1, \ldots, a_n \in \overline{K}.$$

Sei $i : L \hookrightarrow \overline{K}$ fest gewählt. Durch Einschränken erhalten wir $K(a) \hookrightarrow \overline{K}$. Da f das Minimalpolynom jedes der Elemente $a, a_1, \ldots, a_n$ ist, haben wir für jedes k einen Isomorphismus $\sigma : K(a) \to K(a_i)$ mit $a \mapsto a_i$. Nach dem Fortsetzungssatz 3.4 lässt sich dieser fortsetzen zu einem Automorphismus $\tau \in \mathrm{Aut}(\overline{K}/K)$, sodass

$$\begin{array}{ccc} \overline{K} & \overset{\exists\tau}{\dashrightarrow} & \overline{K} \\ \uparrow & & \uparrow \\ K(a) & \xrightarrow{\sigma} & K(a_k) \end{array}$$

kommutiert. Es folgt $a_k = \tau(i(a)) \in \tau(i(L)) = i(L)$, also $a_k = i(b_k)$ für ein $b_k \in L$ und somit zerfällt $f(x) = c \cdot \prod_k (x - b_k)$ auch in $L[x]$. Aus $e)$ folgt schließlich die Aussage $a)$ trivialerweise. $\square$

Definition 4.4. Eine algebraische Erweiterung L/K heißt *normal*, wenn für sie die Eigenschaften aus Satz 4.3 gelten. Wir sagen dann, der Körper L sei *normal über* K.

Beispiel 4.5. Es gilt:

a) Jede Erweiterung L/K mit $[L:K]=2$ ist normal (Übung).

b) Der Körper $L=\mathbb{Q}(\sqrt[3]{2})\subset\mathbb{R}$ ist nicht normal über $\mathbb{Q}$: Denn $f(x)=x^3-2\in\mathbb{Q}[x]$ ist über den rationalen Zahlen irreduzibel, aber nur eine seiner drei komplexen Nullstellen liegt im Teilkörper $L\subseteq\mathbb{R}$ und die übrigen beiden sind nicht reell.

c) Sei $K=\mathbb{Q}\subset L=\mathbb{Q}(\sqrt{2})\subset M=\mathbb{Q}(\sqrt[4]{2})\subset\mathbb{R}$. Dann gilt:

- Die Erweiterungen M/L und L/K sind normal nach Beispiel a).
- Die Erweiterung M/K ist jedoch nicht normal. Denn $f(x)=x^4-2\in K[x]$ ist über K irreduzibel und hat die Nullstelle $\sqrt[4]{2}\in M$, zerfällt jedoch nicht in Linearfaktoren über M: Es ist

$$f(x) \;=\; (x+\sqrt[4]{2})(x-\sqrt[4]{2})(x^2+\sqrt{2}),$$

und $x^2+\sqrt{2}$ ist über M irreduzibel, da es keine reelle Nullstelle hat.

d) Seien $K\subseteq L\subseteq M$ Körpererweiterungen. Wenn M/K normal ist, dann auch M/L.

So wie wir jeden Körper in einen algebraischen Abschluß einbetten können, lässt sich jede algebraische Erweiterung in eine kleinstmögliche normale Erweiterung einbetten:

Definition 4.6. Sei L/K eine algebraische Erweiterung. Eine *normale Hülle* von L/K ist eine algebraische Erweiterung L'/L mit den folgenden beiden Eigenschaften:

a) Die Erweiterung L'/K ist normal.

b) Kein echter Zwischenkörper von L'/L ist normal über K.

Jede algebraische Erweiterung hat eine normale Hülle, und diese ist eindeutig bis auf Isomorphie. Das folgt aus der entsprechenden Aussage für Zerfällungskörper, denn es gilt:

Satz 4.7. *Für algebraische Erweiterungen $K\subseteq L\subseteq L'$ sind äquivalent:*

a) L' ist eine normale Hülle von L/K.

b) L' ist ein Zerfällungskörper der Menge

$$S \;:=\; \{\,\textit{Minimalpolynome von Elementen } a\in L \textit{ über } K\,\} \;\subseteq\; K[x].$$

c) Für jede algebraische Erweiterung M/L, sodass M normal über K ist, gilt:

$$L' \;\simeq\; K(Z) \;\subseteq\; M \quad \textit{mit} \quad Z \;:=\; \{\,\sigma(a)\in M \mid a\in L,\,\sigma\in \mathrm{Hom}_K(L,M)\,\}.$$

d) Die vorige Aussage gilt für einen algebraischen Abschluß $M=\overline{L}$ von L.

Beweis. Sei S die Menge der Minimalpolynome von Elementen $a \in L$. Wenn $a)$ gilt, dann zerfällt wegen der Normalität von L'/K jedes $f \in S$ über L' vollständig in Linearfaktoren, da es per Konstruktion eine Nullstelle $a \in L$ besitzt. Daher ist der Teilkörper

$$K(Z') \subseteq L' \quad \text{erzeugt von} \quad Z' := \{a \in L' \mid \exists f \in S : f(a) = 0\}$$

ein Zerfällungskörper von S über K. Insbesondere ist er normal über K, und wegen der Minimalität der normalen Hülle folgt $K(Z') = L'$ wie in $b)$ behauptet.

Sei nun M/L eine algebraische Erweiterung mit M normal über K. Dann ist der Teilkörper

$$K(Z) \subseteq M \quad \text{erzeugt von} \quad Z := \{b \in M \mid \exists f \in S : f(b) = 0\}$$

ein Zerfällungskörper von S über K. Wenn $b)$ gilt, erhalten wir somit wegen der Eindeutigkeit von Zerfällungskörpern einen Isomorphismus $L' \simeq K(Z) \subseteq M$. Aus der Normalität von M/L folgt zudem

$$\begin{aligned} Z &= \{b \in \overline{M} \mid \exists f \in S : f(b) = 0\} \\ &= \{\sigma(a) \in \overline{M} \mid a \in L,\ \sigma \in \mathrm{Hom}_K(L, \overline{M})\} \\ &= \{\sigma(a) \in M \mid a \in L,\ \sigma \in \mathrm{Hom}_K(L, M)\} \end{aligned}$$

und somit $c)$. Aus $c)$ folgt trivialerweise $d)$. Aus $d)$ folgt $a)$, denn man sieht leicht, dass der Teilkörper

$$K(Z) \subseteq \overline{L} \quad \text{erzeugt von} \quad Z = \{b \in \overline{L} \mid f(b) = 0\}$$

den Körper L enthält, normal über K ist, und minimal mit dieser Eigenschaft ist. □

5 Separable Erweiterungen

Wir haben gesehen, dass für jede algebraische Körpererweiterung L/K die Menge ihrer Automorphismen kontrolliert wird durch Einbettungen in einen algebraischen Abschluß $\overline{K}/K$. Insbesondere ist

$$|\mathrm{Aut}(L/K)| \leq |\mathrm{Hom}_K(L, \overline{K})|,$$

und Gleichheit gilt genau für normale Erweiterungen. Wir wollen nun unabhängig davon, ob die Erweiterung normal ist oder nicht, die rechte Seite der Ungleichung untersuchen. Für Erweiterungen, die von einem Element erzeugt werden, ist dies besonders einfach:

Beispiel 5.1. Sei $L = K(a)$ für ein $a \in L$ mit Minimalpolynom $f \in K[x]$. Lemma 3.1 gibt eine Bijektion

$$\mathrm{Hom}_K(L,\overline{K}) \xrightarrow{\sim} \{b \in \overline{K} \mid f(b) = 0\}, \quad \tau \mapsto \tau(a).$$

Da $f \in K[x]$ über dem algebraischen Abschluß in höchstens $\deg(f)$ verschiedene Linearfaktoren zerfallen kann, folgt

$$|\mathrm{Hom}_K(L,\overline{K})| \leq \deg(f) = [L:K].$$

Gleichheit gilt genau dann, wenn alle Linearfaktoren verschieden sind:

Definition 5.2. Ein irreduzibles Polynom $f \in K[x]$ heißt *separabel*, wenn es in $\overline{K}$ keine mehrfachen Nullstellen hat, wenn also

$$f(x) = c \cdot \prod_{k=1}^{n} (x - a_k) \quad \text{mit paarweise verschiedenen } a_1, \ldots, a_n \in \overline{K}$$

gilt (Etymologie: Die Nullstellen können in $\overline{K}$ voneinander "separiert" werden).

Ein Element a einer algebraischen Erweiterung L/K heißt *separabel über K*, wenn sein Minimalpolynom über K separabel ist. Man beachte, dass hierbei der Grundkörper eine Rolle spielt. Um die Separabilität von a über K zu prüfen, muß man nicht das genaue Minimalpolynom kennen; es genügt, ein Polynom $f \in K[x]$ zu finden, sodass gilt:

a) Es ist $f(a) = 0$,

b) Jeder irreduzible Teiler von f in $K[x]$ ist separabel.

Polynome $f \in K[x]$ mit Eigenschaft b) heißen *separabel*, die übrigen *inseparabel*.

Wir werden bald sehen, dass über Körpern der Charakteristik Null jedes Polynom separabel ist. Über Körpern der Charakteristik $p > 0$ treten jedoch neue Phänomene auf. Sei R ein kommutativer Ring und p eine Primzahl mit $p \cdot 1 = 0$ in R. Dann ist die Abbildung

$$\mathrm{Frob}_p : \quad R \longrightarrow R, \quad a \mapsto a^p$$

ein Ringhomomorphismus: Denn die Verträglichkeit mit der Multiplikation ist klar, und für die Addition berechnet man

$$(a+b)^p = \sum_{k=0}^{p} \binom{p}{k} \cdot a^k b^{p-k} = a^p + b^p$$

weil die auftretenden Binomialkoeffizienten durch p teilbar sind für $0 < k < p$. Wir nennen Frob_p den *Frobenius-Homomorphismus*.

Beispiel 5.3. Sei K ein Körper der Charakteristik $p = \mathrm{char}(K) > 0$. Sei $b \in \overline{K}$ eine Nullstelle von

$$f(x) \;=\; x^p - a \;\in\; K[x].$$

Über dem algebraischen Abschluß des Grundkörpers erhalten wir dann für $f(x)$ die Faktorisierung

$$\begin{aligned} f(x) \;&=\; x^p - b^p && \text{wegen } a = b^p \\ &=\; (x-b)^p && \text{da } \mathrm{Frob}_p : \overline{K}[x] \to \overline{K}[x] \text{ ein Homomorphismus ist} \end{aligned}$$

Daher hat das Polynom $f(x)$ über dem algebraischen Abschluß nur eine Nullstelle, wir schreiben auch

$$b \;=\; \sqrt[p]{a} \;\in\; \overline{K}.$$

Es gilt:

a) Für $\sqrt[p]{a} \in K$ ist das Polynom $f(x)$ separabel.

b) Für $\sqrt[p]{a} \notin K$ ist das Polynom $f(x)$ irreduzibel und nicht separabel.

Der zweite Fall kann eintreteten: Ein Beispiel erhält man, indem man für $K = \mathbb{F}_p(y)$ den Körper der rationalen Funktionen in einer Variablen y über $\mathbb{F}_p$ wählt.

Als nächstes wollen wir zeigen dass das obige Phänomen der einzige Grund für die Existenz inseparabler Polynome ist. Dazu benötigen wir ein Kriterium für die Existenz mehrfacher Nullstellen, das die Ableitung von Polynomen benutzt:

Definition 5.4. Die *(formale) Ableitung* von Polynomen über einem Körper K ist definiert durch

$$f'(x) \;:=\; \sum_{k=1}^{n} a_k \cdot k \cdot x^{k-1} \;\in\; K[x] \quad \text{für} \quad f(x) \;=\; \sum_{k=0}^{n} a_k \cdot x^k \;\in\; K[x].$$

Ein Element $a \in \overline{K}$ heißt eine *mehrfache Nullstelle* von $f \in K[x]$, wenn ein $g \in \overline{K}[x]$ existiert mit

$$f(x) \;=\; (x-a)^2 \cdot g(x).$$

Die Existenz einer mehrfachen Nullstelle kann man durch Berechnen von $\mathrm{ggT}(f, f')$ mit dem Euklidischen Algorithmus prüfen, ohne die Nullstelle zu kennen:

Lemma 5.5. *Sei K ein Körper und $f \in K[x]$.*

a) Es ist $a \in \overline{K}$ eine mehrfache Nullstelle von f genau für $f(a) = f'(a) = 0$.

b) Eine solche mehrfache Nullstelle existiert genau dann, wenn $\mathrm{ggT}(f, f') \neq 1$ *ist.*

Beweis. Sei $a \in \overline{K}$ gegeben und $m = \mathrm{ord}_a(f) \in \mathbb{N}_0$ die Nullstellenordnung in diesem Punkt, also $f(x) = (x-a)^m \cdot g(x)$ für ein $g(x) \in \overline{K}[x]$ mit $g(a) \neq 0$. Die Leibnizregel für Ableitungen zeigt

$$f'(x) \;=\; (x-a)^m \cdot g'(x) + m \cdot (x-a)^{m-1} \cdot g(x)$$

Also gilt $m \geq 2$ genau für $f(a) = f'(a) = 0$ wie in $a)$ behauptet. Ist dies der Fall, so gilt

$$(x-a) \mid \mathrm{ggT}(f, f')$$

in $\overline{K}[x]$ und somit $\mathrm{ggT}(f, f') \neq 1$. Ist umgekehrt letzteres der Fall, so haben f und f' einen gemeinsamen Teiler $h \in K[x]$ mit $\deg(h) > 0$, und jede Nullstelle $a \in \overline{K}$ dieses Teilers ist nach der Leibnizregel eine mehrfache Nullstelle von f. □

Als Folgerung erhalten wir, dass das pathologische Verhalten im Beispiel 5.3 der einzige Grund für die Existenz inseparabler Polynome ist:

Korollar 5.6. *Sei $f \in K[x]$ irreduzibel. Dann sind folgende Aussagen äquivalent:*

a) Das Polynom f ist inseparabel.

b) Es ist $f' = 0$ das Nullpolynom in $K[x]$.

c) Es ist $p = \mathrm{char}(K) > 0$ und $f(x) = g(x^p)$ für ein $g(x) \in K[x]$.

Beweis. Da $f \in K[x]$ irreduzibel ist und $\deg(f') < \deg(f)$ gilt, können f und f' keinen gemeinsamen Teiler haben — es sei denn, die formale Ableitung ist das Nullpolynom. Somit ist $a)$ äquivalent zu $b)$ nach Lemma 5.5. Um die Äquivalenz von $b)$ und $c)$ zu sehen, schreiben wir

$$f'(x) \;=\; \sum_{k=1}^{n} k \cdot a_k \cdot x^{k-1} \;=\; 0 \quad \text{für das Polynom} \quad f(x) \;=\; \sum_{k=0}^{n} a_k \cdot x^k \;\in\; K[x].$$

Dann gilt

$$\begin{aligned} f'(x) = 0 &\iff k \cdot a_k = 0 \text{ für alle } k \geq 1 \\ &\iff a_k = 0 \text{ für alle } k \text{ mit } p \nmid k \\ &\iff f(x) = g(x^p) \text{ für ein Polynom } g(x) \in K[x] \end{aligned}$$

und somit folgt die Behauptung. □

Ein Körper K heißt *perfekt*, falls jedes Polynom $f \in K[x]$ separabel ist. Dies ist offenbar äquivalent zu der Bedingung, dass jedes Element $a \in \overline{K}$ separabel über K ist. Das einfachste Beispiel eines nicht perfekten Körpers ist der bereits betrachtete Funktionenkörper

$$K \;=\; \mathbb{F}_p(y),$$

siehe Beispiel 5.3. Wir fassen zusammen:

Korollar 5.7. *Ein Körper K ist perfekt genau dann, wenn gilt:*

a) Es ist $\mathrm{char}(K) = 0$, oder

b) $\mathrm{char}(K) = p > 0$ und $\mathrm{Frob}_p : K \to K$ ist surjektiv.

Beweis. OBdA sei $\mathrm{char}(K) = p > 0$. Wenn K perfekt ist, muß für jedes $a \in K$ das Polynom $f(x) = x^p - a$ separabel sein; nach Beispiel 5.3 ist dann $\sqrt[p]{a} \in K$. Also ist der Homomorphismus

$$\mathrm{Frob}_p : K \to K$$

surjektiv. Sei nun umgekehrt letzteres der Fall, und sei $f \in K[x]$ irreduzibel. Wenn f eine mehrfache Nullstelle $a \in \overline{K}$ hätte, dann gäbe es nach Korollar 5.6 ein $g \in K[x]$ mit $f(x) = g(x^p)$. Wegen der Surjektivität des Frobeniushomomorphismus könnten wir aber ein Polynom $h \in K[x]$ finden, sodass g durch Anwenden von Frob_p auf die Koeffizienten von h entsteht, und dann wäre $f(x) = g(x^p) = (h(x))^p$ reduzibel. □

Insbesondere müssen imperfekte Körper positive Charakteristik haben, und sie müssen unendlich viele Elemente enthalten:

Korollar 5.8. *Jeder endliche Körper ist perfekt.*

Beweis. Als Körperhomomorphismus ist $\mathrm{Frob}_p : K \to K$ injektiv, und jede injektive Abbildung einer endlichen Menge in sich ist bijektiv. □

Kommen wir zur Frage nach Einbettungen einer algebraischen Erweiterung L/K in einen algebraischen Abschluß $\overline{K}/K$ zurück. Unter dem *Separabilitätsgrad* der Erweiterung verstehen wir die Kardinalität

$$[L : K]_{\mathrm{sep}} := |\mathrm{Hom}_K(L, \overline{K})|.$$

Analog zur Gradformel gilt:

Proposition 5.9. *Für den Separabilitätsgrad endlicher Erweiterungen $K \subseteq L \subseteq M$ gilt*

$$[M : K]_{\mathrm{sep}} = [M : L]_{\mathrm{sep}} \cdot [L : K]_{\mathrm{sep}}.$$

Beweis. Nach dem Fortsetzungssatz 3.4 können wir für jedes $\sigma \in \mathrm{Hom}_K(L, \overline{K})$ eine Fortsetzung

$$\overline{\sigma} \in \mathrm{Aut}(\overline{K}/K) \quad \text{mit} \quad \overline{\sigma}|_L = \sigma_i$$

wählen. Wir fixieren im Folgenden eine solche Wahl $\overline{\sigma}$ für jedes σ und betrachten die Abbildung

$$\mathrm{Hom}_K(L, \overline{K}) \times \mathrm{Hom}_L(M, \overline{K}) \longrightarrow \mathrm{Hom}_K(M, \overline{K}), \quad (\sigma, \tau) \mapsto \overline{\sigma} \circ \tau.$$

Diese Abbildung ist injektiv, denn es gilt:

$$\rho = \overline{\sigma} \circ \tau \quad \Longrightarrow \quad \sigma = \rho|_L \quad \text{und} \quad \tau = \overline{\sigma}^{-1} \circ \rho.$$

Die Abbildung ist zudem surjektiv, denn es gilt:

$$\begin{aligned} \rho \in \mathrm{Hom}_K(M, \overline{K}) \quad &\Longrightarrow \quad \sigma := \rho|_L \in \mathrm{Hom}_K(L, \overline{K}) \\ &\Longrightarrow \quad \tau := \overline{\sigma}^{-1} \circ \rho \in \mathrm{Hom}_L(M, \overline{K}) \quad \text{erfüllt} \quad \rho = \overline{\sigma} \circ \tau \end{aligned}$$

Somit folgt die Behauptung. □

Satz 5.10. *Sei L/K eine endliche Erweiterung. Dann gilt $[L:K]_{\text{sep}} \leq [L:K]$, und folgende Bedingungen sind äquivalent:*

a) Es ist $[L:K]_{\text{sep}} = [L:K]$.

b) Jedes $a \in L$ ist separabel über K.

c) Es gibt über K separable $a_1, \ldots, a_n \in L$ mit $L = K(a_1, \ldots, a_n)$.

Beweis. Sei zunächst $L = K(a)$ für ein $a \in L$ mit Minimalpolynom $f \in K[x]$. Im Fall $\text{char}(K) = 0$ sind dann die drei genannten Eigenschaften immer erfüllt und es ist nichts zu zeigen. Im Fall $p = \text{char}(K) > 0$ liefert sukzessives Anwenden von Korollar 5.6 ein $n \in \mathbb{N}_0$ mit

$$f(x) \;=\; g(x^{p^n}) \quad \text{für ein separables Polynom } g(x) \in K[x].$$

Insbesondere hat das Polynom f dann genau $\deg(g)$ verschiedene Nullstellen in $\overline{K}$ und es folgt

$$[L:K]_{\text{sep}} \;:=\; |\text{Hom}_K(L, \overline{K})| \;=\; \deg(g) \;\leq\; \deg(f) \;=\; [L:K]$$

mit Gleichheit genau dann, wenn das Element $a \in L$ separabel über K ist.

Sei nun allgemein eine endliche Erweiterung $L = K(a_1, \ldots, a_n)$ mit $a_1, \ldots, a_n \in L$ gegeben. Wir setzen $a = a_1$. Nach dem vorigen Schritt und per Induktion über n dürfen wir

$$[L:K(a)]_{\text{sep}} \;\leq\; [L:K(a)] \tag{III.1}$$

$$[K(a):K]_{\text{sep}} \;\leq\; [K(a):K] \tag{III.2}$$

annehmen. Der Gradsatz und Proposition 5.9 liefern dann

$$[L:K]_{\text{sep}} \;=\; [L:K(a)]_{\text{sep}} \cdot [K(a):K]_{\text{sep}} \;\leq\; [L:K(a)] \cdot [K(a):K] \;=\; [L:K]$$

und damit die erste Behauptung des Satzes. Zudem gilt Gleichheit genau dann, wenn in (III.1) und (III.2) Gleichheit gilt. Die Gleichheit in (III.2) ist nach dem zu Beginn Bewiesenen äquivalent zu der Separabilität des Elementes $a \in L$ über K. Da wir dieses Element beliebig wählen dürfen, ist die Äquivalenz der im Satz genannten Bedingungen *a)* und *b)* klar. Aus *b)* folgt *c)* trivialerweise, und aus *c)* folgt *a)* per Induktion über die Anzahl der Erzeuger, weil ein über K separables Element auch separabel über jedem Erweiterungskörper von K ist. □

Eine endliche algebraische Erweiterung L/K heißt *separabel*, wenn sie die drei äquivalenten Eigenschaften des vorigen Satzes erfüllt. Allgemeiner bezeichnen wir eine algebraische Erweiterung L/K als separabel, wenn jedes $a \in L$ separabel über K ist, wenn sie also eine Vereinigung endlicher separabler Erweiterungen ist. Jede endliche separable Erweiterung lässt sich von einem Element erzeugen, genauer gilt sogar:

Satz 5.11. *Sei L/K eine algebraische Erweiterung von der Form $L = K(a, b_1, \ldots, b_n)$ mit*

- *$a \in L$ beliebig,*
- *$b_1, \ldots, b_n \in L$ separabel über K.*

Dann existiert ein Element $c \in L$ mit $L = K(c)$.

Beweis. Wegen $K(a, b_1, \ldots, b_n) = (K(b_2, \ldots, b_n))(a, b_1)$ genügt es per Induktion, den Fall $n = 1$ zu behandeln. Wir betrachten also einen Erweiterungskörper von der Form

$$L \;=\; K(a,b) \quad \text{mit } a,b \text{ algebraisch und } b \text{ separabel über } K.$$

Für das gesuchte Element $c \in L$ mit $L = K(c)$ machen wir den Ansatz $c = a + \lambda b$ mit $\lambda \in K$. Wir betrachten den Zwischenkörper

$$K \;\subseteq\; K(c) \;\subseteq\; L.$$

Wegen $L = K(a,b) = K(b,c)$ sind wir fertig, wenn wir ein λ finden mit $b \in K(c)$.

Nach Voraussetzung ist b separabel über K, also auch über $K(c)$. Wenn $b \notin K(c)$ ist, hat sein Minimalpolynom über $K(c)$ also mindestens zwei unterschiedliche Nullstellen in einem algebraischen Abschluß $\overline{K}/K$. Nach dem Fortsetzungssatz 3.4 existiert dann ein

$$\sigma \;\in\; \mathrm{Hom}_{K(c)}(L, \overline{K}) \;\subseteq\; \mathrm{Hom}_K(L, \overline{K}) \quad \text{mit} \quad \sigma(b) \;\neq\; b.$$

Aus $\sigma(c) = c$ folgt dann $\sigma(a) + \lambda\sigma(b) = a + \lambda b$, und wir erhalten somit insgesamt die Gleichung

$$\lambda \;=\; -\frac{\sigma(a) - a}{\sigma(b) - b}.$$

Für die rechte Seite gibt es aber nur endlich viele Möglichkeiten, und diese sind a priori bereits durch a und b festgelegt: Denn die Elemente $\sigma(a)$ bzw. $\sigma(b)$ müssen ja Nullstellen des Minimalpolynoms von a bzw. b über K sein. Wenn der Körper K unendlich viele Elemente enthält, können wir also $\lambda \in K$ so wählen, dass es mit keinem der endlich vielen durch die Minimalpolynome von a und b bestimmten Werte übereinstimmt; dann leistet $c = a + \lambda b$ das Gewünschte.

Falls K ein endlicher Körper ist, funktioniert dieses Argument nicht. Dieser Fall kann aber direkt behandelt werden: Dann ist auch L endlich, und aus den Übungen wissen wir, dass die multiplikative Gruppe jedes endlichen Körpers zyklisch ist; es gibt also ein $c \in L^\times$ mit $L^\times = \{c^n \mid n \in \mathbb{Z}\}$ und somit folgt $L = K(c)$. □

Korollar 5.12 (Satz vom primitiven Element). *Sei L/K eine endliche separable Erweiterung. Dann ist*

$$L \;=\; K(c) \quad \textit{für ein} \quad c \;\in\; L.$$

Beweis. Folgt sofort aus dem vorigen Satz. □

6 Galoiserweiterungen

Unsere Untersuchung von Automorphismen endlicher Erweiterungen L/K hat auf die Ungleichungen

$$|\mathrm{Aut}(L/K)| \;\leq\; |\mathrm{Hom}_K(L,\overline{K})| \;\leq\; [L:K]$$

geführt, wobei gilt:

- L/K ist normal genau dann, wenn die erste Ungleichung eine Gleichung ist.
- L/K ist separabel genau dann, wenn die zweite Ungleichung eine Gleichung ist.

Körpererweiterungen mit der größtmöglichen Automorphismengruppe haben einen eigenen Namen:

Definition 6.1. Eine algebraische Erweiterung L/K heißt eine *Galoiserweiterung*, wenn sie normal und separabel ist. Für endliche Erweiterungen ist dies äquivalent zu der Bedingung

$$|\mathrm{Aut}(L/K)| \;=\; [L:K].$$

Wir nennen $\mathrm{Gal}(L/K) := \mathrm{Aut}(L/K)$ dann auch die *Galoisgruppe* von L/K.

Die Galoiserweiterungen von Körpern der Charakteristik Null sind genau ihre normalen Erweiterungen, da Separabilität hier automatisch gilt. Schauen wir uns einige einfache Beispiele an:

Beispiel 6.2. Sei L der Zerfällungskörper von $f(x) = x^3 - 2$ über $K = \mathbb{Q}$. Dann ist L/K eine Galoiserweiterung, denn wegen $\mathrm{char}(K) = 0$ ist sie automatisch separabel und als Zerfällungskörper ist sie auch normal. Die Galoisgruppe $\mathrm{Gal}(L/K)$ operiert auf der Menge der Nullstellen

$$Z(f) \;=\; \{a \in \mathbb{C} \mid f(a) = 0\} \;=\; \{\sqrt[3]{2}, \zeta\sqrt[3]{2}, \zeta^2\sqrt[3]{2}\} \quad \text{mit} \quad \zeta \;:=\; e^{2\pi i/3} \;\in\; \mathbb{C},$$

und diese Operation ist treu, da der Zerfällungskörper von der Nullstellenmenge erzeugt wird. Wenn wir die drei Nullstellen numerieren, so können wir $\mathrm{Gal}(L/K)$ also auffassen als eine Untergruppe von $\mathfrak{S}_3$. Insbesondere erhalten wir für den Grad der Erweiterung

$$[L:\mathbb{Q}] \;=\; |\mathrm{Gal}(L/K)| \quad \text{ ist ein Teiler von } \quad |\mathfrak{S}_3| \;=\; 6.$$

Andererseits kann der Grad keine Primzahl sein, denn die Erweiterung besitzt nach Beispiel 4.5 den echten Zwischenkörper $\mathbb{Q}(\sqrt[3]{2})$. Somit erhalten wir $[L:K] = 6$ und es folgt

$$\mathrm{Gal}(L/K) \;\simeq\; \mathfrak{S}_3,$$

d.h. die Galoisgruppe enthält hier sämtliche Permutationen der Nullstellen.

Beispiel 6.3. Die Erweiterung $L = \mathbb{Q}(\zeta)/K = \mathbb{Q}$ erzeugt von $\zeta = e^{2\pi i/5} \in \mathbb{C}$ ist eine Galoiserweiterung, denn sie ist separabel wegen $\mathrm{char}(K) = 0$, und sie ist normal als Zerfällungskörper von

$$f(x) \;=\; x^5 - 1 \;=\; (x-1)(x^4+x^3+x^2+x+1) \;\in\; K[x].$$

In der angegebenen Faktorisierung ist das Polynom $g(x) = x^4+x^3+x^2+x+1 \in K[x]$ irreduzibel, da $g(x+1)$ ein Eisensteinpolynom ist. Für den Grad der Erweiterung erhalten wir somit

$$[L:K] \;=\; 4.$$

Nach Satz 4.3 operiert $\mathrm{Gal}(L/K)$ frei und transitiv auf der Menge $\mathrm{Hom}_K(L,\overline{K})$; da die Erweiterung L/K schon von der einen Nullstelle ζ erzeugt wird, können wir $\mathrm{Hom}_K(L,\overline{K})$ identifizieren mit der Menge der Nullstellen des Polynoms $g(x)$ und erhalten somit im Gegensatz zum vorigen Beispiel 6.2 nicht nur eine treue, sondern sogar eine freie Operation auf dieser Nullstellenmenge. Wir haben also eine Bijektion von Mengen

$$\mathrm{Gal}(L/K) \;\xrightarrow{\sim}\; \big\{\, a \in \mathbb{C} \mid g(a) = 0 \,\big\} \;=\; \big\{\, \zeta, \zeta^2, \zeta^3, \zeta^4 \,\big\} \;\subseteq\; \mathbb{C}, \quad \tau \;\mapsto\; \tau(\zeta).$$

und es bleibt nur die Gruppenstruktur zu klären. Der Automorphismus $\tau \in \mathrm{Gal}(L/K)$ mit $\tau(\zeta) = \zeta^2$ erfüllt $\tau \circ \tau \neq id$, denn

$$\tau\big(\tau(\zeta)\big) \;=\; \tau(\zeta^2) \;=\; \big(\tau(\zeta)\big)^2 \;=\; \big(\zeta^2\big)^2 \;=\; \zeta^4 \;\neq\; \zeta$$

Wegen $|\mathrm{Gal}(L/K)| = 4$ ist somit die Galoisgruppe $\mathrm{Gal}(L/K) = \langle\tau\rangle \simeq \mathbb{Z}/4\mathbb{Z}$.

Die einfachsten Beispiele von Galoiserweiterungen in Charakteristik > 0 liefern die endlichen Körper, die wir bei dieser Gelegenheit klassifizieren wollen. Jeder endliche Körper K mit $p = \mathrm{char}(K) > 0$ ist eine endliche Erweiterung von $\mathbb{F}_p$, es gilt daher

$$|K| \;=\; p^n \quad \text{für} \quad n \;:=\; [K:\mathbb{F}_p].$$

Jeden solchen endlichen Körper können wir als algebraische Erweiterung von $\mathbb{F}_p$ einbetten in einen fest gewählten algebraischen Abschluß $\overline{\mathbb{F}}_p/\mathbb{F}_p$, der folgende Satz beschreibt also alle endlichen Körper:

Satz 6.4. *Sei $\overline{\mathbb{F}}_p/\mathbb{F}_p$ ein algebraischer Abschluß.*

a) Für jedes $n \in \mathbb{N}$ gibt es genau einen Teilkörper $\mathbb{F}_{p^n} \subset \overline{\mathbb{F}}_p$ mit $[\mathbb{F}_{p^n} : \mathbb{F}_p] = n$.

b) Für $m,n \in \mathbb{N}$ ist $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$ genau dann, wenn $m \mid n$ ist. Dann ist $\mathbb{F}_{p^n}/\mathbb{F}_{p^m}$ eine Galoiserweiterung, und

$$\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_{p^m}) \;\simeq\; \mathbb{Z}/k\mathbb{Z} \quad \textit{mit} \quad k \;=\; \frac{n}{m}$$

ist zyklisch, erzeugt von dem Automorphismus $\mathrm{Frob}_{p^m} : \mathbb{F}_{p^n} \longrightarrow \mathbb{F}_{p^n}, a \mapsto a^{p^m}$.

Beweis. Wenn K ein Körper mit $|K| = p^n$ Elementen ist, gilt $a^{p^n} = a$ für alle $a \in K$ nach dem kleinen Satz von Fermat. Wenn wir den Körper als Teilkörper von $\overline{\mathbb{F}}_p$ einbetten, ist also $K \subseteq Z(f_n)$ für die Nullstellenmenge

$$Z(f_n) := \{a \in \overline{\mathbb{F}}_p \mid f_n(x) = 0\} \quad \text{des Polynoms} \quad f_n(x) = x^{p^n} - x \in \mathbb{F}_p[x].$$

Dann gilt insbesondere

$$p^n = |K| \leq |Z(f_n)| \leq \deg(f_n) = p^n$$

und somit $K = Z(f_n)$, was die Eindeutigkeitsaussage in $a)$ zeigt. Für die Existenz müssen wir uns überlegen, dass für jedes $n \in \mathbb{N}$ die Nullstellenmenge $Z(f_n) \subset \overline{\mathbb{F}}_p$ ein Teilkörper ist. Da endliche Integritätsringe automatisch Körper sind, genügt es zu zeigen, dass die Nullstellenmenge ein Teilring ist. Die Abgeschlossenheit unter der Multiplikation folgt aus

$$f_n(ab) = (ab)^{p^n} - ab = a^{p^n} \cdot (b^{p^n} - b) + (a^{p^n} - a) \cdot b,$$

die unter der Addition aus

$$(a+b)^{p^n} = \mathrm{Frob}_{p^n}(a+b) = \mathrm{Frob}_{p^n}(a) + \mathrm{Frob}_{p^n}(b) = a^{p^n} + b^{p^n}$$

weil $\mathrm{Frob}_{p^n} = (\mathrm{Frob}_p)^n$ für Körper der Charakteristik $p > 0$ ein Homomorphismus ist. Damit ist gezeigt, dass es für jedes $n \in \mathbb{N}$ genau einen Teilkörper $\mathbb{F}_{p^n} \subset \overline{\mathbb{F}}_p$ vom Grad n über $\mathbb{F}_p$ gibt, nämlich

$$\mathbb{F}_{p^n} := Z(f_n) = \{\, a \in \overline{\mathbb{F}}_p \mid \mathrm{Frob}_{p^n}(a) = a \,\} \subset \overline{\mathbb{F}}_p.$$

Wir nennen diesen auch den *Fixkörper* des Automorphismus $\mathrm{Frob}_{p^n} : \overline{\mathbb{F}}_p \longrightarrow \overline{\mathbb{F}}_p$.

Für die Aussagen in $b)$ seien nun $m, n \in \mathbb{N}$ gegeben. Wenn $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$ gilt, dann ist insbesondere

$$n = [\mathbb{F}_{p^n} : \mathbb{F}_p] = [\mathbb{F}_{p^n} : \mathbb{F}_{p^m}] \cdot [\mathbb{F}_{p^m} : \mathbb{F}_p] = [\mathbb{F}_{p^n} : \mathbb{F}_{p^m}] \cdot m$$

und somit $m \mid n$. Ist umgekehrt letzteres der Fall, etwa $n = mk$ mit $k \in \mathbb{N}$, so berechnet man

$$\mathrm{Frob}_{p^n}(a) = a^{p^n} = (a^{p^m})^{p^{m(k-1)}} = \cdots = (\mathrm{Frob}_{p^m} \circ \cdots \circ \mathrm{Frob}_{p^m})(a)$$

und somit folgt für die Fixkörper

$$\mathbb{F}_{p^m} = \{a \in \overline{\mathbb{F}}_p \mid \mathrm{Frob}_{p^m}(a) = a\} \subseteq \{a \in \overline{\mathbb{F}}_p \mid \mathrm{Frob}_{p^n}(a) = a\} = \mathbb{F}_{p^n}$$

wie behauptet. In diesem Fall gilt zudem

$$\mathrm{Frob}_{p^m} \in \mathrm{Aut}(\mathbb{F}_{p^n}/\mathbb{F}_{p^m}),$$

denn $\mathrm{Frob}_{p^m} : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ ist ein Homomorphismus und $\mathrm{Frob}_{p^m}(a) = a$ für $a \in \mathbb{F}_{p^m}$ nach unserer Charakterisierung als Fixkörper. Für die Potenzen des Frobenius zeigt unsere obige Rechnung, dass $(\mathrm{Frob}_{p^m})^l = \mathrm{Frob}_{p^{ml}}$ für $l \in \mathbb{N}$ gilt. Im Fall $n = mk$ gilt also:

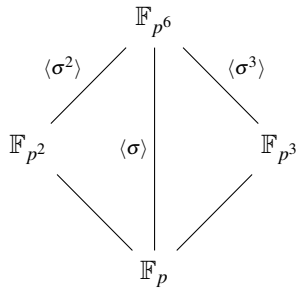
$$(\mathrm{Frob}_{p^m})^l \;=\; 1 \;\in\; \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_{p^m}) \quad\Longleftrightarrow\quad l \;\in\; k\mathbb{Z}.$$

Folglich ist $\mathrm{Frob}_{p^m} \in \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_{p^m})$ ein Gruppenelement der Ordnung k. Also muß in der Ungleichung

$$|\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_{p^m})| \;\leq\; [\mathbb{F}_{p^n} : \mathbb{F}_{p^m}] \;=\; \frac{[\mathbb{F}_{p^n} : \mathbb{F}_p]}{[\mathbb{F}_{p^m} : \mathbb{F}_p]} \;=\; \frac{n}{m} \;=\; k.$$

Gleichheit gelten. Damit ist $\mathbb{F}_{p^n}/\mathbb{F}_{p^m}$ eine Galoiserweiterung und ihre Galoisgruppe wird von Frob_{p^m} erzeugt. □

Man beachte, dass beispielsweise $\mathbb{F}_{p^2}$ kein Teilkörper von $\mathbb{F}_{p^3}$ ist. Das folgende Hassediagramm verdeutlicht die Inklusionsrelationen zwischen den Teilkörpern des endlichen Körpers $\mathbb{F}_{p^6}$. Die neben den Inklusionen angegebenen Gruppen stehen für die jeweiligen Galoisgruppen, wobei wir $\sigma = \mathrm{Frob}_p \in \mathrm{Gal}(\mathbb{F}_{p^6}/\mathbb{F}_p)$ setzen:



Die obige Diskussion von endlichen Körpern zeigt, dass für die Beschreibung von Zwischenkörpern einer Galoiserweiterung die Fixkörper von Untergruppen ihrer Galoisgruppe eine wichtige Rolle spielen:

Definition 6.5. Sei L/K eine Körpererweiterung. Für Untergruppen $H \leq \mathrm{Aut}(L/K)$ bezeichnen wir

$$L^H \;:=\; \{a \in L \mid \forall h \in H :\; h(a) = a\} \;\subseteq\; L$$

als *Fixkörper* der Untergruppe. Es gilt:

- $K \subseteq L^H$ wegen $\sigma|_K = id$ für alle $\sigma \in \mathrm{Aut}(L/K)$.
- $L^H \subseteq L$ ist ein Teilkörper, denn für $a, b \in L^H$ und alle $\sigma \in \mathrm{Aut}(L/K)$ ist

$$\begin{aligned} \sigma(a-b) \;&=\; \sigma(a) \;-\; \sigma(b) \;=\; a-b \\ \sigma(a \cdot b^{-1}) \;&=\; \sigma(a) \cdot \sigma(b)^{-1} \;=\; ab^{-1} \end{aligned}$$

  und somit $a-b \in L^H$ und $ab^{-1} \in L^H$ wie für einen Teilkörper gefordert.

Somit ist $M := L^H$ ein Zwischenkörper von L/K. Für die Automorphismengruppen ist per Definition

$$\begin{aligned} \mathrm{Aut}(L/M) &= \{\sigma \in \mathrm{Aut}(L) \mid \sigma|_M = id\} \\ &= \{\sigma \in \mathrm{Aut}(L/K) \mid \sigma|_M = id\} \leq \mathrm{Aut}(L/K) \end{aligned}$$

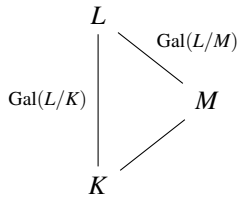
Zudem gilt für Zwischenkörper:

$$\begin{aligned} L/K \text{ normal} &\implies L/M \text{ normal} \\ L/K \text{ separabel} &\iff L/M \text{ und } M/K \text{ separabel} \end{aligned}$$

Falls L/K eine Galoiserweiterung ist, dann auch L/M, und ihre Galoisgruppe ist eine Untergruppe

$$\mathrm{Gal}(L/M) \leq \mathrm{Gal}(L/K).$$

Man beachte, dass wir hierbei nur die obere der beiden Teilerweiterungen in dem Diagramm



betrachten, im Allgemeinen muß die untere Teilerweiterung M/K nicht normal und somit keine Galoiserweiterung sein. Genauer gilt:

Satz 6.6 (Hauptsatz der Galoistheorie). *Sei L/K eine endliche Galoiserweiterung.*

a) Die Abbildung

$$\{\text{Untergruppen von } \mathrm{Gal}(L/K)\} \xrightarrow{H \mapsto L^H} \{\text{Zwischenkörper von } L/K\}$$

ist eine inklusionsumkehrende Bijektion mit inverser Abbildung $M \mapsto \mathrm{Gal}(L/M)$.

b) Für $M = L^H$ sind dabei äquivalent:

- *Die Körpererweiterung M/K ist normal.*
- *Es ist $H = \mathrm{Gal}(L/M) \trianglelefteq \mathrm{Gal}(L/K)$ ein Normalteiler.*

Wenn diese Bedingungen gelten, ist $\mathrm{Gal}(M/K) \simeq \mathrm{Gal}(L/K)/\mathrm{Gal}(L/M)$.

Beweis. *a*) Dass die beiden angegebenen Abbildungen wohldefiniert sind, haben wir schon gesehen. Zudem ist klar, dass die Abbildungen inklusionsumkehrend sind in dem folgenden Sinn:

$$L^{H_1} \subseteq L^{H_2} \quad \text{für } H_2 \subseteq H_1$$
$$\mathrm{Gal}(L/M_1) \subseteq \mathrm{Gal}(L/M_2) \quad \text{für } M_2 \subseteq M_1$$

Wir müssen zeigen:

i) Es ist $M = L^{\mathrm{Gal}(L/M)}$ für jeden Zwischenkörper M von L/K.

ii) Es ist $H = \mathrm{Gal}(L/L^H)$ für jede Untergruppe $H \leq \mathrm{Gal}(L/K)$.

Für die Aussage i) sei M ein beliebiger Zwischenkörper von L/K. Per Definition gilt dann

$$M \subseteq L^H \quad \text{für die Untergruppe} \quad H := \mathrm{Gal}(L/M) \leq \mathrm{Gal}(L/K).$$

Wir müssen zeigen, dass in dieser Inklusion sogar die Gleichheit $M = L^H$ gilt. Wenn dies nicht der Fall wäre, gäbe es ein $a \in L^H$ mit $a \notin M$. Wir hätten dann eine echte Inklusion

$$M \subsetneq M(a) \subseteq L^H$$

Da L/M als Galoiserweiterung insbesondere separabel ist, gilt dasselbe für $M(a)/M$, somit folgt

$$|\mathrm{Hom}_M(M(a), \overline{L})| > 1$$

durch Betrachten von zwei verschiedenen Nullstellen des Minimalpolynoms von a über K. Durch Fortsetzen von Einbettungen zum algebraischen Abschluß erhalten wir somit einen Automorphismus

$$\overline{\sigma} \in \mathrm{Aut}(\overline{L}/M) \quad \text{mit} \quad \overline{\sigma}(a) \neq a.$$

Da L/M als Galoiserweiterung auch normal ist, gilt $\tau(L) = L$. Wir erhalten somit durch Einschränken

$$\sigma := \overline{\sigma}|_L \in \mathrm{Gal}(L/M) = H \quad \text{mit} \quad \sigma(a) \neq a$$

im Widerspruch dazu, dass $a \in L^H$ im Fixkörper von H liegt. Damit ist i) gezeigt.

Für die Aussage ii) sei eine beliebige Untergruppe $H \leq \mathrm{Gal}(L/K)$ gegeben. Per Definition gilt

$$H \subseteq \mathrm{Gal}(L/M) \quad \text{für den Fixkörper} \quad M := L^H \subseteq L.$$

Wir müssen zeigen, dass in dieser Inklusion sogar die Gleichheit $H = \mathrm{Gal}(L/M)$ gilt. Da L/M eine endliche Galoiserweiterung und als solche insbesondere separabel ist, existiert nach dem Satz vom primitiven Element ein $a \in L$ mit $L = M(a)$. Wir schreiben den Orbit von a unter der Operation von H in der Form

$$H \cdot a \;=\; \{a_1,\ldots,a_n\} \quad \text{mit paarweise verschiedenen} \quad a_1,\ldots,a_n \;\in\; L.$$

Dann ist

$$f(x) \;:=\; \prod_{i=1}^{n}(x-a_i) \;\in\; \big(L[x]\big)^H \;=\; L^H[x] \;=\; M[x].$$

Wir erhalten somit

$$\begin{aligned}
[L:M] \;&\leq\; \deg(f) && \text{wegen } L = M(a) \text{ und } f(a) = 0\\
&\leq\; |H| && \text{da } H \text{ transitiv auf } \deg(f) \text{ Punkten operiert}\\
&\leq\; |\mathrm{Gal}(L/M)| && \text{wegen } H \subseteq \mathrm{Gal}(L/M)\\
&=\; [L:M] && \text{weil } L/M \text{ eine Galoiserweiterung ist.}
\end{aligned}$$

Also muß Gleichheit gelten, es ist also $H = \mathrm{Gal}(L/M)$ und somit gilt ii).

Um die Äquivalenz der Aussagen zur Normalität in $b)$ zu sehen, betrachten wir die Operation von $\mathrm{Gal}(L/K)$ auf der Menge ihrer Untergruppen durch Konjugation und auf der Menge der Zwischenkörper durch Automorphismen, d.h. $\sigma \in \mathrm{Gal}(L/K)$ operiere durch

- $H \mapsto \sigma H \sigma^{-1}$ auf der Menge der Untergruppen H von $\mathrm{Gal}(L/K)$,
- $M \mapsto \sigma(M)$ auf der Menge der Zwischenkörper M von L/K.

Man prüft sofort nach, dass diese beiden Operationen miteinander kompatibel sind in dem Sinn, dass

$$L^{\sigma H \sigma^{-1}} \;=\; \sigma(L^H)$$

gilt. Da die Fixpunkte der Operation die Normalteiler bzw. die über K normalen Zwischenkörper sind, folgt:

$$H \trianglelefteq \mathrm{Gal}(L/K) \text{ ist ein Normalteiler} \quad\Longleftrightarrow\quad \text{Die Erweiterung } L^H/K \text{ ist normal}$$

Wenn die Bedingung auf der rechten Seite erfüllt sind, gilt zudem $\sigma(L^H) = L^H$ für alle $\sigma \in \mathrm{Gal}(L/K)$. Durch Einschränken erhalten wir dann einen wohldefinierten Homomorphismus

$$\mathrm{Gal}(L/K) \;\longrightarrow\; \mathrm{Gal}(L^H/K), \quad \sigma \;\mapsto\; \sigma|_{L^H}$$

von Gruppen. Dieser ist surjektiv wegen der Fortsetzbarkeit von Automorphismen, und sein Kern ist per Definition genau die Untergruppe $\mathrm{Gal}(L/L^H) \trianglelefteq \mathrm{Gal}(L/K)$. □

Beispiel 6.7. Sei $L/K = \mathbb{Q}$ ein Zerfällungskörper von $f(x) = x^3 - 2$. In Beispiel 6.2 haben wir gesehen, dass

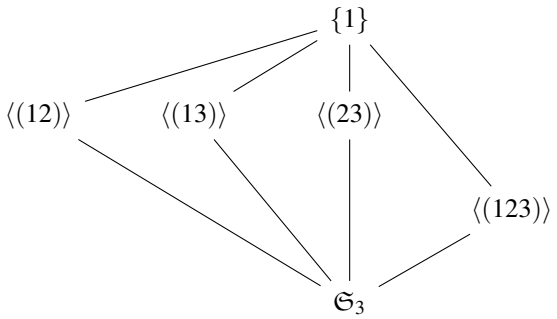
$$\mathrm{Gal}(L/K) \;\simeq\; \mathfrak{S}_3$$

ist, wobei die symmetrische Gruppe durch Permutation der drei Nullstellen von $f(x)$ operiert. Um einen expliziten Isomorphismus zwischen der Galoisgruppe und der

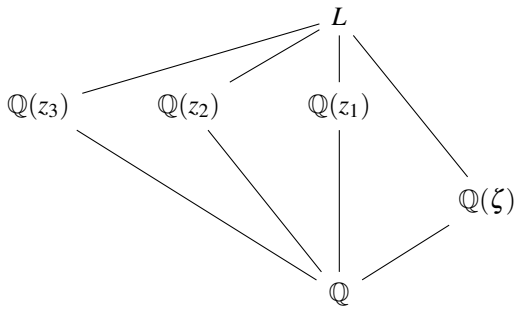
symmetrischen Gruppe hinzuschreiben, müssen wir die Nullstellen numerieren. Sei etwa

$$z_1 = \sqrt[3]{2}, \quad z_2 = \zeta\sqrt[3]{2} \quad \text{und} \quad z_3 = \zeta^2\sqrt[3]{2} \quad \text{mit} \quad \zeta = e^{2\pi i/3} \in \mathbb{C}$$

dann entspricht in dieser Numerierung die komplexe Konjugation $\sigma \in \mathrm{Gal}(L/K)$ der Transposition $\sigma = (23) \in \mathfrak{S}_3$ usw. Wir können nun sämtliche Zwischenkörper von L/K bestimmen als Fixkörper von Untergruppen von $\mathfrak{S}_3$. In der Galoistheorie schreibt man Hassediagramme von Gruppen gern so, dass für jede Inklusion die jeweils *kleinere* Gruppe weiter oben steht:



Im entsprechenden Hassediagramm von Teilkörpern steht dann für jede Inklusion den jeweils *größere* Körper weiter oben. In unserem Fall sieht das Diagramm so aus und wir haben damit alle Teilkörper von L gefunden:



7 Kreisteilungskörper und Konstruierbarkeit

Wir wollen noch einige einfache Anwendungen der Galoistheorie betrachten. Die Frage nach der Konstruierbarkeit von Punkten mit Zirkel und Lineal lässt sich wie folgt beantworten:

Satz 7.1. *Sei $S \subset \mathbb{C}$ eine unter der komplexen Konjugation abgeschlossene Menge komplexer Zahlen. Für $a \in \mathbb{C}$ sind dann äquivalent:*

a) Der Punkt a lässt sich aus S mit Zirkel und Lineal konstruieren.

b) Der Punkt a ist enthalten in einer Galoiserweiterung L/K des Körpers $K = \mathbb{Q}(S)$ vom Grad

$$[L:K] \;=\; 2^n \quad \textit{für ein } n \in \mathbb{N}.$$

Beweis. Vom Beginn der Vorlesung wissen wir, dass eine Zahl $a \in \mathbb{C}$ sich aus der Menge S mit Zirkel und Lineal konstruieren lässt genau dann, wenn $a \in K_m$ ist für eine Kette

$$K_0 \;:=\; K \;=\; \mathbb{Q}(S) \;\subseteq\; K_1 \;\subseteq\; K_2 \;\subseteq\; \cdots \;\subseteq\; K_m \;\subseteq\; \mathbb{C}$$

von Erweiterungen

$$K_i \;=\; K_{i-1}(a_i) \quad \text{mit } a_i^2 \in K_{i-1} \text{ für } i = 1, \ldots, m.$$

Mit K_n/K erhält man auch die normale Hülle $L \subseteq \mathbb{C}$ von K_n/K durch sukzessive Adjunktion endlich vieler Quadratwurzeln, also gilt

$$[L:K] \;=\; 2^n \quad \text{für ein} \quad n \;\in\; \mathbb{N}.$$

Ist umgekehrt L/K eine beliebige Galoiserweiterung mit $[L:K] = 2^n$ für ein $n \in \mathbb{N}$, dann ist

$$|\mathrm{Gal}(L/K)| \;=\; [L:K] \;=\; 2^n$$

und somit ist $\mathrm{Gal}(L/K)$ eine 2-Gruppe. Als solche ist sie auflösbar und besitzt eine Kompositionsreihe

$$G \;=\; G_0 \;\trianglerighteq\; G_1 \;\trianglerighteq\; G_2 \;\trianglerighteq\; \cdots \;\trianglerighteq\; G_n \;=\; \{1\}$$

mit $G_r/G_{r+1} \simeq \mathbb{Z}/2\mathbb{Z}$ für alle r. Nach dem Hauptsatz der Galoistheorie liefert die zugehörige Kette von Fixkörpern eine Kette quadratischer Körpererweiterungen, was die Konstruierbarkeit von $a \in L$ zeigt. □

Wir wollen das obige Resultat nun auf die Frage nach der Konstruierbarkeit eines regulären n-Ecks anwenden. Dazu wollen wir ausgehend von der Menge $S = \{0, 1\}$ die Einheitswurzel

$$\zeta_n \;=\; e^{2\pi i/n} \;\in\; \mathbb{C}$$

konstruieren. Diese ist eine sogenannte *primitive n-te Wurzel*, also ein Erzeuger der Gruppe

$$\mu_n(\mathbb{C}) \;=\; \{z \in \mathbb{C} \mid z^n = 1\} \;=\; \{(\zeta_n)^a \mid a \in \mathbb{Z}\} \;\simeq\; \mathbb{Z}/n\mathbb{Z}.$$

Der Körper $L = \mathbb{Q}(\zeta_n)$ ist folglich ein Zerfällungskörper von $f(x) = x^n - 1 \in \mathbb{Q}[x]$, wir erhalten also eine Galoiserweiterung $L/\mathbb{Q}$. Um den Grad dieser Erweiterung zu bestimmen, müssen wir das Minimalpolynom einer primitiven n-ten Wurzel ζ_n über $\mathbb{Q}$ finden. Wir beginnen mit der folgenden Faktorisierung:

Bemerkung 7.2. Es ist

$$\begin{aligned} x^n - 1 &= \prod_{k=1}^{n} \left(x - e^{\frac{2\pi i k}{n}} \right) \\ &= \prod_{d \mid n} \Phi_d(x) \quad \text{mit} \quad \Phi_d(x) := \prod_{\substack{1 \le c \le d \\ \mathrm{ggT}(c,d)=1}} \left(1 - e^{\frac{2\pi i c}{d}} \right) \in \mathbb{Z}[x]. \end{aligned}$$

Beweis. Die erste Gleichung folgt daraus, dass das Polynom $f(x) = x^n - 1$ normiert ist und die n Nullstellen $e^{2\pi i k/n}$ für $k = 1, \ldots, n$ besitzt, die paarweise verschieden sind. Die zweite Gleichung wird klar, indem man die Indizes $k \in \{1, \ldots, n\}$ schreibt als $k = cf$ mit $f = \mathrm{ggT}(k,n)$ und $d = n/f$ setzt. Um zu sehen, dass $\Phi_d(x) \in \mathbb{Q}[x]$ ist, beachte man zunächst

$$\left\{ z \in \mathbb{C} \mid \Phi_d(z) = 0 \right\} = \left\{ z \in \mathbb{C}^\times \mid \mathrm{ord}(z) = d \right\},$$

wobei $\mathrm{ord}(z)$ die Ordnung von z in der multiplikativen Gruppe $\mathbb{C}^\times$ bezeichne. Die Menge der Nullstellen des Polynoms $\Phi_d(x)$ ist daher invariant unter der Operation von $G = \mathrm{Gal}(L/\mathbb{Q})$. Da das Polynom zudem normiert ist, operiert die Gruppe G somit trivial auf den Koeffizienten dieses Polynoms, alle diese Koeffizienten liegen also bereits im Fixkörper $L^G = \mathbb{Q}$. Dann liegen sie in $\mathbb{Z}$ nach dem Lemma von Gauß, denn $\Phi_d(x)$ ist ein normierter Teiler des normierten Polynoms $x^n - 1 \in \mathbb{Z}[x]$. □

Man nennt $\Phi_d(x) \in \mathbb{Q}[x]$ das *d-te Kreisteilungspolynom*. Für Primzahlen p gilt offenbar

$$\begin{aligned} \Phi_p(x) &= \frac{x^p - 1}{x - 1} \\ &= x^{p-1} + x^{p-2} + \cdots + x^2 + x + 1. \end{aligned}$$

Allgemein lassen sich die Kreisteilungspolynome rekursiv berechnen mithilfe der Identität

$$\Phi_n(x) = \frac{x^n - 1}{\prod_{\substack{d \mid n \\ d < n}} \Phi_d(x)},$$

beispielsweise gilt

$$\begin{aligned} \Phi_{21}(x) &= \frac{x^{21} - 1}{\Phi_1(x)\Phi_3(x)\Phi_7(x)} \\ &= \frac{x^{21} - 1}{(x-1)(x^2 + x + 1)(x^6 + x^5 + \cdots + x + 1)} \\ &= x^{12} - x^{11} + x^9 - x^8 + x^6 - x^4 + x^3 - x + 1. \end{aligned}$$

Per Definition ist die primitive n-te Einheitswurzel $\zeta_n = e^{2\pi i/n}$ eine Nullstelle des Kreisteilungspolynoms $\Phi_n(x)$. Tatsächlich haben wir damit ihr Minimalpolynom gefunden:

Proposition 7.3. *Für jedes $n \in \mathbb{N}$ ist das Polynom $\Phi_n(x) \in \mathbb{Q}[x]$ irreduzibel.*

Beweis. Sei $f(x) \in \mathbb{Z}[x]$ das Minimalpolynom von ζ_n. Dann ist f ein Teiler von Φ_n und somit

$$Z(f) := \{z \in \mathbb{C} \mid f(z) = 0\} \subseteq Z(\Phi_n) = \{(\zeta_n)^k \mid k \in \mathbb{Z}, \mathrm{ggT}(k,n) = 1\}.$$

Da Kreisteilungspolynome per Konstruktion nur einfache Nullstellen haben, reicht es zu zeigen, dass die obige Inklusion der Nullstellenmengen eine Gleichheit ist. Es genügt daher zu zeigen, dass die Menge $Z(f)$ stabil unter der Abbildung $z \mapsto z^k$ ist für alle $k \in \mathbb{Z}$ mit $\mathrm{ggT}(k,n) = 1$. Durch Betrachten der Primfaktorzerlegung von k reduziert man dies auf den Fall, dass $k = p$ eine Primzahl ist. Wir müssen also für $a \in \mathbb{C}$ zeigen:

$$f(a) = 0 \quad \Longrightarrow \quad f(a^p) = 0 \text{ für alle Primzahlen } p \nmid n.$$

Um dies zu sehen, schreiben wir $\Phi_n(x) = f(x)g(x)$ mit $g(x) \in \mathbb{Z}[x]$. Sei $p \nmid n$ prim und $a \in Z(f)$. Für $a^p \notin Z(f)$ gilt

$$f(a^p) \neq 0 \quad \Longrightarrow \quad f(x) \nmid f(x^p).$$

Wegen $\Phi_n(x^p) = f(x^p)g(x^p)$ und der Irreduzibilität des Polynoms $f(x) \in \mathbb{Z}[x]$ folgt dann

$$f(x) \mid g(x^p).$$

Für die Reduktion $\overline{f}(x), \overline{g}(x) \in \mathbb{F}_p[x]$ der obigen Polynome modulo p erhielten wir dann

$$\overline{f}(x) \mid \overline{g}(x^p) = (\overline{g}(x))^p \quad \text{in} \quad \mathbb{F}_p[x]$$

wobei wir benutzen, dass der Frobeniushomomorphismus auf den Koeffizienten der Polynome in $\mathbb{F}_p[x]$ trivial operiert. Dann würde

$$\overline{f}(x)^{p+1} \mid (\overline{f}(x))^p(\overline{g}(x))^p = (\overline{f}(x)\overline{g}(x))^p = (\overline{\Phi}_n(x))^p$$

folgen. Jede Nullstelle von $\overline{f}(x) \in \mathbb{F}_p[x]$ im algebraischen Abschluß von $\mathbb{F}_p$ wäre dann eine mehrfache Nullstelle von

$$\overline{\Phi}_n(x) = \frac{x^n - 1}{\prod_{\substack{d|n \\ d<n}} \overline{\Phi}_d(x)} \in \mathbb{F}_p[x].$$

Dies steht jedoch im Widerspruch dazu, dass das Polynom $h(x) = x^n - 1 \in \mathbb{F}_p[x]$ für $p \nmid n$ wegen $h'(x) = nx^{n-1}$ nur einfache Nullstellen hat. □

Korollar 7.4. *Für $L = \mathbb{Q}(\zeta_n)$ gilt* $\mathrm{Gal}(L/\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$.

Beweis. Nach Proposition 7.3 haben wir für die Galoiserweiterung $L = \mathbb{Q}(\zeta_n)/\mathbb{Q}$ eine Bijektion

$$\mathrm{Gal}(L/\mathbb{Q}) \xrightarrow{\sim} Z(\Phi_n) = \{\zeta_n^a \in \mathbb{Z}/n\mathbb{Z} \mid \mathrm{ggT}(a,n) = 1\}, \quad \sigma \mapsto \sigma(\zeta_n).$$

von Mengen. Wir schreiben diese als

$$h: \quad \mathrm{Gal}(L/\mathbb{Q}) \xrightarrow{\sim} (\mathbb{Z}/n\mathbb{Z})^\times \quad \text{mit} \quad h(\sigma) = a \quad \text{für} \quad \sigma(\zeta_n) = \zeta_n^a,$$

und erhalten damit sogar einen Isomorphismus von Gruppen: Für $\sigma, \tau \in \mathrm{Gal}(L/\mathbb{Q})$ mit $h(\sigma) = a$, $h(\tau) = b$ ist

$$(\sigma \circ \tau)(\zeta_n) = \sigma(\tau(\zeta_n)) = \sigma(\zeta_n^b) = (\sigma(\zeta_n))^b = (\zeta^a)^b = \zeta^{ab}$$

und somit wie gewünscht $h(\sigma \circ \tau) = ab = h(\sigma)h(\tau)$. □

Insbesondere ist der Grad der Galoiserweiterung $L = \mathbb{Q}(\zeta_n)/\mathbb{Q}$ gegeben durch die Funktion

$$\begin{aligned} \varphi: \quad \mathbb{N} \longrightarrow \mathbb{N}, \quad \varphi(n) &:= |(\mathbb{Z}/n\mathbb{Z})^\times| \\ &= |\{a \in \{1,\dots,n\} \mid \mathrm{ggT}(a,n) = 1\}| \end{aligned}$$

die man auch als *Eulersche φ-Funktion* bezeichnet. Die Werte dieser Funktion kann man leicht aus den folgenden beiden elementaren Beobachtungen berechnen:

- Für $a, b \in \mathbb{N}$ teilerfremd ist $\varphi(ab) = \varphi(a)\varphi(b)$.
- Für p prim und $e \in \mathbb{N}$ ist $\varphi(p^e) = p^{e-1}(p-1)$.

Hieraus erhält man den zu Beginn der Vorlesung erwähnten Satz von Gauss:

Korollar 7.5. *Das reguläre n-Eck ist mit Zirkel und Lineal konstruierbar genau dann, wenn*

$$n = 2^k \cdot \prod_{i=1}^{l} F_{m_i}$$

mit $k, l \in \mathbb{N}_0$ und paarweise verschiedenen Fermat-Primzahlen $F_{m_i} = 2^{2^{m_i}} - 1$ ist.

Beweis. Nach Satz 7.1 und Korollar 7.4 ist das reguläre n-Eck konstruierbar genau dann, wenn $\varphi(n)$ eine Zweierpotenz ist. Wegen den obigen Rechenregeln für die Eulersche Funktion ist dies genau dann der Fall, wenn in der Primfaktorzerlegung von n alle eventuell vorkommenden ungeraden Primzahlen von der Form $p = 2^m + 1$ sind und jeweils nur mit Vielfachheit Eins vorkommen. Dabei muß der Exponent m eine Zweierpotenz sein: Für $m = ab$ mit $2 \nmid a$ ist

$$2^m + 1 = (2^b + 1)(2^{(a-1)b} - 2^{(a-2)b} + \cdots + 1)$$

und dann ist $2^m + 1$ nicht prim. □

8 Auflösbarkeit durch Radikale

Wir wollen nun ein galoistheoretisches Kriterium dafür entwickeln, wann sich die Nullstellen eines Polynoms ausgehend von seinen Koeffizienten durch *Radikale* ausdrücken lassen, also nur mit Addition, Subtraktion, Multiplikation, Division und n-ten Wurzeln für $n \in \mathbb{N}$. Dies führt auf die folgenden Begriffe:

Definition 8.1. Eine Körpererweiterung L/K mit $\mathrm{char}(K) = 0$ heißt

a) *Radikalerweiterung*, wenn $L = K(c)$ ist für eine Nullstelle $c \in L$ eines Polynoms von der Form
$$f(x) \;=\; x^n - a \;\in\; K[x].$$

b) *auflösbar durch Radikale*, wenn es eine Kette von Erweiterungen
$$K \;=\; K_0 \;\subseteq\; K_1 \;\subseteq\; \cdots \;\subseteq\; K_m \quad \text{mit} \quad L \;\subseteq\; K_m$$
gibt, sodass jede der Körpererweiterungen K_{i+1}/K_i eine Radikalerweiterung ist.

Man beachte, dass Radikalerweiterungen keine Galoiserweiterungen sein müssen; wenn aber K *alle n-ten Einheitswurzeln enthält* in dem Sinn, dass $\mu_n(K) = \mu_n(\overline{K})$ für einen – und damit jeden – algebraischen Abschluß $\overline{K}/K$ gilt, dann ist für $a \in K$ die Radikalerweiterung
$$L \;=\; K(\sqrt[n]{a})/K$$
eine Galoiserweiterung als Zerfällungskörper des Polynoms $x^n - a \in K[x]$ und hängt nicht ab von der gewählten n-ten Wurzel $\sqrt[n]{a} \in \overline{K}$ (daher die saloppe Notation).

Wir wollen im Folgenden die Radikalerweiterungen und allgemeiner die durch Radikale auflösbaren Erweiterungen durch Galoisgruppen charakterisieren. Dazu verwenden wir folgende Sprechweise:

Definition 8.2. Eine Galoiserweiterung L/K heißt

a) *zyklisch*, wenn $\mathrm{Gal}(L/K)$ zyklisch ist.

b) *auflösbar*, wenn $\mathrm{Gal}(L/K)$ auflösbar ist.

Die Radikalerweiterungen sind im Wesentlichen die zyklischen Erweiterungen, genauer gilt:

Proposition 8.3. *Sei K ein Körper mit $\mathrm{char}(K) \nmid n$, der alle n-ten Einheitswurzeln enthalte. Dann sind die zyklischen Galoiserweiterungen L/K, deren Grad $d = [L:K]$ ein Teiler $d \mid n$ ist, genau die Erweiterungen*
$$L \;=\; K(\sqrt[n]{a}) \quad \textit{mit} \quad a \;\in\; K.$$

Beweis. (a) Sei zunächst $a \in K$ gegeben und sei $c = \sqrt[n]{a} \in \overline{K}$ eine n-te Wurzel in einem algebraischen Abschluß. Wenn K alle n-ten Einheitswurzeln enthält, ist der Körper $K(c) = K(\sqrt[n]{a})$ ein Zerfällungskörper des Polynoms $f(x) = x^n - a$. Dieses

Polynom hat in dem gewählten algebraischen Abschluß genau die Nullstellen $\zeta \cdot c$ mit $\zeta \in \mu_n(K)$. Man beachte, dass $K(c)/K$ wegen $\mathrm{char}(K) \nmid n$ separabel und somit eine Galoiserweiterung ist. Wir erhalten eine Abbildung

$$\mathrm{Gal}(K(c)/K) \hookrightarrow \mu_n(K), \quad \sigma \mapsto \zeta = \frac{\sigma(c)}{c}.$$

Diese ist injektiv, da ein Automorphismus $\sigma \in \mathrm{Gal}(K(c)/K)$ eindeutig durch das Bild $\sigma(c)$ bestimmt ist. Außerdem prüft man sofort nach, dass die Abbildung ein Gruppenhomomorphismus ist. Dabei ist $\mu_n(K)$ wie jede endliche Untergruppe der multiplikativen Gruppe eines Körpers zyklisch. Damit ist $\mathrm{Gal}(K(c)/K))$ zyklisch und $d = [K(c) : K)] = |\mathrm{Gal}(K(c)/K)|$ ist ein Teiler von $|\mu_n(K)| = n$.

(b) Sei umgekehrt eine zyklische Galoiserweiterung L/K vom Grad $d = [L : K] \mid n$ gegeben mit Galoisgruppe

$$G := \mathrm{Gal}(L/K) = \langle \sigma \rangle = \left\{ \sigma^k \mid k = 0, 1, \ldots, d-1 \right\}$$

Wir wollen das Argument in (a) umkehren und wählen dazu zunächst eine beliebige primitive n-te Einheitswurzel $\zeta \in \mu_n(K)$, d.h. einen Erzeuger von $\mu_n(K)$. Wenn wir die Identität

$$\zeta = \frac{\sigma(c)}{c} \quad \text{für ein geeignetes} \quad c \in L^\times \tag{III.3}$$

zeigen können, dann sind wir fertig:

- Es ist $a := c^n \in L^G = K$, denn $\sigma(c^n) = c^n$ wegen $\zeta^n = 1$.
- Somit ist $c = \sqrt[n]{a}$ eine Nullstelle des Polynoms $x^n - a \in K[x]$.
- Für den Zwischenkörper $L' := K(c)$ von L/K gilt dann

$$\begin{aligned} \mathrm{Gal}(L/L') &= \{\tau \in \mathrm{Gal}(L/K) \mid \tau(c) = c\} \\ &= \{\sigma^k \in \mathrm{Gal}(L/K) \mid \sigma^k(c) = c\} \\ &= \{\sigma^k \in \mathrm{Gal}(L/K) \mid \zeta^k = 1\} = \{id_L\}, \end{aligned}$$

  also $L = L'$ nach dem Hauptsatz. Also ist L/K eine Radikalerweiterung.

Wir müssen also nur ein $c \in L^\times$ wie in (III.3) finden. Ein naheliegender Ansatz dazu wäre

$$c = \sum_{k=1}^{n} \zeta^{n-k} \cdot \sigma^k(b) \in L \quad \text{mit} \quad b \in L,$$

denn $\sigma(c) = \zeta \cdot c$ ist dann klar. Wir müssen lediglich $b \in L$ so wählen, dass $c \neq 0$ wird. Das geht, wenn

$$\sum_{k=1}^{n} \zeta^{n-k} \cdot \sigma^k : \quad L^\times \longrightarrow L$$

nicht die Nullabbildung ist. Aber das wird durch das folgende Lemma für $H = L^\times$ und die Charaktere $\sigma^k \in \mathrm{Hom}(H, L^\times)$ garantiert. □

Ein *Charakter* einer Gruppe H ist ein Homomorphismus $\sigma : H \to L^\times$ der Gruppe in die multiplikative Gruppe eines Körpers L. Das punktweise gebildete Produkt zweier Charaktere ist wieder ein Charakter. Im Gegensatz dazu sind punktweise Summen und Vielfache von Charakteren im Allgemeinen keine Charaktere, sondern nur Elemente der Menge

$$\mathrm{Abb}(H,L) \;:=\; \{\text{Abbildungen } f : H \to L\}.$$

Diese Menge bildet allerdings einen Vektorraum über L bezüglich der punktweisen Addition und Skalarmultiplikation von Funktionen. Im Beweis von Proposition 8.3 haben wir die *lineare Unabhängigkeit von Charakteren* benutzt:

Lemma 8.4. *Sei H eine Gruppe, und sei L ein Körper. Dann bildet die Menge der Charaktere*

$$\mathrm{Hom}(H,L^\times) \;\subseteq\; \mathrm{Abb}(H,L)$$

ein über L linear unabhängiges System von Elementen des Vektorraumes $\mathrm{Abb}(H,L)$.

Beweis. Per Definition ist eine Menge von Elementen eines Vektorraumes linear unabhängig, wenn je endlich viele paarweise verschiedene Elemente der Menge es sind. Wenn die Aussage des Lemmas nicht gilt, sei $\{\chi_1,\dots,\chi_n\} \subseteq \mathrm{Hom}(H,L^\times)$ eine linear abhängige Teilmenge mit $n \in \mathbb{N}$ minimal. Es gibt dann eine nichttriviale lineare Relation

$$a_1\chi_1 + \cdots + a_n\chi_n \;=\; 0$$

wobei die $a_i \in L$ wegen der Minimalität alle ungleich Null sind. Da $\chi_{n-1} \neq \chi_n$ ist, existiert ein Element $h_0 \in H$ mit $\chi_{n-1}(h_0) \neq \chi_n(h_0)$. Durch Einsetzen in die obige Relation erhalten wir die Relationen

$$\begin{aligned} a_1\chi_1(h) + \cdots + a_n\chi_n(h) \;&=\; 0, \\ a_1\chi_1(h_0h) + \cdots + a_n\chi_n(h_0h) \;&=\; 0, \end{aligned}$$

für alle $h \in H$. Indem wir die zweite Relation mit $\chi_n(h_0)$ multiplizieren und die dritte Relation davon abziehen, erhalten wir eine neue Relation

$$b_1\chi_1 + \cdots + b_{n-1}\chi_{n-1} \;=\; 0 \quad \text{mit} \quad b_i \;=\; a_i \cdot (\chi_n(h_0) - \chi_i(h_0)).$$

Wegen $b_{n-1} \neq 0$ widerspricht dies der Minimalität von n. □

Kehren wir zurück zur Lösung von Gleichungen durch Radikale. Proposition 8.3 hat Radikalerweiterungen als zyklische Erweiterungen charakterisiert, sofern der Grundkörper genügend Einheitswurzeln enthält. Diese letzte Bedingung kann man erzwingen, indem man zum Kompositum mit einem geeigneten Kreisteilungskörper übergeht. Das *Kompositum* $EF \subseteq L$ von Teilkörpern E und F eines Körpers L ist definiert als der kleinste Teilkörper von L, welcher $E \cup F$ enthält. Das Verhalten von Galoiserweiterungen unter Komposita haben wir in den Übungen studiert; wir können nun das Hauptresultat dieses Abschnitts beweisen, ein Kriterium für die Lösbarkeit von Polynomgleichungen durch Radikale:

Satz 8.5. *Sei F/K eine Galoiserweiterung mit* $\mathrm{char}(K) = 0$. *Dann sind äquivalent:*

a) F/K ist auflösbar durch Radikale.

b) F/K ist auflösbar (d.h. die Galoisgruppe $\mathrm{Gal}(F/K)$ *ist auflösbar).*

Beweis. Sei zunächst F/K auflösbar durch Radikale, es gebe also eine Kette von Radikalerweiterungen

$$K = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_m \subseteq \overline{K} \quad \text{mit} \quad F \subseteq K_m.$$

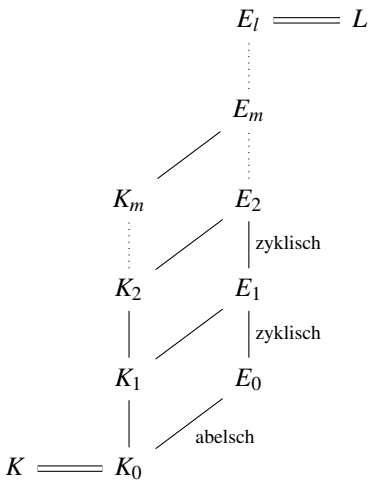
Wir wollen zeigen, dass $\mathrm{Gal}(K_m/K)$ auflösbar ist; dann ist auch $\mathrm{Gal}(F/K)$ auflösbar als Quotient einer auflösbaren Gruppe. Sei $K_{i+1} = K_i(\sqrt[n_i]{a_i})$ mit $a_i \in K_i$ und $n_i \in \mathbb{N}$; wir setzen $n := \mathrm{kgV}(n_1, \ldots, n_m)$ und

$$E := K(\zeta) \quad \text{für eine primitive } n\text{-te Einheitswurzel} \quad \zeta \in \mu_n(\overline{K}).$$

Wir haben dann eine Kette

$$E = E_0 \subseteq E_1 \subseteq \cdots \subseteq E_m = EF \quad \text{für die Komposita} \quad E_i = EK_i \subseteq \overline{K}.$$

Dabei ist $E_{i+1} = E_i(\sqrt[n_i]{a_i})$. Per Konstruktion enthält E_i alle n_i-ten Einheitswurzeln und somit zeigt Proposition 8.3, dass E_{i+1}/E_i eine zyklische Galoiserweiterung ist. Sei L die normale Hülle von E_m/K. Dann können wir auch L/E_m als eine Kette von zyklischen Galoiserweiterungen schreiben (Übungsaufgabe). Wir erhalten ein Hassediagramm der folgenden Form:



Für die Galoisgruppe $G = \mathrm{Gal}(L/K)$ und $G_i = \mathrm{Gal}(L/E_i)$ erhalten wir somit eine Subnormalreihe

$$G \trianglerighteq G_0 \trianglerighteq G_1 \trianglerighteq \cdots \trianglerighteq G_l = \{1\}$$

mit $G_i/G_{i+1} \simeq \mathrm{Gal}(E_{i+1}/E_i)$ abelsch. Also ist G eine auflösbare Gruppe.

Sei nun umgekehrt F/K eine Galoiserweiterung, sodass die Gruppe $\mathrm{Gal}(F/K)$ auflösbar ist. Sei

$$G := \mathrm{Gal}(F/K) \trianglerighteq G_1 \trianglerighteq \cdots \trianglerighteq G_m = \{1\}$$

eine Subnormalreihe mit zyklischen Quotienten $Q_i := G_i/G_{i+1}$. Dann bilden die Fixkörper $K_i := F^{G_i}$ eine aufsteigende Kette

$$K = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_m = F$$

von zyklischen Galoiserweiterungen. Sei $n_i := |Q_i|$ und $n := \mathrm{kgV}(n_1, \ldots, n_m)$. Wir setzen $E = K(\zeta)$ für eine primitive n-te Einheitswurzel $\zeta \in \mu_n(\overline{K})$ und betrachten wie im vorigen Schritt das Diagramm der Komposita $E_i := EK_i$ für $i = 1, \ldots, m$. Nach Proposition 8.3 ist jedes E_i/E_{i-1} eine Radikalerweiterung und somit ist E_m/E_0 durch Radikale auflösbar. Dann gilt dasselbe auch für F/K. □

Die Nullstellen eines Polynoms $f(x) \in K[x]$ lassen sich durch Radikale in den Koeffizienten von $f(x)$ darstellen genau dann, wenn der Zerfällungskörper L/K des Polynoms durch Radikale auflösbar ist. Nach dem obigen Satz ist dies genau dann der Fall, wenn die Gruppe $\mathrm{Gal}(L/K)$ auflösbar ist. Wir können nun leicht Beispiele von Polynomen finden, für welche dies nicht der Fall ist:

Beispiel 8.6. Sei $f(x) = x^5 - 20x + 6 \in \mathbb{Q}[x]$. In den Übungen werden wir zeigen:

- $\mathrm{Gal}(L/\mathbb{Q}) \simeq \mathfrak{S}_5$ für den Zerfällungskörper $L/\mathbb{Q}$ des Polynoms $f(x)$.
- Diese Gruppe ist nicht auflösbar. Daher ist $L/\mathbb{Q}$ nicht auflösbar durch Radikale.
- Die Nullstellen von $f(x)$ lassen sich daher nicht durch Radikale ausdrücken.

Kapitel IV
Ein wenig Funktionentheorie

Zusammenfassung Die komplexe Differenzierbarkeit ist ein viel stärkerer Begriff als sein reelles Analogon. Komplex differenzierbare Funktionen bezeichnet man auch als holomorph. Das Kurvenintegral einer holomorphen Funktion ist nach dem Satz von Cauchy invariant unter Deformationen des Integrationspfads; dies erlaubt es, mit der Cauchyformel die Werte einer holomorphen Funktion im Inneren einer Kreisscheibe durch ihre Werte am Rand darzustellen. Als Folgerung werden wir sehen, dass jede holomorphe Funktion sich lokal als Potenzreihe entwickeln lässt, und wir werden den Residuensatz zur Berechnung von Integralen kennenlernen.

1 Holomorphe Funktionen

Sei $U \subseteq \mathbb{C}$ eine offene Teilmenge. Wir sagen, dass eine Funktion $g : U \setminus \{a\} \longrightarrow \mathbb{C}$ in einem Punkt $a \in U$ gegen einen komplexen Grenzwert $c \in \mathbb{C}$ konvergiert und schreiben

$$c := \lim_{z \to a} g(z) \in \mathbb{C},$$

wenn für alle $\varepsilon > 0$ ein $\delta > 0$ existiert, sodass gilt:

$$|g(z) - c| < \varepsilon \quad \text{für alle} \quad z \in U \setminus \{a\} \quad \text{mit} \quad |z - a| < \delta.$$

Wir definieren nun wie in der reellen Analysis:

Definition 1.1. Eine Funktion $f : U \longrightarrow \mathbb{C}$ auf einer offenen Teilmenge $U \subseteq \mathbb{C}$ heißt in einem Punkt $z \in U$ *komplex differenzierbar* oder *holomorph*, wenn der Grenzwert

$$f'(z) := \lim_{h \to 0} \frac{f(z+h) - f(z)}{h} \in \mathbb{C}$$

existiert. Wir nennen diesen Grenzwert dann die *komplexe Ableitung* von f in z. Die Funktion f heißt *holomorph*, wenn sie in jedem Punkt $z \in U$ holomorph ist.

Beispielsweise ist die Identitätsabbildung $f = id : \mathbb{C} \to \mathbb{C}, z \mapsto z$ holomorph und jede konstante Funktion ist holomorph. Aus diesen beiden Beispielen folgt schon, dass alle Polynomfunktionen und allgemeiner auch alle rationalen Funktionen auf ihrem Definitionsbereich holomorph sind:

Lemma 1.2. *Es gilt:*

a) Die Summe $f+g$ und das Produkt $f \cdot g$ holomorpher Funktionen $f, g : U \to \mathbb{C}$ sind holomorph mit

$$(f+g)'(z) \;=\; f'(z)+g'(z), \quad (f \cdot g)'(z) \;=\; f'(z) \cdot g(z) + f(z) \cdot g'(z).$$

b) Falls $f : U \to \mathbb{C}$ holomorph ist und $f(z) \neq 0$ für alle $z \in U$ gilt, ist auch $1/f$ holomorph mit

$$(1/f)'(z) \;=\; -f'(z)/(f(z))^2$$

c) Für $f : U \to \mathbb{C}$ und $g : V \to \mathbb{C}$ holomorph mit $f(U) \subseteq V$ ist auch $g \circ f : U \to \mathbb{C}$ holomorph mit

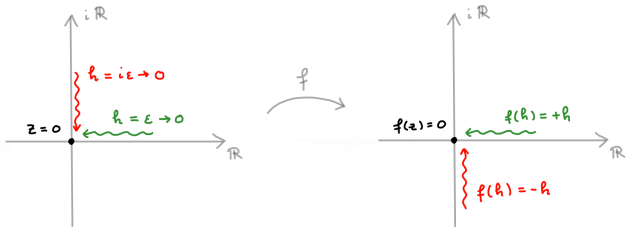
$$(g \circ f)'(z) \;=\; g'(f(z)) \cdot f'(z).$$

Beweis. Wörtlich wie in der reellen Analysis. □

Natürlich hören wir bei Polynomen und rationalen Funktionen nicht auf, wir werden bald viele weitere Beispiele als konvergente Potenzreihen erhalten. Zuvor wollen wir uns aber die Definition der komplexen Differenzierbarkeit etwas genauer ansehen. Man beachte, dass die Existenz des Grenzwertes für $h \to 0$ beinhaltet, dass dieser Grenzwert *unabhängig von der Richtung* sein muß, in der wir uns dem Punkt 0 annähern. Anders als auf der reellen Gerade haben wir in der komplexen Ebene viele Richtungen zur Verfügung:

Beispiel 1.3. Gegeben sei die Funktion $f : \mathbb{C} \to \mathbb{C}, z \mapsto \bar{z}$. Für $z \in \mathbb{C}$ und $h \neq 0$ gilt für den Differenzenquotienten

$$\frac{f(z+h)-f(z)}{h} \;=\; \frac{\mathrm{Re}(h) - i\,\mathrm{Im}(h)}{\mathrm{Re}(h) + i\,\mathrm{Im}(h)} \;=\; \begin{cases} +1 & \text{für } h \in \mathbb{R}, \\ -1 & \text{für } h \in i\mathbb{R}. \end{cases}$$



Der Grenzwert $h \to 0$ existiert also nicht, d.h. die Funktion f ist nicht holomorph.

Auch in der reellen Analysis gibt es einen Begriff der Differenzierbarkeit, der Grenzwerte aus allen Richtungen betrachtet, allerdings für Funktionen in mehreren Variablen: Eine Funktion $f : U \to \mathbb{R}^n$ auf einer offenen Teilmenge $U \subseteq \mathbb{R}^m$ heißt in einem Punkt $x \in U$ *total differenzierbar*, wenn sie lokal durch eine lineare Funktion approximierbar ist in dem Sinn, dass es eine reelle $m \times n$ Matrix $M \in \mathrm{Mat}(m \times n, \mathbb{R})$ gibt mit

$$f(x+h) \;=\; f(x) + M \cdot h + r(h) \quad \text{mit} \quad \lim_{h \to 0} \frac{|r(h)|}{|h|} \;=\; 0.$$

In diesem Fall existieren insbesondere alle partiellen Ableitungen $(\partial f_i/\partial x_j)(x)$, und es ist

$$M \;=\; (Df)(x) \;:=\; \begin{pmatrix} (\partial f_1/\partial x_1)(x) & \cdots & (\partial f_1/\partial x_m)(x) \\ \vdots & & \vdots \\ (\partial f_n/\partial x_1)(x) & \cdots & (\partial f_n/\partial x_m)(x) \end{pmatrix}$$

Wir haben nun zwei Möglichkeiten, zum komplexen Fall überzugehen:

- Wir wählen $m = n = 1$, aber ersetzen $\mathbb{R}$ durch $\mathbb{C}$.
- Wir wählen $m = n = 2$ und nutzen die Identifikation

$$\varphi : \quad \mathbb{R}^2 \;\xrightarrow{\sim}\; \mathbb{C}, \quad (x,y) \;\mapsto\; z \;=\; x + iy,$$

  die wir im Folgenden der Einfachheit halber als Gleichheit $\mathbb{R}^2 = \mathbb{C}$ schreiben.

Die komplexe Differenzierbarkeit bedeutet in diesen beiden Zugängen folgendes:

Satz 1.4. *Sei $U \subseteq \mathbb{C}$ offen und $f : U \to \mathbb{C}$. Für $z \in U$ sind äquivalent:*

a) Die Funktion f ist im Punkt z komplex differenzierbar.

b) Es gibt ein $c \in \mathbb{C}$ mit $f(z+h) = f(z) + c \cdot h + r(h)$ und $\lim_{h\to 0} |r(h)/h| = 0$.

c) Die Funktion f ist im Punkt z total differenzierbar und ihr Differential $(Df)(z)$ ist die Multiplikation mit einer komplexen Zahl $c \in \mathbb{C}$:

$$\begin{array}{ccc} \mathbb{R}^2 & \xrightarrow{(Df)(z)} & \mathbb{R}^2 \\ \| & & \| \\ \mathbb{C} & \xrightarrow{u \mapsto c \cdot u} & \mathbb{C} \end{array}$$

Beweis. Wenn f in z komplex differenzierbar ist, so existiert per Definition der Grenzwert

$$c \;:=\; \lim_{h \to 0} \frac{f(z+h) - f(z)}{h} \;\in\; \mathbb{C}.$$

Für $r(h) := f(z+h) - f(z) - c \cdot h$ folgt

$$\lim_{h \to 0} |r(h)/h| \;=\; \lim_{h \to 0} |(f(z+h) - f(z))/h - c| \;=\; 0,$$

und umgekehrt. Also sind $a)$ und $b)$ äquivalent. Wenn $b)$ gilt, dann ist die Bedingung für die totale Differenzierbarkeit von f erfüllt für die Abbildungsmatrix M zu der linearen Abbildung

$$\mathbb{R}^2 = \mathbb{C} \longrightarrow \mathbb{C} = \mathbb{R}^2, \quad h \mapsto c \cdot h,$$

und diese ist $\mathbb{C}$-linear. Aus $b)$ folgt also $c)$; die Umkehrung sieht man analog. □

Die Bedingung an die Jacobimatrix $(Df)(z)$ in Teil $c)$ lässt sich leicht an ihren Einträgen ablesen: Die Multiplikation mit einer komplexen Zahl $c = a + ib \in \mathbb{C}$ ist gegeben durch

$$z = x + iy \mapsto c \cdot z = (ax - by) + i(ay + bx),$$

also durch die reelle Abbildungsmatrix

$$M = \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \in \mathrm{Mat}(2 \times 2, \mathbb{R}).$$

Die komplexe Differenzierbarkeit einer Funktion läuft damit hinaus auf ein System von zwei Differentialgleichungen für ihre partiellen Ableitungen:

Korollar 1.5. *Sei $U \subseteq \mathbb{C}$ offen. Eine Abbildung $f : U \to \mathbb{C}$ ist in einem Punkt $p \in U$ komplex differenzierbar genau dann, wenn sie dort total differenzierbar ist und für die partiellen Ableitungen der Funktionen $u(x,y) = \mathrm{Re}(f(z))$ und $v(x,y) = \mathrm{Im}(f(z))$ gilt:*

$$\frac{\partial u}{\partial x}(p) = \frac{\partial v}{\partial y}(p), \quad \frac{\partial u}{\partial y}(p) = -\frac{\partial v}{\partial x}(p) \qquad \text{(“Cauchy-Riemannsche DGL”)}$$

Beweis. Nach Satz 1.4 ist die Funktion f komplex differenzierbar im Punkt $p \in U$ genau dann, wenn sie dort total differenzierbar ist und ihre Jacobi-Matrix dort die Gestalt

$$(Df)(p) = \begin{pmatrix} (\partial u/\partial x)(p) & (\partial u/\partial y)(p) \\ (\partial v/\partial x)(p) & (\partial v/\partial x)(p) \end{pmatrix} \stackrel{?}{=} \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \quad \text{für geeignete} \quad a, b \in \mathbb{R}$$

besitzt. Diese letzte Bedingung liefert genau die Cauchy-Riemannschen DGL. □

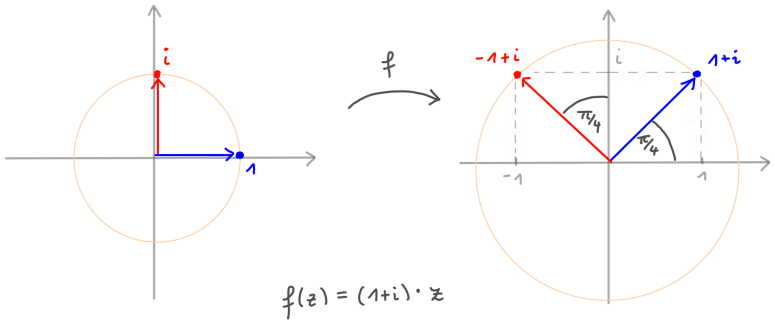
Damit wird klar, warum die komplexe Differenzierbarkeit einer Funktion viel stärker ist als ihre totale Differenzierbarkeit im reellen Sinn: Sie liefert ein System von DGL! Umgekehrt kann man die Cauchy-Riemannschen DGL benutzen, um die komplexe Differenzierbarkeit einer Funktion zu prüfen. Achtung: Dabei muß die totale Differenzierbarkeit bekannt sein, partielle Differenzierbarkeit genügt hierfür nicht. Meist ist das aber kein Problem, z.B. ist jede auf einer offenen Menge *stetig* partiell differenzierbare Funktion dort total differenzierbar.

Bemerkung 1.6. Wir werden später sehen, dass holomorphe Funktionen unendlich oft differenzierbar sind. Also können wir ihre zweiten partiellen Ableitungen bilden und erhalten für $u = \mathrm{Re}(f(z))$ und $v = \mathrm{Im}(f(z))$ aus den Cauchy-Riemannschen DGL die Identität

$$\Delta(u) \;=\; \Delta(v) \;=\; 0 \quad \text{für den Laplace-Operator} \quad \Delta \;:=\; \frac{\partial^2}{\partial x^2} + \frac{\partial^2}{\partial y^2}.$$

Funktionen, die im Kern des Laplace-Operators liegen, nennt man in der reellen Analysis auch *harmonische Funktionen*. Wir können also festhalten: Der Real- und Imaginärteil einer holomorphen Funktion sind harmonische Funktionen.

Geometrisch handelt es sich bei den oben betrachteten Abbildungsmatrizen zur Multiplikation mit einer komplexen Zahl $c = a + ib$ um *Drehstreckungen*, also um lineare Abbildungen der Ebene in sich, die eine Verkettung einer Drehung und einer Streckung mit dem Dehnungsfaktor $r = \sqrt{a^2+b^2} \geq 0$ sind:



Jede von Null verschiedene Drehstreckung ist eine Bijektion, die die Orientierung und Winkel erhält. Man sagt auch, dass holomorphe Funktionen $f : U \to \mathbb{C}$ in jedem Punkt $z \in U$ mit $f'(z) \neq 0$ *lokal winkeltreu* oder *konforme Abbildungen* seien.

Beispiel 1.7. Es gilt:

a) Die komplexe Konjugationsabbildung $f : \mathbb{C} \to \mathbb{C}, z \mapsto \bar{z}$ ist total differenzierbar, aber ihre Jacobimatrix

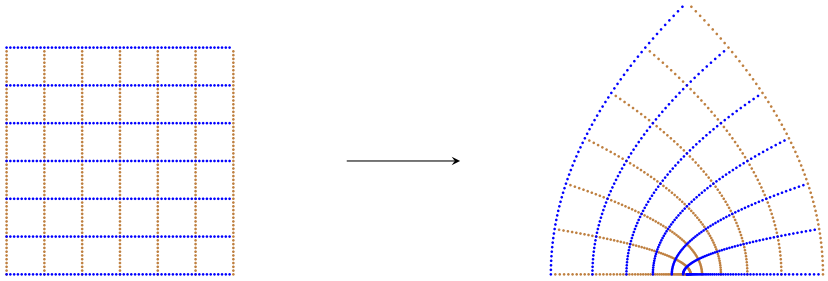
$$(Df)(z) \;=\; \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \;\in\; \mathrm{Mat}(2\times 2, \mathbb{R})$$

beschreibt eine Spiegelung. Das erklärt, warum f nicht holomorph ist.

b) Die Abbildung $f : \mathbb{C} \to \mathbb{C}, z \mapsto z^2$ ist holomorph. Wegen $f'(z) = 2z$ erhalten wir hier

$$(Df)(z) \;=\; 2 \cdot \begin{pmatrix} x & -y \\ y & x \end{pmatrix} \quad \text{für} \quad z \;=\; x + iy.$$

Diese Jacobimatrix ist eine Drehstreckung. Der Drehwinkel und Dehnungsfaktor hängen von z ab. Die folgende Abbildung zeigt die Wirkung von f auf einem rechtwinkligen Gitter im ersten Quadranten:



Das Gitter wird verzerrt, aber in jedem Punkt $z \neq 0$ ist die Abbildung konform, z.B. stehen die Bilder der Gitterlinien noch immer senkrecht aufeinander. Im Punkt $z = 0$ ist die Abbildung natürlich nicht konform.

2 Potenzreihen und analytische Funktionen

Wir wollen uns nun weitere Beispiele holomorpher Funktionen anschauen. Unter einer komplexen Potenzreihe um einen Punkt $z_0 \in \mathbb{C}$ verstehen wir eine Reihe der Form

$$\sum_{n=0}^{\infty} a_n (z - z_0)^n \quad \text{mit Koeffizienten} \quad a_n \in \mathbb{C}$$

Dabei ist z zunächst eine formale Variable, wir werden im konvergenten Fall aber dieselbe Notation auch für konkret einzusetzende Werte verwenden – anders als in der Algebra. Eine Potenzreihe der obigen Form heißt im Punkt $z \in \mathbb{C}$ *konvergent*, wenn der Grenzwert

$$\sum_{n=0}^{\infty} a_n (z - z_0)^n \quad := \quad \lim_{N \to \infty} \sum_{n=0}^{N} a_n (z - z_0)^n \quad \in \quad \mathbb{C}$$

existiert. Die Potenzreihe heißt im Punkt $z \in \mathbb{C}$ *absolut konvergent*, wenn für die Reihe der Beträge

$$\sum_{n=0}^{\infty} |a_n| \, |z - z_0|^n \quad := \quad \lim_{N \to \infty} \sum_{n=0}^{N} |a_n| \, |z - z_0|^n \quad < \quad \infty$$

gilt. Sie heißt *divergent*, wenn sie nicht konvergent ist. Bekanntlich ist jede absolut konvergente Reihe auch konvergent, aber nicht umgekehrt.

Lemma 2.1. *Für jede Potenzreihe $\sum_{k=0}^{\infty} a_k(z-z_0)^k$ existiert ein $R \in \mathbb{R}_{\geq 0} \cup \{\infty\}$, sodass gilt:*

a) Für alle $z \in \mathbb{C}$ mit $|z-z_0| < R$ ist die Reihe absolut konvergent.

b) Für alle $z \in \mathbb{C}$ mit $|z-z_0| > R$ ist die Reihe divergent mit $\sum_{k=0}^{\infty} |a_n||z-z_0|^n = \infty$.

Beweis. Wenn die Potenzreihe in einem Punkt $z_1 \in \mathbb{C}$ konvergiert, so bilden ihre Glieder $a_n(z_1-z_0)^n$ eine Nullfolge. Für $n \geq n_0$ groß gilt also $|a_n||z_1-z_0|^n \leq 1$. Es folgt

$$\sum_{n=n_0}^{\infty} |a_n||z-z_0|^n \;=\; \sum_{n=n_0}^{\infty} |a_n||z_1-z_0|^n \cdot \left|\tfrac{z-z_0}{z_1-z_0}\right|^n \;\leq\; \sum_{n=n_0}^{\infty} \left|\tfrac{z-z_0}{z_1-z_0}\right|^n$$

und somit ist für $|z-z_0| < r := |z_1-z_0|$ die geometrische Reihe auf der rechten Seite eine konvergente Majorante, was die absolute Konvergenz der Reihe für $|z-z_0| < r$ sichert. Für

$$\begin{aligned} R \;&:=\; \sup\Big\{\, |z_1-z_0| \in \mathbb{R} :\;\; z_1 \in \mathbb{C} \text{ und } \sum_{n=n_0}^{\infty} a_n(z_1-z_0)^n \text{ konvergiert} \,\Big\} \\ &=\; \sup\Big\{\, |z-z_0| \in \mathbb{R} :\;\; z \in \mathbb{C} \text{ und } \sum_{n=n_0}^{\infty} |a_n||z-z_0|^n \,<\, \infty \,\Big\} \end{aligned}$$

folgt daher die Behauptung. □

Wir bezeichnen R als den *Konvergenzradius* der Potenzreihe. Dann konvergiert die Potenzreihe auf der offenen Kreisscheibe

$$D_R(z_0) \;:=\; \{z \in \mathbb{C} \mid |z-z_0| < R\},$$

dem *Konvergenzkreis* der Potenzreihe. Die Fälle $R \in \{0, \infty\}$ sind dabei möglich. Auf dem Rand des Konvergenzkreises können wir keine allgemeine Konvergenzaussage treffen: Die Potenzreihen

$$f(z) \;=\; \sum_{n=1}^{\infty} z^n, \quad g(z) \;=\; \sum_{n=1}^{\infty} \frac{z^n}{n} \quad \text{und} \quad h(z) \;=\; \sum_{n=1}^{\infty} \frac{z^n}{n^2}$$

haben alle Konvergenzradius $R = 1$; die erste divergiert auf dem ganzen Rand des Konvergenzkreises, die zweite konvergiert in allen Randpunkten $z \neq 1$ und die dritte konvergiert in allen Randpunkten.

Satz 2.2. *Sei $\sum_{n=0}^{\infty} a_n(z-z_0)^n$ eine Potenzreihe mit Konvergenzradius $R > 0$. Dann ist*

$$f: \quad U \;:=\; D_R(z_0) \;\longrightarrow\; \mathbb{C}, \quad f(z) \;:=\; \sum_{n=0}^{\infty} a_n\,(z-z_0)^n$$

eine holomorphe Funktion, und ihre komplexe Ableitung wird in jedem Punkt $z \in U$ gegeben durch

$$f'(z) \;=\; \sum_{n=0}^{\infty} n \cdot a_n\,(z-z_0)^{n-1} \;\in\; \mathbb{C}.$$

Beweis. Zur Vereinfachung der Notation nehmen wir $z_0 = 0$ an, was durch eine Verschiebung des Koordinatensystems erreichbar ist. Der Differenzenquotient der Potenzreihe wird dann

$$\frac{f(z+h)-f(z)}{h} \;=\; \sum_{n=1}^{\infty} a_n \cdot \frac{(z+h)^n - z^n}{h} \;=\; \sum_{n=1}^{\infty} a_n \cdot \frac{1}{h} \cdot \sum_{k=1}^{n} \tbinom{n}{k} \cdot h^k \cdot z^{n-k}$$

$$= \sum_{n=1}^{\infty} a_n \cdot n \cdot z^{n-1} \;+\; h \cdot g(z,h)$$

mit dem Fehlerterm

$$g(z,h) \;:=\; \sum_{n=2}^{\infty} \sum_{k=2}^{n} a_n \cdot \tbinom{n}{k} \cdot h^{k-2} \cdot z^{n-k}.$$

Mit dem Wurzelkriterium sieht man, dass die durch gliedweises Ableiten gebildete Potenzreihe $\sum_{n=1}^{\infty} a_n \cdot n \cdot z^{n-1}$ denselben Konvergenzradius wie die Potenzreihe $f(z)$ besitzt. Zu zeigen bleibt, dass $g(z,h)$ bei festem z für $h \to 0$ beschränkt bleibt. Dazu beachte man

$$|g(z,h)| \;\le\; \frac{1}{|h_0|^2} \cdot \sum_{n=2}^{\infty} |a_n| \cdot (|z| + |h_0|)^n \quad \text{für} \quad |h| \;\le\; |h_0|.$$

Dabei wird $|h_0|$ im Folgenden fest gewählt und hängt nur von R und z ab. Für $|h_0|$ klein genug erhalten wir $|z| + |h_0| < R$ und dann konvergiert nach Voraussetzung die Reihe auf der rechten Seite. Hieraus folgt die Behauptung. □

Bemerkung 2.3. Insbesondere ist in der Situation von Satz 2.2 auch $f' : U \to \mathbb{C}$ eine holomorphe Funktion: Potenzreihen sind im Inneren ihres Konvergenzkreises unendlich oft komplex differenzierbar!

Beispiel 2.4. Die Potenzreihe

$$\exp(z) \;:=\; \sum_{k=0}^{\infty} \frac{z^k}{k!}$$

konvergiert nach der aus der reellen Analysis bekannten Abschätzung absolut für alle $z \in \mathbb{C}$. Sie definiert also eine holomorphe Funktion

$$\exp : \quad \mathbb{C} \;\longrightarrow\; \mathbb{C}, \quad z \;\mapsto\; \exp(z),$$

und gliedweises Ableiten zeigt wie in der reellen Analysis $\exp'(z) = \exp(z)$. Wir schreiben auch kurz $e^z := \exp(z)$. Da wir absolut konvergente Potenzreihen beliebig umordnen dürfen, erhalten wir durch Zusammenfassen aller geraden bzw. ungeraden Indices k in der Potenzreihe die *Eulersche Formel*

$$\exp(i\varphi) \;=\; \cos(\varphi) + i\sin(\varphi) \quad \text{für} \quad \varphi \;\in\; \mathbb{R}.$$

Wir können den Spieß umdrehen und definieren allgemeiner für komplexe $z \in \mathbb{C}$ die *Cosinus- und Sinusfunktion* durch

$$\cos(z) := \frac{e^{iz}+e^{-iz}}{2} = \sum_{l=0}^{\infty} \frac{(-1)^l}{(2l)!} \cdot z^{2l}$$

$$\sin(z) := \frac{e^{iz}-e^{-iz}}{2i} = \sum_{l=0}^{\infty} \frac{(-1)^l}{(2l+1)!} \cdot z^{2l+1}$$

dann gilt $\exp(iz) = \cos(z) + i\sin(z)$ auch für komplexe Werte $z \in \mathbb{C}$.

Lemma 2.5. *Gegeben seien zwei Potenzreihen $f(z) = \sum_{k=0}^{\infty} a_k z^k$ und $g(z) = \sum_{l=0}^{\infty} b_l z^l$ mit dem Konvergenzradius $\geq R$. Für $|z| < R$ ist dann das Produkt der beiden Reihen gegeben durch*

$$f(z)\,g(z) = \sum_{m=0}^{\infty} c_m z^m \quad \textit{mit} \quad c_m := \sum_{k+l=m} a_k b_l$$

Beweis. Wie in der reellen Analysis. □

Beispiel 2.6. Für alle $z, w \in \mathbb{C}$ gilt

$$\exp(z+w) := \exp(z) \cdot \exp(w).$$

Indem wir hierbei speziell $z = i\alpha$ und $w = i\beta$ mit $\alpha, \beta \in \mathbb{R}$ setzen, die Eulersche Formel anwenden und das Ergebnis Real- und Imaginärteil aufteilen, erhalten wir die Additionstheoreme

$$\begin{aligned} \cos(\alpha+\beta) &= \cos(\alpha)\cos(\beta) - \sin(\alpha)\sin(\beta), \\ \sin(\alpha+\beta) &= \sin(\alpha)\cos(\beta) + \cos(\alpha)\sin(\beta). \end{aligned}$$

Holomorphe Funktionen helfen also auch in der reellen Analysis weiter.

Wir haben gesehen, dass jede Potenzreihe im Innern ihres Konvergenzkreises absolut konvergiert und dort eine holomorphe Funktion definiert. In jedem Punkt außerhalb des Konvergenzkreises divergiert die Potenzreihe. Damit ist aber nicht gesagt, dass es keine Fortsetzung zu einer holomorphen Funktion auf einer größeren offenen Teilmenge $U \subseteq \mathbb{C}$ gäbe:

Beispiel 2.7. Es ist

$$\frac{1}{z^2+1} = \sum_{k=0}^{\infty} (-1)^k z^{2k} \quad \text{für} \quad |z| < 1.$$

Die Potenzreihe auf der rechten Seite hat nur den Konvergenzradius $R = 1$, obwohl die linke Seite eine auf ganz $U = \mathbb{C} \setminus \{\pm i\}$ holomorphe Funktion darstellt.

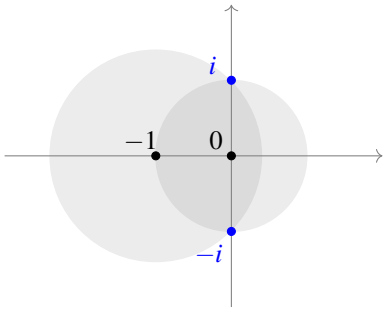
Der aus reeller Sicht nicht ganz verständliche Konvergenzradius erklärt sich in diesem Beispiel aus den Polen in den Punkten $z = \pm i \in \mathbb{C}$. Anstatt die gegebene Funktion in eine Potenzreihe um den Nullpunkt zu entwickeln, könnten wir sie aber auch in eine Potenzreihe um andere Punkte entwickeln und so ganz U ausschöpfen, z.B. ist

$$\frac{1}{z^2+1} = \frac{1}{2i}\cdot\left[\frac{1}{z-i} - \frac{1}{z+i}\right] \qquad \text{mit} \qquad \frac{1}{z\mp i} = \frac{1}{(z+1)-(1\pm i)}$$

$$= -\sum_{k=0}^{\infty} \frac{1}{(1\pm i)^{k+1}} \cdot (z+1)^k$$

$$\text{für} \quad |z+1| < \sqrt{2}.$$

Die folgende Skizze zeigt die Konvergenzkreise der ursprünglichen Potenzreihe um den Punkt $z_0 = 0$ und derjenigen um $z_0 = -1$:



Wir könnten natürlich genauso eine Potenzreihenentwicklung um jeden anderen Punkt $z_0 \in U$ erhalten, der Konvergenzradius wird $R = \min\{|z_0 - i|, |z_0 + i|\} > 0$ sein. Dies motiviert die folgende Definition:

Definition 2.8. Sei $U \subseteq \mathbb{C}$ offen. Eine Funktion $f : U \to \mathbb{C}$ heißt *analytisch*, wenn sie sich lokal um jeden Punkt in eine Potenzreihe entwickeln lässt, d.h. wenn es zu jedem $z_0 \in U$ eine Potenzreihe $\sum_{k=0}^{\infty} a_k (z - z_0)^k$ vom Konvergenzradius $R > 0$ gibt mit

$$f(z) = \sum_{k=0}^{\infty} a_k (z - z_0)^k \qquad \text{für alle} \qquad z \in U \cap D_R(z_0).$$

Da die komplexe Differenzierbarkeit einer Funktion eine lokale Eigenschaft ist, sind analytische Funktionen nach Satz 2.2 holomorph. Ihre lokale Entwicklung um jeden Punkt ist eindeutig bestimmt, es handelt sich dabei um die Taylorreihe der Funktion in dem jeweiligen Punkt:

Bemerkung 2.9. Wenn eine Funktion $f : U \to \mathbb{C}$ sich lokal um einen Punkt $z_0 \in U$ durch eine Potenzreihe

$$f(z) \;=\; \sum_{k=0}^{\infty} a_k (z - z_0)^k$$

mit dem Konvergenzradius $R > 0$ darstellen lässt, so erhält man durch Ableiten der Potenzreihe

$$a_k \;=\; f(z_0), \quad a_1 \;=\; f'(z_0), \quad a_2 \;=\; \tfrac{1}{2} f''(z_0), \quad \cdots, \quad a_k \;=\; \tfrac{1}{k!} f^{(k)}(z_0), \quad \cdots$$

Wir können also von *der* Potenzreihenentwicklung von f um den Punkt z_0 sprechen.

Analytische Funktionen erben viele gute Eigenschaften von Potenzreihen. Wir werden bald sehen, dass im Gegensatz zur Situation in der reellen Analysis *jede* komplex differenzierbare Funktion analytisch ist!

3 Ein Beispiel: Der komplexe Logarithmus

Die Funktion $\exp : \mathbb{C} \to \mathbb{C}^\times$ ist wegen $\exp(z + 2\pi i) = \exp(z)$ nicht injektiv. Sie induziert einen Isomorphismus

$$\exp : \quad (\mathbb{C}/2\pi i\mathbb{Z}, +) \;\xrightarrow{\sim}\; (\mathbb{C}^\times, \cdot\,)$$

von Gruppen, dessen Inverses man komplexen Logarithmus nennen könnte. In der Analysis möchten wir den Logarithmus aber als komplexwertige Funktion ansehen und müssen dazu die Winkel in Polarkoordinaten eindeutig festlegen. Dazu fordert man meist, dass sie im halboffenen Intervall $(-\pi, \pi]$ liegen sollen.

Definition 3.1. Die Funktion

$$\begin{aligned} \mathrm{Arg} : \quad \mathbb{C} \setminus \{0\} \;&\longrightarrow\; (-\pi, \pi], \\ re^{i\alpha} \;&\mapsto\; \alpha \quad \text{für } r > 0 \text{ und } \alpha \in (-\pi, \pi], \end{aligned}$$

heißt der *Hauptwert der Arguments* komplexer Zahlen; der Begriff Hauptwert deutet an, dass hier eine willkürliche Wahl getroffen wurde und man ebensogut z.B. auch Winkel in $(0, 2\pi]$ betrachten könnte. Der *Hauptwert des Logarithmus* ist definiert durch

$$\mathrm{Log} : \quad \mathbb{C} \setminus \{0\} \;\longrightarrow\; \mathbb{C}, \quad z \mapsto \mathrm{Log}(z) \;:=\; \log(|z|) + i\,\mathrm{Arg}(z),$$

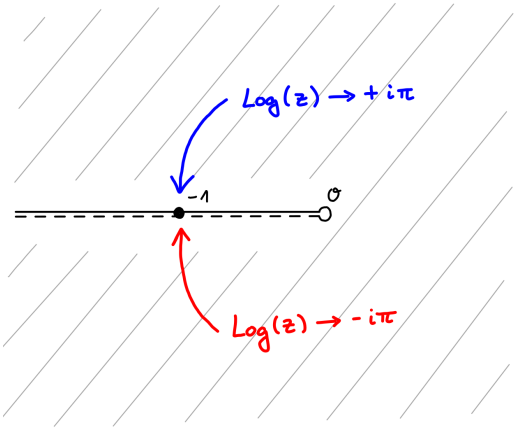
wobei $\log : \mathbb{R}_{>0} \to \mathbb{R}$ den natürlichen Logarithmus reeller Zahlen bezeichnet. Es gilt also

$$\begin{aligned} \exp(\mathrm{Log}(z)) \;&=\; z && \text{für alle } z \in \mathbb{C}^\times \\ \mathrm{Log}(\exp(w)) \;&\in\; w + 2\pi i\mathbb{Z} && \text{für alle } w \in \mathbb{C}. \end{aligned}$$

Statt *Hauptwert* sagt man auch *Hauptzweig*. Man beachte, dass für jedes $x \in \mathbb{R}_{<0}$ gilt:

$$\lim_{\substack{\varepsilon\to 0\\ \varepsilon>0}} \Big(\operatorname{Log}(x+i\varepsilon) - \operatorname{Log}(x-i\varepsilon)\Big) \;=\; i \lim_{\substack{\varepsilon\to 0\\ \varepsilon>0}} \Big(\operatorname{Arg}(x+i\varepsilon) - \operatorname{Arg}(x-i\varepsilon)\Big) \;=\; 2\pi i.$$

Der Hauptzweig des Logarithmus ist also auf der negativen reellen Halbgeraden unstetig. Die folgende Abbildung illustriert sein Sprungverhalten:



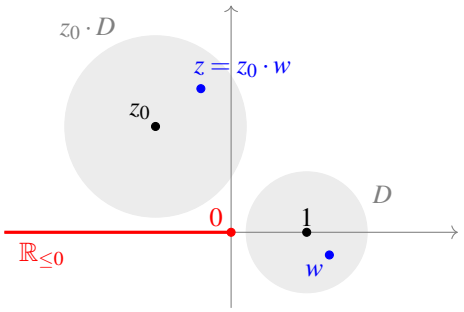
Auf der *geschlitzten Ebene*, dem Komplement der negativen reellen Halbgeraden, sieht die Situation jedoch besser aus:

Satz 3.2. *Die Funktion* $\operatorname{Log} : U := \mathbb{C} \setminus \mathbb{R}_{\leq 0} \longrightarrow \mathbb{C}$ *ist analytisch.*

Beweis. Sei $z_0 \in U$ beliebig, aber fest vorgegeben. Wir wählen $r \in (0,1)$ so klein, dass

$$z_0 \cdot D \;:=\; \{z_0 \cdot w \mid w \in D\} \;\subset\; U \quad \text{für} \quad D \;:=\; \{w \in \mathbb{C} \mid |w-1| < r\}.$$

ist wie in der folgenden Skizze gezeigt:



Dann ist insbesondere die Funktion

$$f: \quad D \longrightarrow \mathbb{C}, \quad f(w) := \operatorname{Log}(z_0 \cdot w) - \operatorname{Log}(z_0) - \operatorname{Log}(w)$$

wohldefiniert und auf ihrem gesamten Definitionsbereich stetig. Wir wollen uns überlegen, dass diese Funktion überall Null ist, und dann eine Potenzreihe für den Logarithmus um den Punkt z_0 mithilfe der bekannten Logarithmusreihe um $w_0 = 1$ erhalten. Zunächst gilt

$$\begin{aligned}
\exp(f(w)) &= \exp\big(\operatorname{Log}(z_0 \cdot w) - \operatorname{Log}(z_0) - \operatorname{Log}(w)\big) && \text{per Definition von } f \\
&= \frac{\exp(\operatorname{Log}(z_0 \cdot w))}{\exp(\operatorname{Log}(z_0)) \cdot \exp(\operatorname{Log}(w))} && \text{da exp multiplikativ ist} \\
&= \frac{z_0 \cdot w}{z_0 \cdot w} && \text{wegen } \exp \circ \operatorname{Log} = \mathrm{id} \\
&= 1.
\end{aligned}$$

Also erhalten wir, dass $f(w) \in 2\pi i\mathbb{Z}$ für alle $w \in D$ ist. Als stetige Funktion auf der zusammenhängenden Menge D mit Werten in der diskreten Teilmenge $2\pi i\mathbb{Z} \subseteq \mathbb{C}$ muß dann f eine konstante Funktion sein. Wegen $f(1) = 0$ ist die Funktion Null, also

$$\operatorname{Log}(z_0 \cdot w) = \operatorname{Log}(z_0) + \operatorname{Log}(w) \quad \text{für alle} \quad w \in D.$$

wie behauptet. Wir erhalten nun eine Reihenentwicklung von $\operatorname{Log}(z)$ um z_0 durch Einsetzen von $w = z/z_0$ in die aus der reellen Analysis bekannte Logarithmusreihe der Form

$$\operatorname{Log}(w) = \sum_{n=1}^{\infty} \tfrac{(-1)^{n+1}}{n} \cdot (w-1)^n \quad \text{für} \quad w \in D.$$

Diese Gültigkeit dieser Potenzreihenentwicklung von Log auf der Kreisscheibe D können wir wie in der reellen Analysis prüfen: Zunächst ist die Potenzreihe auf der rechten Seite für $w \in D$ konvergent, stellt also eine analytische Funktion $g : D \to \mathbb{C}$ dar. Nach Satz 2.2 ist

$$g'(w) = \sum_{n=1}^{\infty} (-1)^{n+1} \cdot (w-1)^{n-1} = \frac{1}{1+(w-1)} = \frac{1}{w} \quad \text{für} \quad w \in D.$$

Als Verkettung analytischer Funktionen ist auch die Funktion $g \circ \exp$ analytisch auf der Menge $V := \{z \in \mathbb{C} \mid \exp(z) \in D\}$, und mit der Kettenregel in Lemma 1.2 erhalten wir dann

$$(g \circ \exp)'(z) = 1 \quad \text{für alle} \quad z \in V.$$

Insbesondere verschwinden alle höheren Ableitungen der Funktion $g \circ \exp$ und nach Bemerkung 2.9 ist dann $(g \circ \exp)(z) = z + c$ für ein $c \in \mathbb{C}$. Auswerten in $z = 0$ liefert $c = 0$, also erhalten wir $g(\exp(z)) = z = \operatorname{Log}(\exp(z))$ für alle $z \in V$ und somit folgt wie gewünscht $g(w) = \operatorname{Log}(w)$ für alle $w \in D = \{\exp(z) \mid z \in V\}$. □

Mithilfe des komplexen Logarithmus können wir beispielsweise eine Wurzel komplexer Zahlen definieren durch die auf der geschlitzten Ebene holomorphe Funktion

$$f\colon \quad \mathbb{C}^\times \longrightarrow \mathbb{C}, \quad z \mapsto \exp\left(\tfrac{1}{2}\mathrm{Log}(z)\right)$$

mit $(f(z))^2 = z$ für alle $z \neq 0$. Man beachte, dass diese Funktion auf der negativen reellen Halbgeraden unstetig ist: Beim Überqueren dieser Halbgeraden springt ihr Vorzeichen, denn

$$\lim_{\substack{\varepsilon\to 0\\ \varepsilon>0}} f(x\pm i\varepsilon) \;=\; \exp\left(\lim_{\substack{\varepsilon\to 0\\ \varepsilon>0}} \tfrac{1}{2}\mathrm{Log}(x\pm i\varepsilon)\right) \;=\; \exp\left(\frac{\log(|x|)\pm i\pi}{2}\right) \;=\; \pm\sqrt{|x|}.$$

Wen dies nicht stört, der kann sogar Potenzen mit komplexen Exponenten definieren durch

$$z^\alpha \stackrel{??}{:=} \exp(\alpha\cdot\mathrm{Log}(z)) \quad \text{für} \quad z\in\mathbb{C}^\times \quad \text{und} \quad \alpha\in\mathbb{C}.$$

Dabei ist allerdings etwas Vorsicht geboten: Diese Definition ist willkürlich, weil unsere Wahl des Hauptzweiges Log auf der Konvention beruhte, die Winkel für Polarkoordinaten in $(-\pi,\pi]$ zu wählen. Man hätte ebensogut andere Konventionen für die Winkel treffen können, der Hauptzweig des komplexen Logarithmus wäre dann ersetzt worden durch einen anderen Logarithmus, der sich von Log um ein ganzzahliges Vielfaches von $2\pi i$ unterscheidet. Daher könnte man mit gleichem Recht jede der Zahlen

$$z^\alpha \stackrel{??}{:=} \exp(\alpha\cdot(\mathrm{Log}(z)+2\pi ik)) \;=\; \exp(\alpha\cdot\mathrm{Log}(z))\cdot\exp(2\pi ik\alpha) \quad \text{für} \quad k\in\mathbb{Z}$$

als eine α-te Potenz von z betrachten. Konkret:

- Für $\alpha\in\mathbb{Z}$ gibt es keine Wahlmöglichkeiten.
- Für $\alpha = 1/2$ haben wir das Vorzeichen $\exp(\pi ik)\in\{\pm 1\}$ zu wählen.
- Für $\alpha = 1/n$ haben wir eine n-te Einheitswurzel $\exp(2\pi ik/n)$ zu wählen.
- Für $\alpha\notin\mathbb{Q}$ haben wir unendlich viele Wahlmöglichkeiten.

Beim Rechnen mit Potenzen ist also Vorsicht geboten. Wo ist beispielsweise der Fehler in

$$-1 \;=\; i\cdot i \;=\; (-1)^{1/2}\cdot(-1)^{1/2} \;=\; ((-1)\cdot(-1))^{1/2} \;=\; 1^{1/2} \;=\; 1?$$

4 Der Integralsatz von Cauchy

Wir wollen uns nun wieder der allgemeinen Untersuchung holomorpher Funktionen zuwenden. Das zentrale Hilfsmittel dafür ist das Pfadintegral stetiger Funktionen über einen stückweise glatten Pfad:

Definition 4.1. Unter einem *Pfad* in einer offenen Teilmenge $U \subseteq \mathbb{C} = \mathbb{R}^2$ verstehen wir eine stetige Abbildung

$$\gamma\colon \quad I \;=\; [0,1] \;\longrightarrow\; U.$$

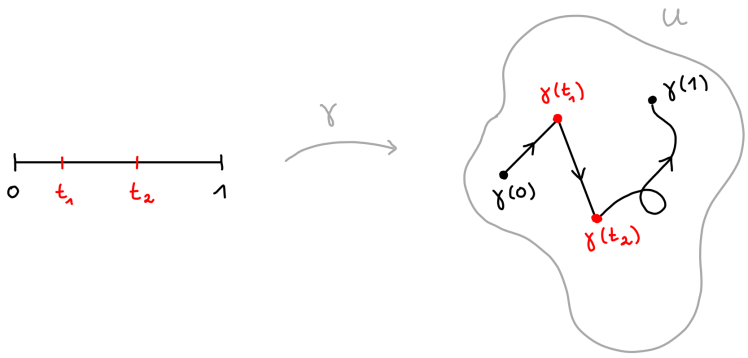
Der Pfad heißt *stückweise glatt*, wenn er außerhalb endlich vieler Punkte $t \in [0,1]$ eine glatte Abbildung im Sinn der reellen Analysis ist. Wir setzen dann

$$\gamma'(t) \;:=\; \tfrac{d}{dt}\gamma(t) \;=\; \tfrac{d}{dt}\operatorname{Re}(\gamma(t)) + i\cdot \tfrac{d}{dt}\operatorname{Im}(\gamma(t))$$

für fast alle $t \in [0,1]$. Das *Pfadintegral* einer stetigen Funktion $f : U \to \mathbb{C}$ entlang γ ist definiert als

$$\begin{aligned}\int_\gamma f(z)dz \;&:=\; \int_0^1 f(\gamma(t))\gamma'(t)dt \\ &:=\; \int_0^1 \operatorname{Re}\big(f(\gamma(t)\gamma'(t)\big)dt \;+\; i\cdot\int_0^1 \operatorname{Im}\big(f(\gamma(t)\gamma'(t)\big)dt.\end{aligned}$$

Man beachte, dass hier noch keine komplexe Analysis vorkommt: Denn $\gamma'(t)$ ist eine gewöhnliche Ableitung nach der reellen Variablen t, und f muß lediglich eine stetige Funktion sein.



Unter einer *Reparametrisierung* von $\gamma : [0,1] \to U$ verstehen wir einen Pfad $\gamma \circ \sigma$ für eine bijektive, stetige, stückweise glatte Abbildung $\sigma : [0,1] \to [0,1]$. Dabei ist $\{\sigma(0), \sigma(1)\} = \{0,1\}$, und wir setzen

$$sgn(\sigma) \;:=\; \begin{cases} +1 & \text{falls } \sigma(0) = 0 \text{ und } \sigma(1) = 1 \text{ ist,} \\ -1 & \text{falls } \sigma(0) = 1 \text{ und } \sigma(1) = 0 \text{ ist.} \end{cases}$$

Die *Länge* von γ ist definiert durch

$$\ell(\gamma) \;:=\; \int_0^1 |\gamma'(t)|\,dt.$$

Lemma 4.2. *Sei $\gamma : [0,1] \to U$ ein stückweise stetiger Pfad.*

a) Das Pfadintegral $\int_\gamma f(z)dz$ hängt linear von $f : U \to \mathbb{C}$ ab.

b) Für Reparametrisierungen $\tau = \gamma \circ \sigma$ ist $\int_{\gamma\circ\sigma} f(z)dz = sgn(\sigma) \cdot \int_\gamma f(z)dz$.

c) Falls ein $c \geq 0$ existiert mit $|f(z)| \leq c$ für alle $z \in U$, so gilt $|\int_\gamma f(z)dz| \leq \ell(\gamma) \cdot c$.

Beweis. Die Linearität ist klar. Die Invarianz unter Reparametrisierung folgt aus der Substitutionsformel für Integrale:

$$\begin{aligned}
\int_{\gamma\circ\sigma} f(z)dz &= \int_0^1 f(\gamma(\sigma(t)))(\gamma\circ\sigma)'(t)dt && \text{per Definition} \\
&= \int_0^1 f(\gamma(\sigma(t)))\gamma'(\sigma(t))\sigma'(t)dt && \text{nach der Kettenregel} \\
&= \int_{\sigma(0)}^{\sigma(1)} f(\gamma(s))\gamma'(s)ds && \text{mit der Substitution } s = \sigma(t) \\
&= sgn(\sigma) \cdot \int_\gamma f(z)dz && \text{per Definition von } sgn(\sigma).
\end{aligned}$$

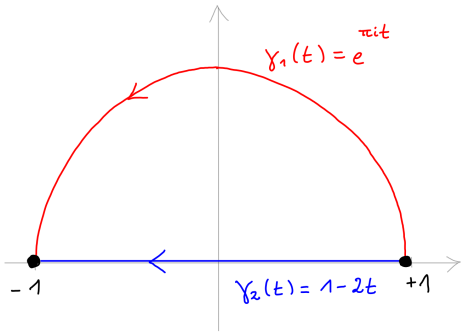
Die Abschätzung in c) folgt ebenfalls direkt aus der Definition. □

Das Pfadintegral einer stetigen Funktion hängt im Allgemeinen nicht nur vom Anfangs- und Endpunkt des Pfades ab:

Beispiel 4.3. Seien $\gamma_1, \gamma_2 : [0,1] \to \mathbb{C}$ gegeben durch $\gamma_1(t) = e^{\pi it}$ und $\gamma_2(t) = 1 - 2t$, dann gilt

$$\int_{\gamma_1} \bar{z}dz = \int_0^1 e^{-\pi it} \cdot \pi i e^{\pi it}\, dt = \pi i \int_0^1 dt = \pi i,$$

$$\int_{\gamma_2} \bar{z}dz = \int_0^1 (1-2t) \cdot (-2)\, dt = \int_0^1 (4t-2)\, dt = 0.$$



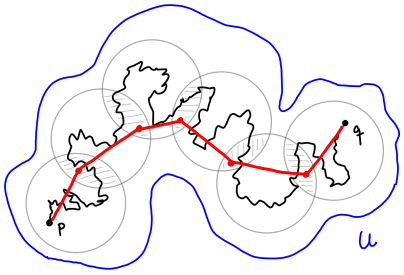
Die Pfadintegrale sind verschieden, obwohl $\gamma_1(0) = \gamma_2(0)$ und $\gamma_1(1) = \gamma_2(1)$ ist!

Wir werden bald sehen, dass sich Pfadintegrale über *holomorphe* Funktionen besser verhalten. Doch zunächst noch einige Definitionen:

Definition 4.4. Eine Teilmenge $U \subseteq \mathbb{C}$ heißt *wegzusammenhängend*, wenn es für alle $p, q \in U$ einen stetigen Pfad

$$\gamma\colon \quad [0,1] \longrightarrow U \quad \text{mit } \gamma(0) = p \text{ und } \gamma(1) = q$$

gibt. Ein *Gebiet* ist eine offene wegzusammenhängende Teilmenge $U \subseteq \mathbb{C}$. Da das Einheitsintervall kompakt ist, lässt sich das Bild von jedem stetigen Pfad in einer offenen Menge U durch endlich viele Kreisscheiben in U überdecken; daher lassen sich in einem Gebiet je zwei Punkte durch einen stückweise glatten – sogar durch einen stückweise linearen – Pfad miteinander verbinden.



Soweit nicht anders gesagt, setzen wir daher ab jetzt alle Pfade als stückweise glatt voraus. Ein Pfad $\gamma\colon [0,1] \to U$ heißt *geschlossen*, wenn $\gamma(0) = \gamma(1)$ ist.

Unter einer *Stammfunktion* einer gegebenen Funktion $f : U \to \mathbb{C}$ verstehen wir eine holomorphe Funktion $F : U \to \mathbb{C}$, sodass $F' = f$ ist. Das Pfadintegral von f über beliebige Pfade können wir dann nach dem Hauptsatz der Differential- und Integralrechnung ausrechnen als

$$\begin{aligned}
\int_\gamma f(z)dz &= \int_\gamma F'(z)dz \\
&= \int_0^1 F'(\gamma(t))\gamma'(t)dt \\
&= \int_0^1 \tfrac{d}{dt}(F(\gamma(t)))dt \\
&= F(\gamma(1)) - F(\gamma(0))
\end{aligned}$$

denn man prüft leicht nach, dass $\frac{d}{dt}(F(\gamma(t))) = F'(\gamma(t))\gamma'(t)$ ist. Insbesondere ist in diesem Fall also das Pfadintegral über jeden geschlossenen Pfad Null. Diese letzte Eigenschaft charakterisiert holomorphe Funktionen mit einer Stammfunktion:

Proposition 4.5. *Sei $U \subseteq \mathbb{C}$ ein Gebiet. Für holomorphe Funktionen $f : U \to \mathbb{C}$ sind äquivalent:*

a) Die Funktion f besitzt eine Stammfunktion $F : U \to \mathbb{C}$.

b) Es ist $\int_\gamma f(z)dz = 0$ für jeden geschlossenen Pfad $\gamma : [0,1] \to U$.

c) Das Integral $\int_\gamma f(z)dz$ hängt nicht von γ, sondern nur von $\gamma(0)$ und $\gamma(1)$ ab.

Beweis. Dass $b)$ aus $a)$ folgt, haben wir gerade gesehen. Aus $b)$ folgt $c)$, denn für je zwei verschiedene Pfade $\gamma_1, \gamma_2 : [0,1] \to U$ mit Anfangspunkt $\gamma_1(0) = \gamma_2(0)$ und Endpunkt $\gamma_1(1) = \gamma_2(1)$ ist

$$\gamma\colon \quad [0,1] \longrightarrow U, \quad t \mapsto \begin{cases} \gamma_1(2t) & \text{für } t \le 1/2, \\ \gamma_2(2-2t) & \text{für } t > 1/2, \end{cases}$$

ein geschlossener Pfad. Wenn $b)$ gilt, folgt also

$$0 = \int_\gamma f(z)dz = \int_{\gamma_1} f(z)dz - \int_{\gamma_2} f(z)dz,$$

wegen der Additivität und der Substitutionsregel für Integrale. Wenn schließlich $c)$ gilt, wählen wir $z_0 \in U$ beliebig und definieren

$$F\colon \quad U \longrightarrow \mathbb{C}, \quad z \mapsto \int_{z_0}^{z} f(w)dw,$$

wobei das Integral über einen beliebigen Pfad von z_0 nach z genommen werden kann; ein solcher Pfad existiert, da U wegzusammenhängend ist, und das Integral hängt nach Annahme nicht vom gewählten Pfad in U ab. Für $z, z+h \in U$ folgt aus der Additivität des Integrals

$$\begin{aligned} F(z+h) - F(z) &= \int_{z_0}^{z+h} f(w)dw - \int_{z_0}^{z} f(w)dw \\ &= \int_{z}^{z+h} f(w)dw \\ &= f(z)\cdot h + r(h) \quad \text{mit} \quad r(h) := \int_{z}^{z+h} (f(w) - f(z))dw \end{aligned}$$

und wegen der Stetigkeit von f gilt $\lim_{h\to 0} |r(h)/h| = 0$, also ist $a)$ erfüllt. □

Die Frage nach der Existenz von Stammfunktionen einer holomorphen Funktion ist also gleichbedeutend zur Frage nach Integralen über geschlossene Pfade. Wir beginnen mit Dreieckswegen: Unter einer *Dreiecksfläche* verstehen wir die konvexe Hülle

$$\Delta := \left\{ t_1 p_1 + t_2 p_2 + t_3 p_3 \in \mathbb{C} \mid t_1, t_2, t_3 \in \mathbb{R}_{\ge 0}, t_1 + t_2 + t_3 = 1 \right\}$$

von drei Punkten $p_1, p_2, p_3 \in \mathbb{C}$. Ihr Rand $\partial\Delta \subset \Delta$ lässt sich parametrisieren durch den Pfad

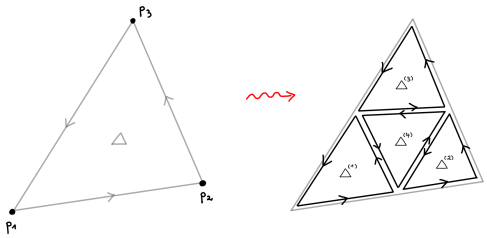
$$\partial\Delta: \quad [0,3] \longrightarrow \mathbb{C}, \quad t \mapsto \begin{cases} p_1 + t \cdot p_{12} & \text{für } 0 \le t < 1, \\ p_2 + (t-1) \cdot p_{23} & \text{für } 1 \le t < 2, \\ p_3 + (t-2) \cdot p_{31} & \text{für } 2 \le t \le 3, \end{cases}$$

mit $p_{jk} := p_k - p_j$. Man beachte, dass für die Orientierung von $\partial\Delta$ die gewählte Reihenfolge der drei Eckpunkte p_1, p_2, p_3 eine Rolle spielt.

Satz 4.6 (Satz von Cauchy für Dreieckspfade). *Sei $f : U \to \mathbb{C}$ holomorph. Dann gilt*

$$\int_{\partial\Delta} f(z)dz = 0 \quad \textit{für jede ganz in } U \textit{ enthaltene Dreiecksfläche} \quad \Delta \subset U.$$

Beweis. Wir unterteilen die Dreiecksfläche Δ durch Halbieren ihrer Seiten in vier kleinere Dreiecke $\Delta^{(1)}, \ldots, \Delta^{(4)}$ wie in der folgenden Skizze gezeigt:



Jedes der vier im Inneren von Δ liegenden Geradensegmente tritt im Rand $\partial\Delta^{(k)}$ für genau zwei Indices k auf. Wenn wir die Dreiecke alle kompatibel orientieren, dann sind die Orientierungen des Segmentes für die zwei Indices k entgegengesetzt, die Integrale über diese Teile der Randkurven heben sich also nach Lemma 4.2b) weg und wir erhalten

$$\int_{\partial\Delta} f(z)dz = \sum_{k=1}^{4} \int_{\partial\Delta^{(k)}} f(z)dz.$$

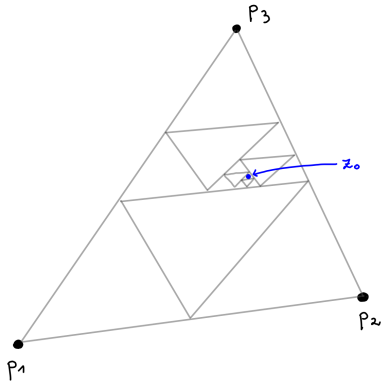
Sei $\Delta_1 := \Delta^{(k)}$ für einen Index k, sodass das entsprechende Integral auf der rechten Seite den maximalen Absolutbetrag hat. Dann ist also

$$\left| \int_{\partial\Delta} f(z)dz \right| \le 4 \cdot \left| \int_{\partial\Delta_1} f(z)dz \right|.$$

Wir unterteilen nun Δ_1 erneut in vier zueinander kongruente Dreiecke und fahren induktiv fort. Wir erhalten so eine Folge ineinandergeschachtelter Dreiecke

$$\Delta \supset \Delta_1 \supset \Delta_2 \supseteq \cdots \quad \text{mit} \quad \left| \int_{\partial\Delta} f(z)dz \right| \le 4^n \cdot \left| \int_{\partial\Delta_n} f(z)dz \right|,$$

wobei Δ_n kongruent zu $2^{-n} \cdot \Delta$ ist:



Nach dem Satz von Bolzano-Weierstrass existiert ein $z_0 \in \bigcap_{n\geq 1} \Delta_n$. Da f holomorph ist, können wir

$$f(z) \;=\; f(z_0) + f'(z_0)\cdot(z-z_0) + r(z) \quad \text{mit} \quad \lim_{z\to z_0} \frac{r(z)}{z-z_0} \;=\; 0$$

schreiben. Da jede affin-lineare Funktion eine Stammfunktion hat, ist das Integral über die ersten beiden Summanden Null. Also gilt

$$\int_{\partial\Delta_n} f(z)dz \;=\; \int_{\partial\Delta_n} r(z)dz$$

für alle $n \in \mathbb{N}$. Zu beliebig vorgegebenem $\varepsilon > 0$ wählen wir nun $n \in \mathbb{N}$ groß genug, sodass

$$|r(z)| \;\leq\; \varepsilon \cdot |z-z_0| \quad \text{für alle} \quad z \;\in\; \Delta_n$$

ist. Sei $\ell := \ell(\partial\Delta)$ die Länge des ursprünglich gegebenen Dreieckspfads. Die Länge der durch Unterteilung erhaltenen Dreieckspfade ist dann $\ell_n := \ell(\partial\Delta_n) = 2^{-n}\cdot\ell$ und wir erhalten

$$\left|\int_{\partial\Delta} f(z)dz\right| \;\leq\; 4^n \cdot \left|\int_{\partial\Delta_n} f(z)dz\right| \;\leq\; 4^n \cdot \ell_n \cdot \max_{z\in\partial\Delta_n} |r(z)| \;\leq\; 4^n \cdot \ell_n \cdot \varepsilon \cdot \ell_n \;\leq\; \varepsilon \cdot \ell^2$$

Da $\varepsilon > 0$ beliebig war, muß die linke Seite Null sein. □

An dieser Stelle sei betont, dass für den obigen Satz $\Delta \subset U$ gelten muß: Der Satz gilt im Allgemeinen *nicht* für holomorphe Funktionen, welche nur in einer kleinen Umgebung des Randes $\partial\Delta$ definiert sind, sondern f muß auf dem ganzen Inneren der Dreiecksfläche holomorph sein! Die Beschränkung auf Dreieckswege ist etwas künstlich, aber schon in der jetzigen Form ist der Satz von Cauchy nützlich:

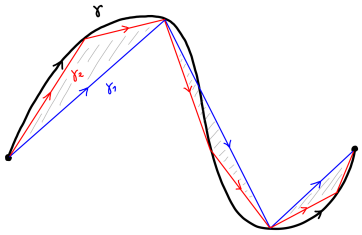
Beispiel 4.7. Sei $\gamma : [0,1] \to U$ ein stetiger, aber nicht notwendig stückweise glatter Pfad. Für eine hinreichend feine Unterteilung $\Sigma = \{0 = t_0 < t_1 < \cdots < t_n = 1\}$ können wir annehmen, dass das Geradensegment zwischen je zwei benachbarten Punkten $\gamma(t_i)$ und $\gamma(t_{i+1})$ ganz in U liegt, wie in der Abbildung in Definition 4.4 gezeigt. Sei

$$\gamma_\Sigma : \quad [0,1] \longrightarrow U$$

die durch diese Geradensegmente gegebene stückweise lineare Approximation des Pfades. Wir definieren das Pfadintegral über eine holomorphe Funktion $f : U \to \mathbb{C}$ entlang γ durch

$$\int_\gamma f(z)dz := \lim_{|\Sigma|\to 0} \int_{\gamma_\Sigma} f(z)dz$$

wobei $|\Sigma| := \max\{|t_{i+1} - t_i|\}$ die Maschenweite von $\Sigma = \{t_0 < t_1 < \cdots < t_n\}$ bezeichne. Der Limes ist wohldefiniert, denn die Differenz der Integrale über je zwei genügend feine stückweise lineare Approximationen ist eine Summe von Integralen über Dreieckswege ist und verschwindet somit nach Satz 4.6:

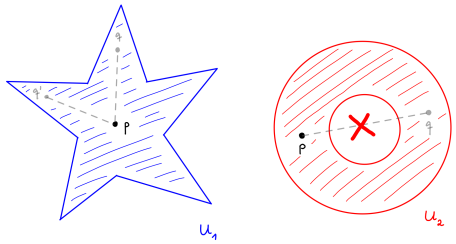


Man beachte, dass γ nur stetig, aber in keinem Punkt differenzierbar sein muß! In der reellen Integrationstheorie wäre so etwas nicht möglich.

Definition 4.8. Ein *Sterngebiet* ist eine offene Teilmenge $U \subseteq \mathbb{C}$, sodass ein $p \in U$ existiert mit der folgenden Eigenschaft:

$$\forall q \in U \; \forall\, t \in [0,1] : \quad t \cdot p + (1-t) \cdot q \; \in \; U.$$

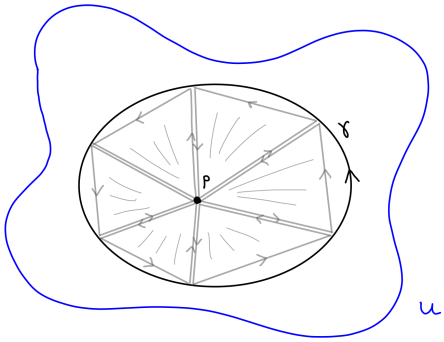
Der Punkt p muß nicht eindeutig sein; wir nennen ihn einen *Sternpunkt*. In der folgenden Skizze ist also das blaue Gebiet ein Sterngebiet. Das rote Gebiet ist kein Sterngebiet, denn kein Punkt lässt sich mit dem hierzu antipodalen Punkt durch ein Geradensegment verbinden:



Korollar 4.9 (Cauchy für Sterngebiete). *Sei $U \subseteq \mathbb{C}$ ein Sterngebiet und $f : U \to \mathbb{C}$ holomorph. Dann ist*

$$\int_\gamma f(z)dz \;=\; 0 \quad \textit{für jeden geschlossenen Pfad} \quad \gamma\colon\ [0,1] \;\longrightarrow\; U.$$

Beweis. Sei $p \in U$ ein Sternpunkt. Indem wir $\gamma : [0,1] \to U$ durch eine stückweise lineare Approximation ersetzen, können wir das Integral über γ ersetzen durch eine Summe von Integralen über Dreieckspfade:



Die Sternförmigkeit von U stellt sicher, dass alle Dreiecksflächen in U enthalten sind. Nach Satz 4.6 sind die Integrale über die Dreieckspfade Null. Die Beiträge der inneren Dreiecksseiten heben sich gegenseitig weg, und wir sind fertig. □

In Anwendungen treten besonders häufig Integrale über Kreislinien auf. Wir schreiben

$$\oint_{|z-z_0|=r} f(z)dz \;:=\; \int_\gamma f(z)dz \quad \text{für} \quad \gamma\colon\ [0,1] \;\longrightarrow\; \mathbb{C},\ t \;\mapsto\; z_0 + r\exp(2\pi i t).$$

Das folgende Beispiel zeigt, dass die Sternförmigkeit im Integralsatz von Cauchy nicht ersatzlos gestrichen werden darf:

Beispiel 4.10. Die Funktion $f : U = \mathbb{C} \setminus \{0\} \to \mathbb{C}, z \mapsto 1/z$ ist holomorph auf der punktierten komplexen Ebene. Ihr Integral über den Einheitskreis ist jedoch von Null verschieden, es ist

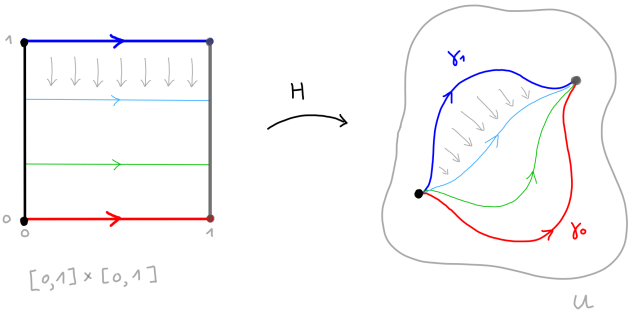
$$\oint_{|z|=1} \frac{1}{z}\,dz \;=\; \int_0^1 \frac{1}{e^{2\pi i t}} \cdot 2\pi i \cdot e^{2\pi i t} dt \;=\; 2\pi i.$$

Das Problem in diesem Beispiel ist anschaulich, dass der Definitionsbereich des Integranden ein “Loch” in der Mitte hat. Der Integrationspfad umrundet das “Loch” einmal, daran ändert sich auch nichts, wenn wir den Pfad innerhalb von U stetig deformieren. Wir wollen diese intuitive Vorstellung nun formal präzise fassen:

Definition 4.11. Zwei Pfade $\gamma_0, \gamma_1 : [0,1] \to U$ heißen *in U homotop*, wenn eine stetige Abbildung

$$H: \quad [0,1]\times[0,1] \longrightarrow U \quad \text{mit} \quad \begin{cases} H(0,t) = \gamma_0(t) & \text{für alle } t, \\ H(1,t) = \gamma_1(t) & \text{für alle } t, \\ H(s,0) = H(0,0) & \text{für alle } s, \\ H(s,1) = H(0,1) & \text{für alle } s, \end{cases}$$

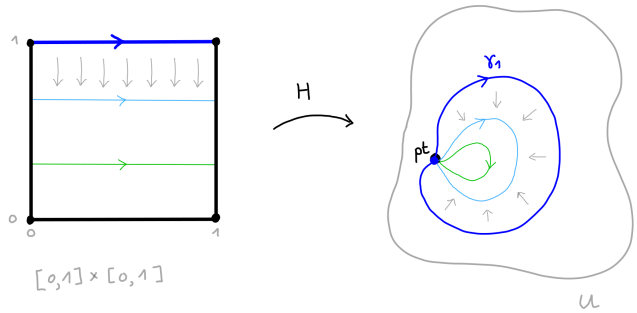
existiert. Insbesondere ist dann $\gamma_0(0) = \gamma_1(0)$ und $\gamma_0(1) = \gamma_1(1)$:



Man prüft leicht nach, dass durch

$$\gamma_0 \sim_U \gamma_1 \quad :\Longleftrightarrow \quad \gamma_0 \text{ und } \gamma_1 \text{ sind in } U \text{ zueinander homotop}$$

eine Äquivalenzrelation auf der Menge aller stetigen Pfade in U definiert wird. Die Äquivalenzklassen bezeichnet man als *Homotopieklassen* von Pfaden, wobei die offene Menge $U \subseteq \mathbb{C}$ für den Begriff der Homotopie immer dazugesagt werden sollte, wenn sie aus dem Kontext nicht klar ist. Ein geschlossener Pfad $\gamma\colon [0,1] \to U$ heißt *in U zusammenziehbar*, wenn er in U homotop zu einem konstanten Pfad ist, wir schreiben dann auch $\gamma \sim_U pt$:



Wir können nun die endgültige Version des Integralsatzes von Cauchy formulieren als eine Aussage zur Homotopieinvarianz von Pfadintegralen:

Satz 4.12 (Integralsatz von Cauchy). *Sei $f : U \to \mathbb{C}$ holomorph.*

a) Es gilt

$$\int_{\gamma_0} f(z)dz \;=\; \int_{\gamma_1} f(z)dz \quad \textit{für je zwei in } U \textit{ homotope Pfade} \quad \gamma_0 \sim_U \gamma_1.$$

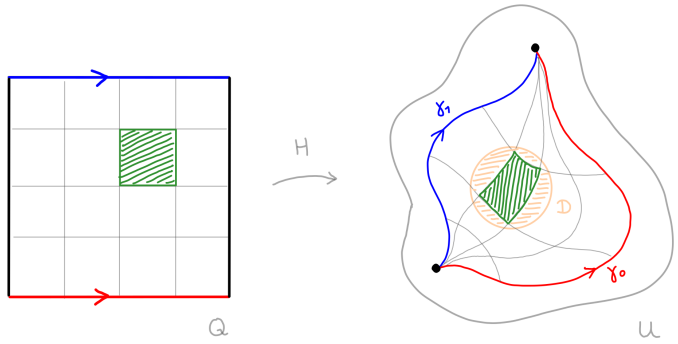
b) Insbesondere ist

$$\int_{\gamma} f(z)dz \;=\; 0 \quad \textit{für jeden in } U \textit{ zusammenziehbaren Pfad} \quad \gamma \sim_U pt.$$

Beweis. Die Aussage $b)$ folgt aus $a)$, weil das Pfadintegral über konstante Pfade Null ist. Es genügt daher, die Homotopieinvarianz $a)$ zu zeigen. Sei also $\gamma_0 \sim_U \gamma_1$ und

$$H: \quad Q \;=\; [0,1]\times[0,1] \;\longrightarrow\; U$$

wie in Definition 4.11. Wir zerlegen nun das Einheitsquadrat Q durch sukzessive Seitenhalbierungen in 4^n kleinere Quadrate $Q_{n,k}$ wie in der folgenden Abbildung gezeigt. Da H stetig und das Einheitsquadrat kompakt ist, können wir für $n \gg 0$ erreichen, dass das Bild jedes dieser Quadrate unter H enthalten ist in einer offenen Kreisscheibe in U:



Seien $\partial Q : [0,1] \to Q$ und $\partial Q_{n,k} : [0,1] \to Q_{n,k}$ die im mathematisch positiven Sinn einmal durchlaufenem Randkurven der Quadrate. Durch Verketten mit H erhalten wir hieraus geschlossene Pfade

$$H\circ\partial Q: \quad [0,1] \;\longrightarrow\; U \quad \text{und} \quad H\circ\partial Q_{n,k}: \quad [0,1] \;\longrightarrow\; D_{n,k} \;\subseteq\; U.$$

Da Kreisscheiben sternförmig sind, gilt $\int_{H\circ\partial Q_{n,k}} f(z)dz = 0$ nach Korollar 4.9. Dann folgt

$$\int_{\gamma_0} f(z)dz - \int_{\gamma_1} f(z) \;=\; \int_{H\circ\partial Q} f(z)dz \;=\; \sum_k \int_{H\circ\partial Q_{n,k}} f(z)dz \;=\; 0,$$

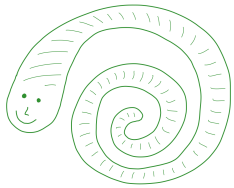
da sich die Beiträge entgegengesetzt orientierter Seiten aufheben. □

Wir nennen ein Gebiet $U \subseteq \mathbb{C}$ *einfach zusammenhängend*, wenn jeder geschlossene Pfad $\gamma : [0,1] \to U$ in dem Gebiet U zusammenziehbar ist.

Beispiel 4.13. Sterngebiete $U \subseteq \mathbb{C}$ sind einfach zusammenhängend: Sei $p \in U$ ein Sternpunkt, dann kann man jede Kurve $\gamma : [0,1] \to U$ auf den konstanten Pfad in p zusammenziehen mittels

$$H : \quad [0,1] \times [0,1] \longrightarrow U \quad \text{mit} \quad H(s,t) := p + s \cdot (\gamma(t) - p).$$

Es gibt aber viele einfach zusammenhängende Gebiete, die keine Sterngebiete sind:



Aus dem Integralsatz von Cauchy erhalten wir:

Korollar 4.14. *Auf einfach zusammenhängenden Gebieten besitzt jede holomorphe Funktion eine Stammfunktion.*

Beweis. Folgt aus Satz 4.12 und Proposition 4.5. □

Insbesondere hängt das Pfadintegral über holomorphe Funktionen auf einfach zusammenhängenden Gebieten nur vom Anfangs- und Endpunkt der Pfade ab!

5 Die Cauchy-Formel und Anwendungen

Wir wollen nun einige Anwendungen aus dem Integralsatz von Cauchy ziehen. Wir beginnen mit der folgenden *Integralformel von Cauchy*, welche die Funktionswerte einer holomorphen Funktion im Inneren einer Kreisscheibe aus ihren Werten auf dem Rand rekonstruiert; dabei schreiben wir wie in der Analysis $\overline{D} \subseteq \mathbb{C}$ für den Abschluß einer Teilmenge $D \subseteq \mathbb{C}$ in der komplexen Ebene.

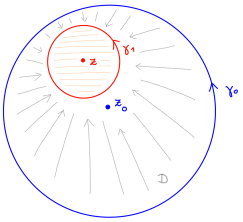
Satz 5.1 (Cauchy-Formel). *Sei $f : U \to \mathbb{C}$ holomorph, und seien $z_0 \in U$ und $r > 0$ gegeben mit*

$$\overline{D} \subseteq U \quad \textit{für die Kreisscheibe} \quad D := \{z \in \mathbb{C} \mid |z - z_0| < r\}$$

Dann gilt

$$f(z) = \frac{1}{2\pi i} \oint_{|\zeta - z_0| = r} \frac{f(\zeta)}{\zeta - z}\, d\zeta \qquad \textit{für alle} \quad z \in D.$$

Beweis. Für festes $z \in D$ ist eine Kreisscheibe um z von kleinem Radius $\varepsilon > 0$ ganz in D enthalten. Dann sind die Randkurve dieser kleinen Kreisscheibe und die Randkurve der ursprünglichen Kreisscheibe zueinander homotop in $\overline{D} \setminus \{z\}$:



Nach dem Satz von Cauchy folgt

$$\begin{aligned} \oint_{|\zeta - z_0| = r} \frac{f(\zeta)}{\zeta - z}\, d\zeta &= \oint_{|\zeta - z| = \varepsilon} \frac{f(\zeta)}{\zeta - z}\, d\zeta \\ &= \oint_{|\zeta - z| = \varepsilon} \frac{f(\zeta) - f(z)}{\zeta - z}\, d\zeta + \oint_{|\zeta - z| = \varepsilon} \frac{f(z)}{\zeta - z}\, d\zeta. \end{aligned}$$

Die linke Seite ist von ε unabhängig. Für $\varepsilon \to 0$ geht das erste Integral auf der rechten Seite gegen Null, da der Integrand wegen der Differenzierbarkeit von f beschränkt bleibt. Für das zweite Integral auf der rechten Seite gilt

$$\oint_{|\zeta - z| = \varepsilon} \frac{f(z)}{\zeta - z}\, d\zeta = f(z) \cdot \oint_{|\zeta - z| = \varepsilon} \frac{1}{\zeta - z}\, d\zeta = f(z) \cdot 2\pi i$$

und somit folgt die Behauptung. □

Im Fall $z = z_0$ folgt, dass der Wert einer holomorphen Funktion $f : U \to \mathbb{C}$ in einem Punkt gleich dem Mittelwert ihrer Funktionswerte auf einer Kreislinie um den Punkt ist:

$$f(z) = \frac{1}{2\pi} \int_0^{2\pi} f\left(z + re^{it}\right) dt \qquad \text{für} \quad \overline{D_r(z)} \subseteq U.$$

Die Cauchy-Formel zeigt zudem, dass holomorphe Funktionen analytisch sind:

Korollar 5.2. *Sei $f : U \to \mathbb{C}$ holomorph. Dann gibt es um jeden Punkt $z_0 \in U$ eine Potenzreihenentwicklung*

$$f(z) = \sum_{k=0}^{\infty} a_k \cdot (z - z_0)^k \quad \textit{mit} \quad a_k = \frac{1}{2\pi i} \oint_{|\zeta - z_0| = r} \frac{f(\zeta)}{(\zeta - z_0)^{k+1}}\, d\zeta,$$

und diese gilt auf jeder offenen Kreisscheibe $D = \{z \in \mathbb{C} \mid |z - z_0| < r\}$ mit $\overline{D} \subseteq U$.

Beweis. Durch Verschieben unseres Koordinatensystems dürfen wir oBdA $z_0 = 0$ annehmen. Sei $r > 0$ mit

$$D := \{z \in \mathbb{C} \mid |z| < r\} \subseteq \overline{D} \subseteq U.$$

Für $|z| < |\zeta| = r$ kann der Integrand in der Cauchy-Formel mit der geometrischen Reihen entwickelt werden:

$$\frac{f(\zeta)}{\zeta - z} = \frac{f(\zeta)}{\zeta} \cdot \frac{1}{1 - z/\zeta} = \frac{f(\zeta)}{\zeta} \cdot \sum_{k=0}^{\infty} \left(\frac{z}{\zeta}\right)^k = \sum_{k=0}^{\infty} \frac{f(\zeta)}{\zeta^{k+1}} \cdot z^k$$

Sei nun $z \in D$ fixiert. Dann konvergiert die Reihe auf der rechten Seite gleichmäßig in der Variable

$$\zeta \in \partial D = \{w \in \mathbb{C} \mid |w| = r\},$$

da $f(\zeta)$ stetig von ζ abhängt. Aus der reellen Analysis wissen wir, dass gleichmäßig konvergente Reihen von Funktionen gliedweise integriert werden können. Somit erhalten wir

$$\oint_{|\zeta|=r} \frac{f(\zeta)}{\zeta - z}\, d\zeta = \sum_{k=0}^{\infty} \left(\oint_{|\zeta|=r} \frac{f(\zeta)}{\zeta^{k+1}}\, d\zeta \right) \cdot z^k$$

für alle $z \in D$, und die Behauptung folgt aus der Cauchy-Formel. □

Insbesondere ist jede holomorphe Funktion auf ihrem Definitionsbereich sogar unendlich oft komplex differenzierbar! Die Integralformel für die Koeffizienten ist für Abschätzungen hilfreich — beispielsweise für sogenannte *ganze Funktionen*, also Funktionen

$$f: \quad \mathbb{C} \longrightarrow \mathbb{C},$$

die auf der ganzen komplexen Ebene holomorph sind:

Korollar 5.3 (Satz von Liouville). *Jede beschränkte ganze Funktion ist konstant.*

Beweis. Jede ganze Funktion lässt sich auf der gesamten komplexen Ebene in eine Potenzreihe $f(z) = \sum_{k=0}^{\infty} a_k z^k$ entwickeln. Im Fall $c := \sup_{z \in \mathbb{C}} |f(z)| < \infty$ erhalten wir

$$|a_k| = \frac{1}{2\pi} \left| \oint_{|z|=r} \frac{f(\zeta)}{\zeta^{k+1}} d\zeta \right| \leq \frac{1}{2\pi} \cdot \frac{c}{r^{k+1}} \cdot 2\pi r = \frac{c}{r^k} \quad \text{für alle} \quad r > 0$$

aus der Cauchy-Formel. Im Grenzübergang $r \to \infty$ folgt $a_k = 0$ für alle $k > 0$. □

Dies liefert beispielsweise einen sehr einfachen Beweis für den Fundamentalsatz der Algebra durch Abschätzen des Wachstumsverhaltens von Polynomen:

Korollar 5.4. *Jedes Polynom $p(z) \in \mathbb{C}[z]$ vom Grad > 0 hat eine Nullstelle $z_0 \in \mathbb{C}$.*

Beweis. Für $p(z) = a_n z^n + a_{n-1} z^{n-1} + \cdots + a_0 = z^n \cdot (a_n + a_{n-1}/z + \cdots + a_0/z^n)$ mit $n > 0$ gilt

$$\lim_{|z| \to \infty} |p(z)| \; = \; \infty.$$

Wenn $p(z)$ keine Nullstelle hat, wäre also $f(z) = 1/p(z)$ eine beschränkte ganze Funktion und somit nach dem Satz von Liouville konstant, ein Widerspruch. □

Doch kommen wir zurück zum lokalen Verhalten holomorpher Funktionen. Wir beginnen mit einem lokalen Umkehrsatz:

Proposition 5.5. *Sei $f : U \to \mathbb{C}$ holomorph. Für $z_0 \in U$ sind äquivalent:*

a) Es ist $f'(z_0) \neq 0$.

b) Es gibt eine offene Umgebung $V \subseteq U$ von z_0, auf der sich f einschränkt zu einer Bijektion

$$f: \quad V \; \to \; W \; = \; f(V).$$

In diesem Fall ist auch die lokale Umkehrabbildung $g = f^{-1} : W \to V$ holomorph.

Beweis. Da jede holomorphe Funktion f sich lokal als Potenzreihe darstellen lässt, ist sie unendlich oft komplex differenzierbar, insbesondere *stetig* differenzierbar im reellen Sinn. Wir können daher den Satz über die lokale Umkehrabbildung aus der reellen Analysis anwenden: Wenn $f'(z_0) \neq 0$ ist, zeigt das kommutative Diagramm

$$\begin{array}{ccc} \mathbb{R}^2 & \xrightarrow{(Df)(z_0)} & \mathbb{R}^2 \\ \| & & \| \\ \mathbb{C} & \xrightarrow{w \mapsto f'(z_0) \cdot w} & \mathbb{C} \end{array}$$

dass die Jacobimatrix $(Df)(z_0) \in$ invertierbar ist. Nach dem Umkehrsatz ist dann f lokal invertierbar und die lokale Umkehrfunktion $g : W \to V$ ist ebenfalls stetig differenzierbar mit Jacobimatrix

$$(Dg)(f(z)) \; = \; ((Df)(z))^{-1}$$

für alle z in einer genügend kleinen Umgebung $V \subseteq U$ von z_0. Insbesondere ist diese Jacobimatrix ebenfalls gegeben durch die Multiplikation mit einer komplexen Zahl, nämlich mit dem Inversen $1/f'(z) \in \mathbb{C}$. Somit ist $g : W \to V$ holomorph.

Zu zeigen bleibt, dass umgekehrt f in keinem Punkt $z_0 \in U$ mit $f'(z_0) = 0$ lokal invertierbar ist. Man beachte, dass die analoge Aussage im Reellen nicht gilt, wie die glatte Bijektion $\mathbb{R} \to \mathbb{R}, x \mapsto x^3$ zeigt. Allerdings ist die Abbildung $\mathbb{C} \to \mathbb{C}, z \mapsto z^k$ für $k > 1$ in keiner Umgebung des Nullpunkts injektiv. Wir wollen zeigen, dass sich jede holomorphe Funktion lokal wie eine k-te Potenz verhält:

Wenn f in einer Umgebung von z_0 identisch verschwindet, ist nichts zu zeigen; wir dürfen daher annehmen, dass in der Potenzreihenentwicklung der Funktion um den Punkt z_0 nicht alle Koeffizienten Null sind. Indem wir von der Funktion eine Konstante abziehen, dürfen wir zudem $f(z_0) = 0$ annehmen. Wir haben dann eine lokale Entwicklung

$$f(z) \;=\; \sum_{n=k}^{\infty} a_n \cdot (z-z_0)^n \quad \text{beginnend bei einem Index } k \geq 1 \text{ mit } a_k \neq 0.$$

Durch Ausklammern der führenden Potenz erhalten wir eine lokale Darstellung von der Form

$$\begin{aligned} f(z) \;&=\; a_k \cdot (z-z_0)^k \cdot g(z) && \text{mit} \quad g(z_0) \;=\; 1 \\ &=\; \big(h(z)\big)^k && \text{mit} \quad h(z) \;:=\; c \cdot (z-z_0) \cdot \exp\big(\tfrac{1}{k}\operatorname{Log}(g(z))\big) \end{aligned}$$

für $|z-z_0|$ klein genug und $c \in \mathbb{C}$ mit $c^k = a_k$. Dabei ist

$$h'(z_0) \;=\; c \cdot \exp\big(\tfrac{1}{k}\operatorname{Log}(g(z_0))\big) \;=\; c \cdot \exp(0) \;=\; c \;\neq\; 0,$$

also ist h nach dem ersten Teil des Beweises auf einer kleinen Umgebung $V \subseteq U$ von z_0 bijektiv. Aus der Faktorisierung

$$f\colon \quad V \xrightarrow[\text{bijektiv}]{h} W \;=\; h(V) \xrightarrow{\;w \mapsto w^k\;} \mathbb{C}$$

erhalten wir die Äquivalenzen:

$$\begin{aligned} f \text{ ist im Punkt } z_0 \text{ lokal invertierbar} \quad &\Longleftrightarrow \quad \text{Die Abbildung } \mathbb{C} \to \mathbb{C}, w \mapsto w^k \\ &\qquad\quad \text{ist im Punkt 0 lokal invertierbar} \\ &\Longleftrightarrow \quad \text{Es ist } k = 1, \text{ d.h. } f'(z_0) \neq 0 \end{aligned}$$

Somit folgt die Behauptung. □

Definition 5.6. Eine *lokal biholomorphe Funktion* oder *konforme Abbildung* ist eine holomorphe Funktion

$$f\colon \quad U \longrightarrow \mathbb{C} \quad \text{mit} \quad f'(z) \;\neq\; 0 \quad \text{für alle} \quad z \in U.$$

Nach der obigen Proposition ist eine solche Funktion f in jedem Punkt $z \in U$ lokal invertierbar und die lokale Umkehrfunktion ist ebenfalls holomorph. Allgemeiner definieren wir die *Nullstellenordnung* einer holomorphen Funktion $f : U \to \mathbb{C}$ in einem Punkt $z_0 \in U$ durch

$$\operatorname{ord}_{z_0}(f) \;:=\; \min\{k \in \mathbb{N}_0 \mid f^{(k)}(z_0) \neq 0\} \;=\; \min\{k \in \mathbb{N}_0 \mid a_k \neq 0\}$$

für die lokale Potenzreihenentwicklung

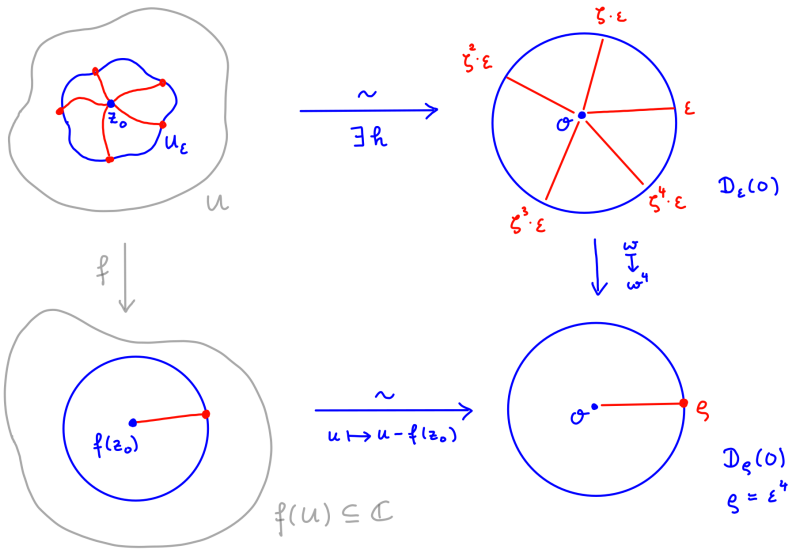
$$f(z) \;=\; \sum_{k=0}^{\infty} a_k \cdot (z-z_0)^k$$

Für die Nullfunktion $f=0$ setzen wir dabei formal $\operatorname{ord}_{z_0}(f) := \infty$.

Korollar 5.7. *Sei $f : U \to \mathbb{C}$ holomorph, $z_0 \in U$ und $k = \operatorname{ord}_{z_0}(f - f(z_0)) \in \mathbb{N}$. Für genügend kleines $\varepsilon > 0$ existieren*

- *eine Umgebung $U_\varepsilon \subseteq U$ von z_0,*
- *eine biholomorphe Abbildung $h : U_\varepsilon \xrightarrow{\sim} D_\varepsilon(0)$ mit $h(z_0) = 0$,*

sodass $f(z) - f(z_0) = (h(z))^k$ für alle $z \in U_\varepsilon$ gilt.



Beweis. In einer Umgebung von z_0 haben wir im Beweis von Proposition 5.5 eine Darstellung $f(z) - f(z_0) = (h(z))^k$ mit lokal biholomorphem h konstruiert. Hieraus folgt die Behauptung mit $U_\varepsilon := h^{-1}(D_\varepsilon(0))$ für $\varepsilon > 0$ klein genug. □

Wir erhalten, dass eine holomorphe Funktion bereits festgelegt ist durch ihre Werte auf einer beliebigen nicht diskreten Teilmenge ihres Definitionsbereiches:

Korollar 5.8 (Identitätssatz). *Es seien $f_1, f_2 : U \to \mathbb{C}$ holomorphe Funktionen auf einem Gebiet $U \subseteq \mathbb{C}$, und die Menge*

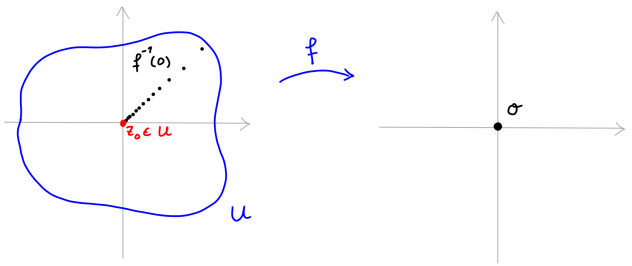
$$M \;=\; \big\{ z \in U \mid f_1(z) = f_2(z) \big\} \;\subseteq\; U$$

habe einen Häufungspunkt $z_0 \in U$. Dann gilt bereits $f_1(z) = f_2(z)$ für alle $z \in U$.

Beweis. Die Funktion $f : U \to \mathbb{C}, z \mapsto f_1(z) - f_2(z)$ ist holomorph. Wenn $z_0 \in U$ ein Häufungspunkt der Nullstellenmenge dieser Funktion ist, muß $\operatorname{ord}_{z_0}(f) = \infty$ gelten, da nach Korollar 5.7 die Nullstellen endlicher Ordnung diskret liegen. Dann ist f identisch Null in einer kleinen Umgebung des Punktes z_0. Wir haben damit gezeigt, dass die Menge

$$N := \left\{ z_0 \in U \mid \operatorname{ord}_{z_0}(f) = \infty \right\} \subseteq U$$

offen und nicht leer ist. Ihr Komplement ist aber ebenfalls offen: Jedes $z_0 \in U \setminus N$ hat nach Korollar 5.7 eine kleine punktierte Umgebung, in der f von Null verschieden ist und somit insbesondere endliche Nullstellenordnung hat. Somit haben wir das Gebiet $U = N \sqcup (U \setminus N)$ als disjunkte Vereinigung von zwei offenen Teilmengen geschrieben. Da Gebiete wegzusammenhängend sind und $N \neq \varnothing$ gilt, folgt $N = U$ und damit ist die Funktion f identisch Null. □



Bemerkung 5.9. Der Identitätssatz greift nur, wenn der Häufungspunkt z_0 in U liegt: Die Funktion

$$f : \quad U = \mathbb{C} \setminus \{0\} \longrightarrow \mathbb{C}, \quad z \mapsto \sin(\pi/z)$$

ist holomorph und nicht identisch Null. Sie hat jedoch Nullstellen in $z = 1/n$ für alle $n \in \mathbb{Z} \setminus \{0\}$, ihre Nullstellen häufen sich also im Nullpunkt $0 \in \mathbb{C} \setminus U$.

Eine Folge aus dem Identitätssatz ist, dass es in der komplexen Analysis keine Partitionen der Eins gibt. Aus algebraischer Sicht führt dies zu folgender schöner Eigenschaft:

Korollar 5.10. *Sei $U \subseteq \mathbb{C}$ ein Gebiet. Dann ist*

$$\mathcal{O}(U) := \left\{ \text{holomorphe Funktionen } f : U \to \mathbb{C} \right\} \quad \textit{ein Integritätsring.}$$

Beweis. Die Menge der holomorphen Funktionen ist ein kommutativer Ring mit der punktweisen Addition und Multiplikation; zu zeigen ist die Nullteilerfreiheit. Seien dazu $f_1, f_2 \in \mathcal{O}(U)$ mit $f_1 f_2 = 0$. Dann ist $U = f_1^{-1}(0) \cup f_2^{-1}(0)$. Mindestens eine der beiden Mengen $f_k^{-1}(0)$ muß also in U einen Häufungspunkt besitzen und es folgt $f_k = 0$ nach dem Identitätssatz. □

Eine weitere nützliche Anwendung der lokalen Darstellung von nicht konstanten holomorphen Funktionen ist die Beobachtung, dass sie offene Mengen auf offene Mengen abbilden:

Korollar 5.11 (Satz von der Gebietstreue). *Sei $U \subseteq \mathbb{C}$ ein Gebiet und $f : U \to \mathbb{C}$ eine nicht konstante holomorphe Funktion. Dann ist auch $f(U) \subseteq \mathbb{C}$ ein Gebiet.*

Beweis. Nach dem Identitätssatz wissen wir $\operatorname{ord}_{z_0}(f) < \infty$ für alle $z_0 \in U$. Dass das Bild $f(U) \subseteq \mathbb{C}$ offen ist, folgt daher aus der lokalen Darstellung als Potenzabbildung in Korollar 5.7. Als stetiges Bild einer wegzusammenhängenden Menge ist $f(U)$ wegzusammenhängend, denn für je zwei Punkte $f(z_0), f(z_1) \in f(U)$ wähle man einen Pfad $\gamma : [0,1] \to U$ mit $\gamma(0) = z_0$ und $\gamma(1) = z_1$, dann ist $f \circ \gamma : [0,1] \to f(U)$ ein Pfad, welcher die beiden Punkte verbindet. □

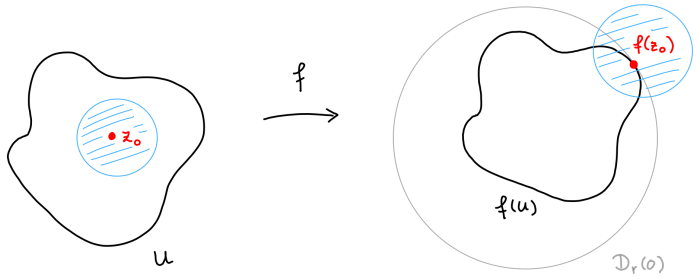
Als direkte Folgerung erhalten wir die wichtige Eigenschaft, dass holomorphe Funktionen im Innern ihres Definitionbereiches kein Betragsmaximum annehmen:

Korollar 5.12 (Maximumprinzip). *Sei $f : U \to \mathbb{C}$ eine nicht konstante holomorphe Funktion auf einem Gebiet. Dann nimmt die Funktion $|f| : U \to \mathbb{R}$, $z \mapsto |f(z)|$ auf dem Gebiet U kein Maximum an.*

Beweis. Sei $r := \sup_{z \in U} |f(z)|$. Wenn ein $z_0 \in U$ mit $|f(z_0)| = r$ existieren würde, dann wäre

$$f(z_0) \in \partial D \quad \text{ein Randpunkt der Kreisscheibe} \quad D := \{z \in \mathbb{C} \mid |z| < r\}$$

wie in der folgenden Skizze gezeigt:



Wegen $f(U) \subseteq \overline{D}$ könnte dann keine offene Umgebung von $f(z_0)$ im Bild $f(U)$ enthalten sein, dieses Bild wäre also nicht offen im Widerspruch zum Satz von der Gebietstreue. □

6 Singularitäten und Laurententwicklung

Bisher haben wir holomorphe Funktionen meist lokal auf offenen Kreisscheiben betrachtet; im Gegensatz dazu wollen wir nun holomorphe Funktionen studieren, die nur auf einer *punktierten* Kreisscheibe definiert sind, also auf einer Teilmenge der Form

$$\dot{D}_r(z_0) := D_r(z_0) \setminus \{z_0\}.$$

Wir interessieren uns dafür, wie sich solche Funktionen für $z \to z_0$ verhalten.

Definition 6.1. Sei $f : U \to \mathbb{C}$ eine holomorphe Funktion. Eine *isolierte Singularität* von f ist ein isolierter Punkt des Komplements $\mathbb{C} \setminus U$, d.h. ein $z_0 \in \mathbb{C}$ mit $\dot{D}_\varepsilon(z_0) \subseteq U$ für kleines $\varepsilon > 0$. Die Singularität heißt

a) *hebbar*, wenn f sich fortsetzt zu einer holomorphen Funktion $f : U \cup \{z_0\} \to \mathbb{C}$.

b) ein *Pol*, wenn $(z - z_0)^n f(z)$ für ein $n \in \mathbb{N}$ eine hebbare Singularität in z_0 hat.

c) eine *wesentliche Singularität*, wenn sie nicht hebbar und kein Pol ist.

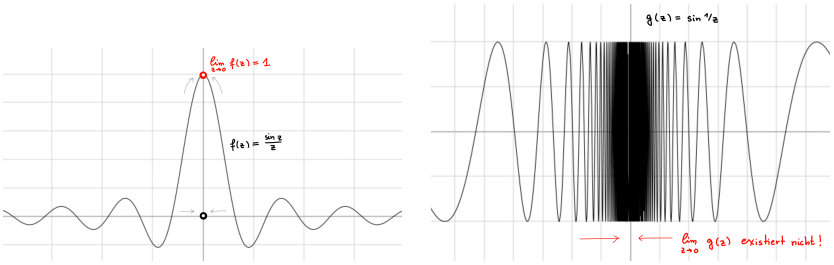
Beispiel 6.2. Falls $f : U \to \mathbb{C}$ in einem Punkt z_0 eine hebbare Singularität besitzt, dann ist die per Definition existierende holomorphe Fortsetzung $f : U \cup \{z_0\} \to \mathbb{C}$ aus Stetigkeitsgründen eindeutig bestimmt: Z.B. hat

$$f : \quad U = \mathbb{C} \setminus \{0\} \longrightarrow \mathbb{C}, \quad z \mapsto \frac{\sin z}{z}$$

im Punkt $z_0 = 0$ eine hebbare Singularität mit $f(0) = \lim_{z \to 0} \frac{\sin(z)}{z} = 1$, wie man aus der Potenzreihenentwicklung des Sinus sieht. Ein Beispiel für eine Funktion mit einer wesentlichen Singularität ist

$$g : \quad U = \mathbb{C} \setminus \{0\} \longrightarrow \mathbb{C}, \quad z \mapsto \sin(1/z).$$

Die Nullstellenmenge dieser Funktion besitzt einen Häufungspunkt im Punkt $z_0 = 0$; dasselbe gilt dann auch für $z^n \cdot g(z)$ für alle $n \in \mathbb{N}$. Nach dem Identitätssatz kann somit im Nullpunkt weder eine hebbare Singularität noch ein Pol vorliegen, d.h. der Nullpunkt ist eine wesentliche Singularität. Das folgende reelle Bild illustriert das Verhalten der Realteile der beiden Funktionen für reelle Werte $z \in \mathbb{R}$:



Als nächstes wollen wir Quotienten von holomorphen Funktionen $f, g : U \to \mathbb{C}$ betrachten, wobei g nicht die Nullfunktion sei. Die in U liegenden Singularitäten der Funktion f/g sind genau die Nullstellen des Nenners, also die Punkte $z_0 \in U$ mit $g(z_0) = 0$. Den Typ der Singularität kann man dabei an der Nullstellenordnung ablesen: Wir dürfen annehmen, dass f nicht die Nullfunktion ist, und schreiben auf einer Kreisscheibe $D_\varepsilon(z_0) \subseteq U$ die Funktionen als

$$\begin{aligned} f(z) &= (z-z_0)^m \cdot F(z) && \text{mit } m = \operatorname{ord}_{z_0}(f) \text{ und } F(z_0) \neq 0, \\ g(z) &= (z-z_0)^n \cdot G(z) && \text{mit } n = \operatorname{ord}_{z_0}(g) \text{ und } G(z_0) \neq 0. \end{aligned}$$

Durch Verkleinern von ε können wir $G(z) \neq 0$ für alle $z \in D_\varepsilon(z_0)$ erreichen. Dann folgt

$$\frac{f(z)}{g(z)} = (z-z_0)^{m-n} \cdot \frac{F(z)}{G(z)} \quad \text{für alle} \quad z \in \dot{D}_\varepsilon(z_0) = D_\varepsilon(z_0) \setminus \{z_0\}.$$

Da F/G eine auf ganz $D_\varepsilon(z_0)$ holomorphe Funktion ist, gibt es zwei Fälle:

a) Für $m \geq n$ ist z_0 eine hebbare Singularität von f/g, wir setzen dann

$$(f/g)(z_0) := \lim_{z \to z_0} f(z)/g(z) = \begin{cases} F(z_0)/G(z_0) & \text{für } m = n, \\ 0 & \text{für } m > n. \end{cases}$$

b) Für $m < n$ ist z_0 ein Pol von f/g. Wir setzen dann formal $(f/g)(z_0) := \infty$.

Dies führt auf den folgenden Begriff:

Definition 6.3. Eine *meromorphe Funktion* auf einer offenen Teilmenge $U \subseteq \mathbb{C}$ ist eine Abbildung

$$f: \quad U \longrightarrow \mathbb{C} \cup \{\infty\}$$

mit den folgenden Eigenschaften:

a) Die Menge $S := f^{-1}(\infty)$ ist diskret in U (nicht notwendig in $\mathbb{C}$).

b) Die Einschränkung $f|_{U_0} : U_0 = U \setminus S \longrightarrow \mathbb{C}$ ist holomorph.

c) In den Punkten $z_0 \in S$ hat die Funktion $f|_{U_0}$ Pole.

Die *Null- und Polstellenordnung* einer meromorphen Funktion $f : U \to \mathbb{C} \cup \{\infty\}$ in einem Punkt $z_0 \in U$ ist definiert als

$$\operatorname{ord}_{z_0}(f) := \sup \left\{ n \in \mathbb{Z} \mid (z-z_0)^{-n} f(z) \text{ hat eine hebbare Singularität in } z_0 \right\},$$

falls die Funktion nicht in einer gesamten Umgebung von z_0 verschwindet. Falls f in einer ganzen Umgebung von z_0 verschwindet, setzen wir $\operatorname{ord}_{z_0}(f) := \infty$.

Beispiel 6.4. Es gilt:

a) Jede holomorphe Funktion ist meromorph.

b) Der Quotient von zwei holomorphen Funktionen ist meromorph. Umgekehrt ist aus der Definition einer Polstelle klar, dass jede meromorphe Funktion $f : U \to \mathbb{C}$ sich *lokal* als Quotient von zwei holomorphen Funktionen schreiben lässt. Mit mehr Arbeit kann man zeigen, dass jede meromorphe Funktion sogar *global* ein Quotient von zwei holomorphen Funktionen auf U ist. Das ist nicht trivial, da meromorphe Funktionen unendlich viele Polstellen haben können:

c) Die Funktion $\tan : \mathbb{C} \to \mathbb{C} \cup \{\infty\}, z \mapsto \frac{\sin z}{\cos z}$ ist meromorph mit Polen in $\pi\mathbb{Z}$.

d) Man kann zeigen, dass durch

$$\Gamma : \quad H := \{z \in \mathbb{C} \mid \mathrm{Re}(z) > 0\} \longrightarrow \mathbb{C}, \quad z \mapsto \int_0^\infty t^{z-1} e^{-t} dt$$

eine holomorphe Funktion definiert wird und dass $\Gamma(z+1) = z\Gamma(z)$ für alle $z \in H$ gilt. Hieraus folgt

$$\Gamma(z) = \frac{\Gamma(z+n)}{z(z+1)\cdots(z+n-1)}$$

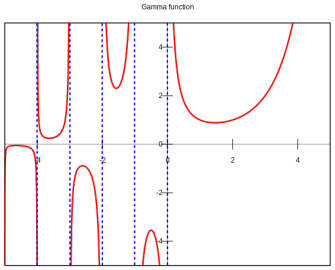
für alle $n \in \mathbb{N}$. Diese letzte Gleichung gilt zunächst nur für $z \in H$, die rechte Seite ist aber eine meromorphe Funktion auf ganz $H_n := \{z \in \mathbb{C} \mid \mathrm{Re}(z) > -n\}$. Wir haben damit die holomorphe Funktion $\Gamma : H \to \mathbb{C}$ zu einer meromorphen Funktion $\Gamma : H_n \to \mathbb{C} \cup \{\infty\}$ fortgesetzt, für beliebiges $n \in \mathbb{N}$. Insgesamt erhalten wir eine meromorphe Funktion

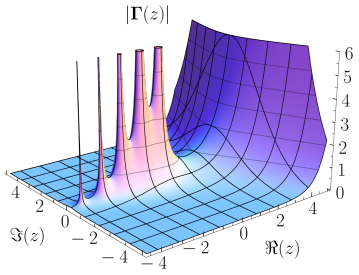
$$\Gamma : \quad \mathbb{C} \longrightarrow \mathbb{C} \cup \{\infty\}$$

mit einfachen Polen in $\{0, -1, -2, \dots\} \subset \mathbb{C}$, die sogenannte *Gammafunktion*. Sie interpoliert die Fakultätsfunktion auf den natürlichen Zahlen: Wegen $\Gamma(1) = 1$ ist

$$\Gamma(n+1) = n! \quad \text{für alle} \quad n \in \mathbb{N}.$$

Das folgenden Bilder zeigen $\mathrm{Re}(\Gamma(z))$ für $z \in \mathbb{R}$ und $|\Gamma(z)|$ für $z \in \mathbb{C}$:





Quelle: `https://en.wikipedia.org/wiki/Gamma_function`

Mit meromorphen Funktionen kann man ebenso rechnen wie mit holomorphen Funktionen: Z.B. ist die *Summe* zweier meromorpher Funktionen $f, g : U \to \mathbb{C} \cup \{\infty\}$ punktweise definiert. Ein wenig Vorsicht ist lediglich in den Polstellen geboten, da sich Pole der beiden Funktionen herauskürzen und somit eine hebbare Singularität auftreten könnte. Für $z_0 \in f^{-1}(\infty) \cup g^{-1}(\infty)$ definieren wir den Wert $(f+g)(z_0)$ durch

$$(f+g)(z_0) := \begin{cases} \lim_{z \to z_0} (f(z)+g(z)) & \text{falls dieser Limes existiert,} \\ \infty & \text{sonst.} \end{cases}$$

Man prüft leicht nach, dass die so definierte Summe $f+g : U \to \mathbb{C} \cup \{\infty\}$ wieder eine meromorphe Funktion ist. Analog definiert man das Produkt zweier meromorpher Funktionen. Aus dem Identitätssatz erhalten wir:

Bemerkung 6.5. Sei $U \subseteq \mathbb{C}$ ein Gebiet. Dann ist

$$\mathscr{M}(U) := \{\text{meromorphe Funktionen auf } U\} \quad \text{ein Körper.}$$

Die hier nicht bewiesene Aussage, dass jede meromorphe Funktion auf U sich als ein Quotient zweier holomorpher Funktionen darstellen lässt, können wir auch so fassen, dass $\mathscr{M}(U)$ der Quotientenkörper des Integritätsringes $\mathscr{O}(U)$ ist.

Holomorphe Funktionen können lokal um jeden Punkt ihres Definitionsbereichs als Potenzreihe entwickelt werden. Ebenso ist jede meromorphe Funktion lokal eine Summe einer Potenzreihe in $z - z_0$ und eines Polynoms in $1/(z-z_0)$. Wenn wir hier Polynome durch Potenzreihen ersetzen, können wir auch wesentliche Singularitäten beschreiben: Z.B. ist

$$\exp\left(\tfrac{1}{z}\right) = \sum_{n=0}^{\infty} \tfrac{1}{n!} \cdot \left(\tfrac{1}{z}\right)^n \quad \text{für alle} \quad z \in \mathbb{C} \setminus \{0\}.$$

Definition 6.6. Eine *Laurentreihe* um den Punkt $z_0 \in \mathbb{C}$ ist eine formale Potenzreihe der Form

$$\sum_{n=-\infty}^{\infty} a_n (z-z_0)^n \quad \text{mit} \quad a_n \in \mathbb{C}.$$

Wir fassen diese auf als Summe zweier verschiedener Potenzreihen:

$$\sum_{n=0}^{\infty} a_n (z-z_0)^n \quad \text{heißt } \textit{Nebenteil} \text{ der Laurentreihe,}$$

$$\sum_{n=1}^{\infty} a_{-n} \left(\tfrac{1}{z-z_0}\right)^n \quad \text{heißt } \textit{Hauptteil} \text{ der Laurentreihe.}$$

Wir sagen, die Laurentreihe *konvergiert* in einem Punkt $z \in \mathbb{C}$, wenn in diesem Punkt sowohl ihr Nebenteil als auch ihr Hauptteil (letzterer als Potenzreihe in $1/(z-z_0)$) konvergieren. In diesem Fall definieren wir den Wert der Potenzreihe als die Summe der Werte des Neben- und Hauptteils.

Lemma 6.7. *Für jede Laurentreihe um z_0 existieren $0 \le r \le R \le \infty$, sodass gilt:*

a) Die Reihe konvergiert in jedem Punkt des offenen Kreisrings

$$U \;:=\; \{z \in \mathbb{C} \mid r < |z - z_0| < R\} \;\subseteq\; \mathbb{C}$$

und stellt auf diesem offenen Kreisring eine holomorphe Funktion dar.

b) Die Reihe konvergiert in keinem $z \in \mathbb{C}$ mit $|z - z_0| < r$ oder $|z - z_0| > R$.

Beweis. Sei $\sum_{n=-\infty}^{\infty} a_n (z - z_0)^n$ die gegebene Laurentreihe. Die Behauptung folgt dann mit

$$R \;:=\; \text{Konvergenzradius der Potenzreihe } \sum_{n=0}^{\infty} a_n x^n,$$

$$\frac{1}{r} \;:=\; \text{Konvergenzradius der Potenzreihe } \sum_{n=1}^{\infty} a_{-n} y^n,$$

aus dem Konvergenzverhalten gewöhnlicher Potenzreihen. □

Jede holomorphe Funktion auf einem beliebigen Kreisring lässt sich dort in eine Laurentreihe entwickeln, und die Koeffizienten sind dabei eindeutig bestimmt:

Satz 6.8. *Sei $f : U = \{z \in \mathbb{C} \mid r < |z - z_0| < R\} \to \mathbb{C}$ eine holomorphe Funktion auf einem Kreisring. Dann wird die Funktion auf diesem Kreisring durch genau eine Laurentreihe*

$$f(z) \;=\; \sum_{n=-\infty}^{\infty} a_n (z - z_0)^n$$

dargestellt. Die Koeffizienten dieser Laurentreihe sind gegeben durch

$$a_n \;=\; \frac{1}{2\pi i} \oint_{|\zeta - z_0| = \rho} \frac{f(\zeta)}{(\zeta - z_0)^{n+1}}\, d\zeta \qquad \textit{für jedes } \rho \textit{ mit } r < \rho < R.$$

Beweis. OBdA sei $z_0 = 0$. Wenn in U eine Laurententwicklung $f(z) = \sum_{n=-\infty}^{\infty} a_n z^n$ existiert, dann dürfen wir für $k \in \mathbb{N}$ aufgrund der gleichmäßigen Konvergenz die Reihe

$$\frac{f(\zeta)}{\zeta^{k+1}} \;=\; \sum_{n=-\infty}^{\infty} a_n \zeta^{n-k-1}$$

gliedweise entlang $|\zeta| = \rho$ integrieren. Alle Terme mit $n \neq k$ besitzen aber eine Stammfunktion und tragen somit nichts zum Integral über einen geschlossenen Pfad bei. Somit folgt

$$\oint_{|\zeta| = \rho} \frac{f(\zeta)}{\zeta^{k+1}} d\zeta \;=\; \oint_{|\zeta| = \rho} a_k \zeta^{-1} d\zeta \;=\; 2\pi i a_k$$

und damit die behauptete Formel für die Koeffizienten und die Eindeutigkeit der Laurententwicklung auf dem gegebenen Kreisring.

Um die Existenz der Laurententwicklung zu zeigen, sei $z \in U$ gegeben. Für $\varepsilon > 0$ klein genug ist dann

$$\begin{aligned} f(z) &= \frac{1}{2\pi i} \oint_{|\zeta - z| = \varepsilon} \frac{f(\zeta)}{\zeta - z} d\zeta \\ &= \frac{1}{2\pi i} \oint_{|\zeta| = R - \varepsilon} \frac{f(\zeta)}{\zeta - z} d\zeta \; - \; \frac{1}{2\pi i} \oint_{|\zeta| = r + \varepsilon} \frac{f(\zeta)}{\zeta - z} d\zeta \end{aligned}$$

wobei die erste Gleichung die Cauchy-Formel und die zweite den Satz von Cauchy und die folgende Homotopie benutzt:

Durch Einsetzen der geometrischen Reihe

$$\frac{1}{\zeta - z} = \begin{cases} \frac{1}{\zeta} \sum_{k=0}^{\infty} \left(\frac{z}{\zeta} \right)^k & \text{für } |z| < |\zeta| = R - \varepsilon \\ -\frac{1}{z} \sum_{k=0}^{\infty} \left(\frac{\zeta}{z} \right)^k & \text{für } |z| > |\zeta| = r + \varepsilon \end{cases}$$

in den Integrand erhalten wir die gesuchte Laurententwicklung. □

Man beachte, dass die Eindeutigkeitsaussage des obigen Satzes nur für jeweils einen festen Kreisring gilt. Laurententwicklungen auf verschiedenen Kreisringen sehen im allgemeinen verschieden aus:

Beispiel 6.9. Die Funktion $f(z) = \frac{1}{1-z} - 1$ besitzt

- auf $\{0 < |z| < 1\}$ die Laurententwicklung $f(z) = \sum_{n=1}^{\infty} z^n$ mit Hauptteil Null,
- auf $\{1 < |z| < \infty\}$ die Laurententwicklung $f(z) = \sum_{n=1}^{\infty} z^{-n}$ mit Nebenteil Null.

Übungsaufgabe: Entwickeln Sie

$$g(z) = \frac{1}{z(z-1)(z-2)}$$

in eine Laurentreihe auf den drei die Pole vermeidenden Kreisringen in $\mathbb{C} \setminus \{0, 1, 2\}$.

Bemerkung 6.10. Für holomorphe Funktionen $f : U \to \mathbb{C}$ lässt sich der Typ einer isolierten Singularität z_0 an der Laurentreihe

$$f(z) \;=\; \sum_{n=-\infty}^{\infty} a_n (z-z_0)^n$$

um z_0 ablesen: Die Singularität ist

a) hebbar, wenn der Hauptteil Null ist, d.h. $a_n = 0$ für alle $n < 0$ gilt.

b) ein Pol, wenn der Hauptteil endlich ist, d.h. $a_n = 0$ für fast alle $n < 0$ gilt.

c) wesentlich, wenn $a_n \neq 0$ für unendlich viele $n < 0$ ist.

Das folgt direkt aus den Definitionen und der Eindeutigkeit der Laurententwicklung.

Ähnlich wie bei der Cauchy-Formel führt auch für Laurentreihen die Formel für die Koeffizienten zu nützlichen Abschätzungen:

Korollar 6.11 (Riemannscher Hebbarkeitssatz). *Sei $f : U \to \mathbb{C}$ eine holomorphe Funktion mit einer isolierten Singularität in einem Punkt z_0. Wenn die Funktion f in einer Umgebung $\dot{D}_\varepsilon(z_0) \subseteq U$ beschränkt ist, ist z_0 eine hebbare Singularität.*

Beweis. Sei $|f(z)| \leq c < \infty$ für alle $z \in \dot{D}_\varepsilon(z_0)$. Aus der Formel für die Koeffizienten der Laurentreihe

$$f(z) \;=\; \sum_{n=-\infty}^{\infty} a_n (z-z_0)^n \quad \text{für} \quad z \;\in\; \dot{D}_\varepsilon(z_0)$$

folgt $|a_n| \leq c \cdot \varepsilon^{-n}$ für alle $n \in \mathbb{Z}$. Für $n < 0$ und $\varepsilon \to 0$ erhalten wir $a_n = 0$. □

Wenn f in z_0 einen Pol hat, gilt andererseits $\lim_{z \to z_0} |f(z)| = \infty$, wie man durch Abschätzen des Hauptteils sieht. In der Nähe wesentlicher Singularitäten springt die Funktion wild:

Korollar 6.12 (Satz von Casorati-Weierstrass). *Sei $f : U \to \mathbb{C}$ eine holomorphe Funktion mit einer wesentlichen Singularität im Punkt z_0. Dann ist für jedes $\varepsilon > 0$ mit $\dot{D}_r(z_0) \subseteq U$ das Bild $f(\dot{D}_\varepsilon(z_0)) \subseteq \mathbb{C}$ eine dichte Teilmenge.*

Beweis. Wenn ein Punkt $w \in \mathbb{C}$ existiert, der nicht im Abschluß von $f(\dot{D}_\varepsilon(z_0))$ liegt, dann hat

$$g : \quad \dot{D}_\varepsilon(z_0) \;\longrightarrow\; \mathbb{C}, \quad g(z) \;:=\; \frac{1}{f(z)-w}$$

in z_0 eine hebbare Singularität nach dem Riemannschen Hebbarkeitssatz. Dann besitzt aber die Funktion $f(z) = w + 1/g(z)$ im Punkt z_0 einen Pol der Ordnung $\operatorname{ord}_{z_0}(1/g) = -\operatorname{ord}_{z_0}(g)$, also keine wesentliche Singularität. □

Es gilt sogar viel mehr: Wenn eine holomorphe Funktion in einem Punkt z_0 eine wesentliche Singularität besitzt, nimmt sie jeden komplexen Wert mit höchstens einer Ausnahme in jeder punktierten Umgebung von z_0 unendlich oft an. Dieser sogenannte *große Satz von Picard* ist aber schwieriger zu beweisen.

7 Der Residuensatz

Wir haben bei der Herleitung der Formel für die Koeffizienten von Laurentreihen benutzt, dass

$$\oint_{|z-z_0|=r} \frac{1}{(z-z_0)^k} dz \;=\; \begin{cases} 0 & \text{für } k \neq 1 \\ 2\pi i & \text{für } k = 1 \end{cases}$$

gilt. Wenn $f(z)$ eine holomorphe Funktion mit einer isolierten Singularität in einem Punkt z_0 ist, erhalten wir aus der Laurentreihe $f(z) = \sum_{n=-\infty}^{\infty} a_n (z-z_0)^n$ somit das Integral

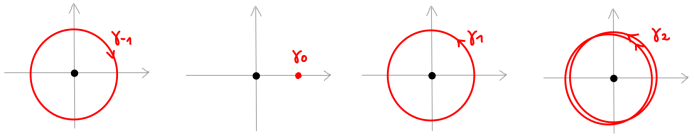
$$\oint_{|z-z_0|=r} f(z) dz \;=\; 2\pi i \cdot a_{-1}$$

für kleine $r > 0$. Das Pfadintegral über eine holomorphe Funktion entlang einer Kreislinie um eine isolierte Singularität kann man also bereits an einem einzigen Koeffizienten der Laurententwicklung ablesen!

Wenn man dies auf Integrale über beliebige geschlossene Kurven verallgemeinern will, muß man allerdings etwas aufpassen, da Pfade einen Punkt mehrfach oder in umgekehrter Orientierung umlaufen können:

Beispiel 7.1. Sei $k \in \mathbb{Z}$. Dann ist

$$\int_{\gamma_k} \frac{1}{z} dz \;=\; 2\pi i \cdot k \quad \text{für den geschlossenen Pfad} \quad \gamma_k : \quad [0,1] \to \mathbb{C},\; t \mapsto e^{2\pi i k t}.$$



Dies motiviert die folgende Definition:

Definition 7.2. Für einen geschlossenen Pfad $\gamma : [0,1] \to \mathbb{C}$ in der komplexen Ebene definieren wir die *Umlauf-* oder auch *Windungszahl* des Pfades um $a \in \mathbb{C} \setminus \gamma([0,1])$ durch

$$n(a,\gamma) \;:=\; \frac{1}{2\pi i} \int_\gamma \frac{1}{z-a} dz.$$

Wir sagen, dass der Pfad γ den Punkt a *umläuft*, wenn $n(a,\gamma) \neq 0$ ist.

Diese Definition ist geometrisch nicht sehr intuitiv. Bevor wir weitermachen, wollen wir uns überlegen, dass diese Definition auch wirklich Windungszahlen zählt und wie man diese konkret ausrechnen kann. Da jeder stetige Pfad homotop ist zu einem stückweise glatten Pfad, zeigt die folgende Proposition insbesondere, dass Windungszahlen immer ganzzahlig sind:

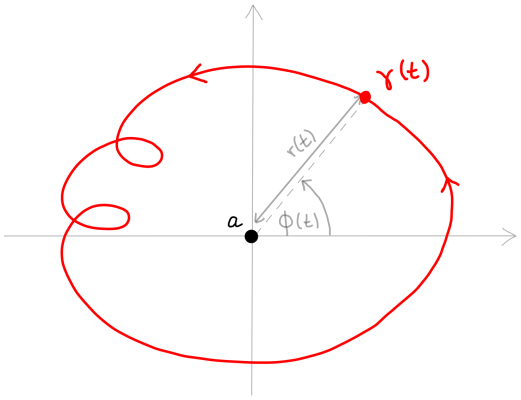
Proposition 7.3. *Sei $a \in \mathbb{C}$.*

a) Je zwei in $\mathbb{C} \setminus \{a\}$ homotope geschlossene Pfade $\gamma_1, \gamma_2 : [0,1] \to \mathbb{C} \setminus \{a\}$ haben die gleiche Windungszahl

$$n(a, \gamma_1) \;=\; n(a, \gamma_2).$$

b) Sei $\gamma : [0,1] \to \mathbb{C} \setminus \{a\}$ ein geschlossener Pfad der Form $\gamma(t) = a + r(t)\exp(i\phi(t))$ mit stetigen, stückweise glatten Funktionen $r : [0,1] \to \mathbb{R}_{>0}$, $\phi : [0,1] \to \mathbb{R}$. Dann ist die Windungszahl

$$n(a, \gamma) \;=\; \frac{\phi(1) - \phi(0)}{2\pi} \;\in\; \mathbb{Z}.$$

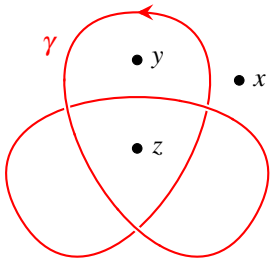


Beweis. Teil *a*) folgt sofort aus dem Satz von Cauchy. Für $\gamma(t) = a + r(t)\exp(i\phi(t))$ wie in *b*) berechnet man

$$\begin{aligned}
2\pi i \cdot n(a,\gamma) \;&=\; \int_\gamma \frac{1}{z-a}\,dz \\
&=\; \int_0^1 \frac{1}{r(t)\exp(i\phi(t))} \cdot \big(r'(t) + ir(t)\phi'(t)\big)\exp(i\phi(t))\,dt \\
&=\; \int_0^1 \Big(\tfrac{r'(t)}{r(t)} + i\cdot\phi'(t)\Big)\,dt \\
&=\; \Big[\log(r(t)) + i\cdot\phi(t)\Big]_{t=0}^{t=1} \\
&=\; i\cdot(\phi(1) - \phi(0)),
\end{aligned}$$

wobei wir im letzten Schritt $r(0) = r(1)$ benutzt haben. □

Beispiel 7.4. Der in der folgenden Skizze gezeigte Pfad $\gamma : [0,1] \to \mathbb{C}$ hat um die gegebenen Punkte x, y, z die Windungszahlen $0, 1, 2$:



$$n(x,\gamma) = 0$$
$$n(y,\gamma) = 1$$
$$n(z,\gamma) = 2$$

In diesem Beispiel besteht das Komplement des Bildes von γ aus vier Gebieten; die Windungszahl um einen Punkt hängt nur davon ab, in welchem der vier Gebiete der Punkt liegt, und die Menge aller Punkte mit von Null verschiedener Windungszahl ist beschränkt. Allgemein gilt:

Lemma 7.5. *Sei $\gamma : [0,1] \to \mathbb{C}$ ein geschlossener Pfad und $U := \mathbb{C} \setminus \gamma([0,1])$. Dann ist die Funktion*

$$n(-,\gamma): \quad U \longrightarrow \mathbb{Z}, \quad a \mapsto n(a,\gamma)$$

lokalkonstant und ihr Träger $\{a \in U \mid n(a,\gamma) \neq 0\} \subseteq \mathbb{C}$ ist eine beschränkte Menge.

Beweis. Da $1/(z-a)$ für $z \in \gamma([0,1])$ stetig von $a \in U$ abhängt, gilt dasselbe für das Integral

$$n(a,\gamma) \;=\; \frac{1}{2\pi i} \int_\gamma \frac{1}{z-a} dz.$$

Also ist $n(-,\gamma) : U \to \mathbb{Z}$ eine stetige Funktion. Da ihr Wertebereich $\mathbb{Z}$ diskret ist, muß die Funktion somit lokalkonstant sein. Zu zeigen bleibt, dass der Träger der Funktion beschränkt ist: Die Menge $\gamma([0,1])$ ist als stetiges Bild eines kompakten Intervalls kompakt und liegt somit in einer Kreisscheibe D vom Radius $R < \infty$. Die Umlaufzahl von γ um alle Punkte außerhalb der Kreisscheibe ist Null, da man γ im Innern von D zusammenziehen kann. □

Nach diesen allgemeinen Bemerkungen über Windungszahlen kommen wir nun zurück zu der Berechnung von Pfadintegralen. Wir erinnern zunächst daran, dass hierbei nur ein einziger Koeffizient der Laurentreihe eine Rolle spielt:

Definition 7.6. Sei f holomorph mit einer isolierten Singularität in einem Punkt z_0 und der Laurentreihe

$$f(z) \;=\; \sum_{n=-\infty}^{\infty} a_n (z-z_0)^n$$

um z_0. Dann heißt $\mathrm{Res}_{z_0}(f) := a_{-1}$ das *Residuum* der Funktion im Punkt z_0.

Das Residuum einer holomorphen Funktion in einer isolierten Singularität ist leicht auszurechnen, wir werden das gleich mit einigen Beispielen erklären. Der folgende Satz macht damit die Berechnung von Integralen über geschlossene Pfade zu einem Kinderspiel:

Satz 7.7 (Residuensatz). *Sei $U \subseteq \mathbb{C}$ ein Gebiet, und sei $f : U \setminus S \to \mathbb{C}$ holomorph auf dem Komplement einer endlichen Teilmenge $S \subset U$. Dann gilt*

$$\frac{1}{2\pi i} \int_\gamma f(z)\,dz \;=\; \sum_{a \in S} n(a,\gamma) \cdot \mathrm{Res}_a(f).$$

für jeden in U zusammenziehbaren geschlossenen Pfad $\gamma : [0,1] \to U \setminus S$.

Beweis. Für $a \in S$ sei

$$P_a(z) \;=\; \sum_{n=1}^{\infty} c_{-n,a} \cdot (z-a)^{-n} \quad \text{der Hauptteil der Laurentreihe von } f \text{ um } a.$$

Da die Funktion f in einer punktierten Umgebung der isolierten Singularität $a \in S$ holomorph ist, konvergiert ihre Laurentreihe auf einem Kreisring

$$\{z \in \mathbb{C} \mid r < |z-a| < R\} \quad \text{mit} \quad R \;>\; r \;=\; 0.$$

Für die Konvergenz des Hauptteils einer Laurentreihe ist nur der "innere" Radius des jeweiligen Kreisringes relevant, daher konvergiert in unserem Fall der Hauptteil für $|z| > r = 0$, also für alle $z \neq 0$. Daher ist $P_a(z)$ holomorph auf ganz $\mathbb{C} \setminus \{a\}$ und folglich ist

$$g(z) \;:=\; f(z) - \sum_{a \in S} P_a(z) \quad \text{holomorph auf} \quad U \setminus S.$$

Per Konstruktion verschwinden die Hauptteile der Laurententwicklung von g um alle $a \in S$ und somit ist g auch in allen Punkten $a \in S$ holomorph. Da der Pfad γ in U zusammenziehbar ist, erhalten wir aus dem Satz von Cauchy und der Definition von g dann

$$0 \;=\; \int_\gamma g(z)dz \;=\; \int_\gamma f(z)dz \;-\; \sum_{a \in S} \int_\gamma P_a(z)dz$$

Da die Funktion $z \mapsto (z-a)^{-n}$ für alle $n \neq -1$ eine holomorphe Stammfunktion hat, gilt dabei

$$\int_\gamma P_a(z) \;=\; \sum_{n=1}^{\infty} \int_\gamma \frac{c_{-n,a}}{(z-a)^n} dz \;=\; \int_\gamma \frac{c_{-1,a}}{z-a} dz \;=\; c_{-1,a} \cdot 2\pi i \cdot n(a,\gamma)$$

und mit $c_{-1,a} = \mathrm{Res}_a(f)$ folgt die Behauptung. □

Falls $S = \varnothing$ ist oder f in den Punkten aus S nur hebbare Singularitäten hat, ist die obige Aussage genau der Satz von Cauchy. Man kann den Residuensatz also als eine Verallgemeinerung des Satzes von Cauchy auf Funktionen mit isolierten Singularitäten auffassen. Um ihn anwenden zu können, stellen wir einige Regeln für das Berechnen von Residuen für Funktionen mit Polen zusammen:

Bemerkung 7.8. Seien $f, g : U \to \mathbb{C} \cup \{\infty\}$ meromorph. Für $z_0 \in U$ gilt dann:

a) Falls f im Punkt z_0 höchstens einen einfachen Pol hat, d.h. $\operatorname{ord}_{z_0}(f) \geq -1$ ist, gilt

$$\operatorname{Res}_{z_0}(f) \;=\; \lim_{z \to z_0} (z - z_0) f(z).$$

Allgemeiner sei $\operatorname{ord}_{z_0}(f) \geq -k$ für ein $k \in \mathbb{N}$. Dann ist

$$\operatorname{Res}_{z_0}(f) \;=\; \frac{1}{(k-1)!} \cdot h^{(k-1)}(z_0) \quad \text{mit} \quad h(z) \;:=\; (z - z_0)^k \cdot f(z).$$

b) Falls f holomorph und nicht identisch Null ist in einer Umgebung von z_0, dann gilt

$$\operatorname{Res}\left(\frac{f'}{f}\right) \;=\; \operatorname{ord}_{z_0}(f).$$

c) Falls f und g beide holomorph sind und die Nullstellenordnung $\operatorname{ord}_{z_0}(g) = 1$ ist, gilt

$$\operatorname{Res}_{z_0}\left(\frac{f}{g}\right) \;=\; \frac{f(z_0)}{g'(z_0)}$$

Der Beweis erhält man jeweils durch direktes Nachrechnen mit Potenzreihen. Mit den obigen Regeln lässt sich der Residuensatz sehr gut anwenden:

Beispiel 7.9. Die Funktion

$$f(z) \;:=\; \frac{1}{(z^2+1)^3}$$

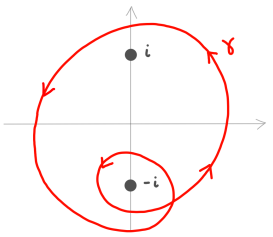
hat jeweils einen Pol der Ordnung drei in den Punkten $z_0 = \pm i$. Bemerkung 7.8 a) liefert

$$\operatorname{Res}_{\pm i}(f) \;=\; \frac{1}{2!} \cdot h''(\pm i) \;=\; \mp \frac{3i}{16} \qquad \text{mit} \quad h(z) \;:=\; \frac{1}{(z \pm i)^3}$$

Dasselbe hätte man natürlich auch durch Partialbruchzerlegung von $f(z)$ bekommen können. Der Residuensatz sagt hier

$$\int_\gamma \frac{1}{(z^2+1)^3} dz \;=\; -\frac{3i}{16} \cdot \Big(n(+i, \gamma) - n(-i, \gamma) \Big)$$

für jeden geschlossenen Pfad $\gamma : [0,1] \to \mathbb{C} \setminus \{\pm i\}$. In der folgenden Skizze gilt z.B.:



$$\int_\gamma \frac{1}{(z^2+1)^3} dz \;=\; -\frac{3i}{16} \cdot \big(n(i,\gamma) - n(-i,\gamma) \big) \;=\; \frac{3i}{16}$$

Beispiel 7.10. Die Funktion

$$h(z) := \frac{\cos \pi z}{\sin \pi z}$$

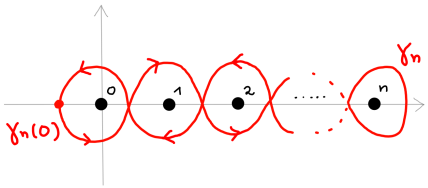
hat Pole genau in den ganzen Zahlen. Für ihr Residuum dort liefert Bemerkung 7.8 c) den Wert

$$\mathrm{Res}_a(h) = \frac{\cos \pi a}{\pi \cos \pi a} = \frac{1}{\pi} \quad \text{für} \quad a \in \mathbb{Z}.$$

Der Residuensatz sagt also

$$\int_\gamma h(z)dz = 2i \sum_{a \in \mathbb{Z}} n(a,\gamma) \quad \text{für jeden geschlossenen Pfad } \gamma : [0,1] \to \mathbb{C} \setminus \mathbb{Z}.$$

Man beachte, dass das Bild jedes solchen Pfades enthalten ist in einer beschränkten Teilmenge der komplexen Ebene, sodass nur endlich viele Pole beitragen. Für das Integrale über den Pfad γ_n in der folgenden Skizze erhalten wir beispielsweise:



$$\int_{\gamma_n} \frac{\cos \pi z}{\sin \pi z} dz = \begin{cases} 2i & \text{für } 2 \mid n \\ 0 & \text{für } 2 \nmid n \end{cases}$$

Das vorige Beispiel lässt sich wie folgt verallgemeinern zu einem Integral, das Null- und Polstellen zählt:

Korollar 7.11. *Sei $U \subseteq \mathbb{C}$ einfach zusammenhängend, sei $f : U \longrightarrow \mathbb{C} \cup \{\infty\}$ eine meromorphe Funktion, und sei $S \subset \mathbb{C}$ die Menge ihrer Null- und Polstellen. Dann gilt*

$$\frac{1}{2\pi i} \int_\gamma \frac{f'(z)}{f(z)} dz = \sum_{a \in S} n(a,\gamma) \cdot \mathrm{ord}_a(f)$$

für jeden geschlossenen Pfad $\gamma : [0,1] \to U \setminus S$.

Beweis. Folgt sofort aus dem Residuensatz und Bemerkung 7.8 b). □

Im Spezialfall des Integrals über den Rand einer Kreisscheibe $D = D_R(z_0) \subseteq U$ erhalten wir

$$\frac{1}{2\pi i} \oint_{|z-z_0|=R} \frac{f'(z)}{f(z)} dz = N_0(f,D) - N_\infty(f,D),$$

wobei $N_0(f,D)$ die Anzahl der Nullstellen und $N_\infty(f,D)$ die der Pole von f in D bezeichne, jeweils mit Vielfachheit der Null- bzw. Polstellen gezählt. Dies kann man benutzen, um zu prüfen, ob in einem gegebenen Gebiet Nullstellen liegen.

Der Residuensatz erlaubt auch eine einfache Berechnung von trigonometrischen Integralen, also Integralen über Funktionen von Sinus und Cosinus:

Korollar 7.12. *Sei $R = P/Q \in \mathbb{C}(x,y)$ eine rationale Funktion in zwei Variablen, also ein Quotient zweier von Null verschiedener Polynome $P,Q \in \mathbb{C}[x,y]$, und es gelte $Q(x,y) \neq 0$ für alle $(x,y) \in \mathbb{R}^2$ mit $x^2+y^2 = 1$. Dann ist*

$$\int_0^{2\pi} R(\cos t, \sin t)\, dt \;=\; 2\pi i \sum_{|a|<1} \operatorname{Res}_a(f),$$

wobei $f(z) \in \mathbb{C}(z)$ definiert sei durch

$$f(z) \;:=\; \frac{1}{iz} \cdot R\left(\tfrac{z+z^{-1}}{2},\, \tfrac{z-z^{-1}}{2i}\right).$$

Beweis. Per Definition der Funktion $f(z)$ gilt $R(\cos t, \sin t) = f(\exp(it)) \cdot i\exp(it)$, also ist

$$\int_0^{2\pi} R(\cos t, \sin t)\, dt \;=\; \oint_{|z|=1} f(z)dz$$

ein komplexes Pfadintegral. Die Behauptung folgt daher aus dem Residuensatz. □

Beispiel 7.13. Nach dem obigen Korollar ist

$$\int_0^{2\pi} \frac{1}{2+\cos t} dt \;=\; 2\pi i \sum_{|a|<1} \operatorname{Res}_a(f)$$

für die Funktion

$$f(z) \;:=\; \frac{1}{iz} \cdot \left(2 + \frac{z+z^{-1}}{2}\right)^{-1} \;=\; -\frac{4i}{z^2+4z+1} \;=\; -\frac{4i}{(z+2+\sqrt{3})(z+2-\sqrt{3})}$$

Der einzige im Einheitskreis liegende Pol von f ist $a = \sqrt{3}-2$. Da es sich um einen einfachen Pol handelt, ist

$$\operatorname{Res}_a(f) \;=\; \lim_{z\to a}(z-a)f(z) \;=\; -\frac{4i}{2\sqrt{3}} \;=\; -\frac{2i}{\sqrt{3}}.$$

nach Bemerkung 7.8 a). Wir erhalten somit

$$\int_0^{2\pi} \frac{1}{2+\cos t} dt \;=\; \frac{4\pi}{\sqrt{3}}.$$

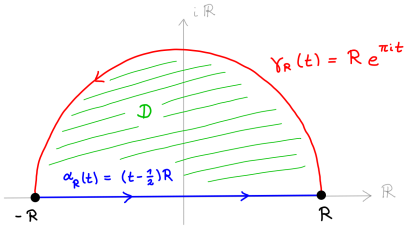
Eine besonders wichtige Anwendung des Residuensatzes ist die Berechnung von unbestimmten reellen Integralen

$$\int_{-\infty}^{\infty} f(x)dx := \int_{-\infty}^{0} f(x)dx + \int_{0}^{\infty} f(x)dx \quad \text{mit stetigen} \quad f: \quad \mathbb{R} \longrightarrow \mathbb{R}.$$

Ein solches Integral heißt *konvergent*, wenn jedes der beiden auf der rechten Seite stehenden unbestimmten Integrale endlich ist. Dann ist insbesondere

$$\int_{-\infty}^{\infty} f(x)dx = \lim_{R\to\infty} \int_{-R}^{R} f(x)dx.$$

Falls f sich fortsetzt zu einer meromorphen Funktion $f : \mathbb{C} \to \mathbb{C} \cup \{\infty\}$, können wir solche Integrale mit dem Residuensatz berechnen. Dazu betrachten wir die in der folgenden Skizze gezeigten Pfade:



Wenn $R > 0$ so gewählt wird, dass $\gamma_R : [0,1] \to \mathbb{C}, t \mapsto Re^{\pi it}$ keinen Pol von f trifft, sagt der Residuensatz

$$\int_{-R}^{R} f(x)dx + \int_{\gamma_R} f(z)dz = \sum_{a\in D} \operatorname{Res}_a(f) \quad \text{für} \quad D := \{z \in \mathbb{C} \mid \operatorname{Im}(z) > 0, |z| < R\}.$$

Wenn das Integral über γ_R für $R \to \infty$ gegen Null geht, erhalten wir das gesuchte reelle Integral. Ein Beispiel hierfür liefern rationale Funktionen:

Korollar 7.14. *Seien $P, Q \in \mathbb{C}[z]$ Polynome mit $\deg(Q) \geq \deg(P) + 2$, und Q habe keine reellen Nullstellen. Dann gilt*

$$\int_{-\infty}^{\infty} \frac{P(x)}{Q(x)}dx = 2\pi i \sum_{\operatorname{Im}(a)>0} \operatorname{Res}_a\left(\frac{P}{Q}\right).$$

Beweis. Wegen $\deg(Q) \geq \deg(P) + 2$ existiert ein $c \in \mathbb{R}$ mit $|P(z)/Q(z)| \leq c \cdot |z|^{-2}$ für $|z| \gg 0$ groß genug. Also ist

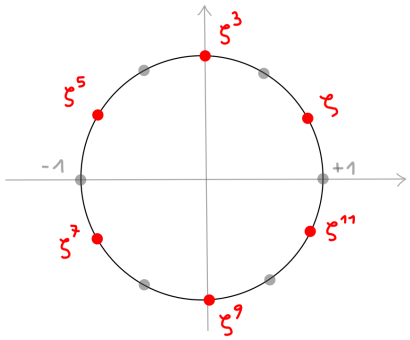
$$\lim_{R\to\infty} \int_{\gamma_R} \frac{P(z)}{Q(z)}dz = 0$$

und die Behauptung folgt wie beschrieben aus dem Residuensatz. □

Beispiel 7.15. Nach dem vorigen Korollar ist

$$\int_0^\infty \frac{1}{1+x^6}dx \;=\; \frac{1}{2}\int_{-\infty}^{\infty} \frac{1}{1+x^6}dx \;=\; \pi i \sum_{\mathrm{Im}(a)>0} \mathrm{Res}_a\left(\frac{1}{1+z^6}\right).$$

Die in der oberen Halbebene liegenden Nullstellen von $Q(z) = 1+z^6$ sind genau die Zahlen $a = \zeta, \zeta^3, \zeta^5$ mit $\zeta = \exp(\pi i/6)$:



Die Residuen dort sind nach Bemerkung 7.8 c)

$$\mathrm{Res}_a\left(\frac{1}{Q}\right) \;=\; \frac{1}{Q'(a)} \;=\; \frac{1}{6\cdot a^5} \;=\; -\frac{a}{6} \quad \text{wegen} \quad \zeta^6 \;=\; -1.$$

Wir erhalten daher

$$\int_0^\infty \frac{1}{1+x^6} \;=\; -\frac{\pi i}{6}\cdot\left(\zeta+\zeta^3+\zeta^5\right) \;=\; \frac{\pi}{3}.$$

8 Ausblick: Riemannsche Flächen

Die komplexe Analysis hätte viele weitere interessante Themen zu bieten, die aber den engen zeitlichen Rahmen dieser Vorlesung sprengen würden. Wir wollen uns hier begnügen mit einem kurzen Ausblick auf die Theorie Riemannscher Flächen und ihren Bezug zur Galoistheorie. Wie in der reellen Analysis kann man auch in der komplexen Analysis Mannigfaltigkeiten betrachten, wobei man fordert, dass die Kartenwechsel nicht nur glatt, sondern sogar holomorph sind; da wir hier nur holomorphe Funktionen in einer Variablen betrachtet haben, beschränken wir uns auf komplex eindimensionale Mannigfaltigkeiten:

Definition 8.1. Sei S ein topologischer Raum. Eine *komplexe Karte* auf S ist ein Homöomorphismus

$$\varphi: \quad U \xrightarrow{\sim} V$$

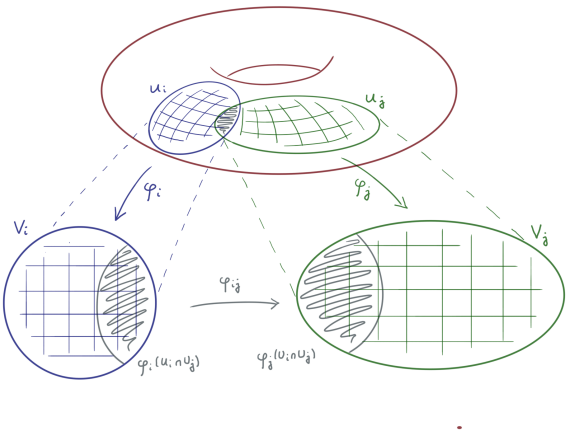
zwischen offenen Mengen $U \subseteq S$ und $V \subseteq \mathbb{C}$. Ein *(komplexer) Atlas* auf S ist eine Familie von Karten

$$\varphi_i : \quad U_i \xrightarrow{\sim} V_i \subseteq \mathbb{C} \quad \text{zu einer offenen Überdeckung} \quad S = \bigcup_{i \in I} U_i,$$

wobei wir fordern, dass die Karten miteinander *kompatibel* sind in dem Sinn, dass die Kartenwechsel

$$\varphi_{ij} = \varphi_j \circ \varphi_i^{-1} : \quad \varphi_i(U_i \cap U_j) \xrightarrow{\sim} \varphi_j(U_i \cap U_j)$$

auf dem Schnitt von je zwei Karten biholomorph sind:



Zwei Atlanten heißen *äquivalent*, wenn ihre Vereinigung wieder ein Atlas ist, d.h. wenn alle Karten des ersten Atlas mit allen Karten des zweiten Atlas kompatibel sind. Jede Äquivalenzklasse von Atlanten enthält genau einen maximalen Atlas; eine *Riemannsche Fläche* ist ein Hausdorffscher zusammenhängender topologischer Raum S zusammen mit einem maximalen Atlas.

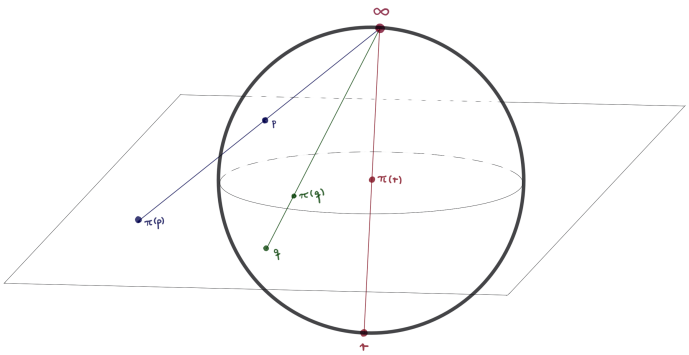
Beispiel 8.2. Es gilt:

a) Jedes Gebiet $S = U \subseteq \mathbb{C}$ ist eine Riemannsche Fläche. Wir können hier den aus nur einer Karte mit der identischen Abbildung bestehenden Atlas nehmen.

b) Die Einheitssphäre $S = \{(x,y,z) \in \mathbb{R}^3 \mid x^2+y^2+z^2 = 1\}$ trägt die Struktur einer Riemannschen Fläche. Wir wählen einen Atlas zur Überdeckung durch folgende zwei offene Teilmengen:

- Das Komplement $U_0 = S \setminus \{\infty\}$ des Nordpols $\infty := (0,0,1)$,
- Das Komplement $U_\infty = S \setminus \{0\}$ des Südpols $0 := (0,0,-1)$.

Die Karte $\varphi_0 : U_0 \xrightarrow{\sim} V_0 = \mathbb{C}$ definieren wir durch stereographische Projektion vom Nordpol wie in der folgenden Skizze gezeigt:



Für die Karte $\varphi_\infty : U_\infty \xrightarrow{\sim} V_\infty = \mathbb{C}$ nehmen wir das komplex Konjugierte der stereographischen Projektion vom Südpol. In Formeln:

$$\varphi_0(x,y,z) \;=\; \frac{x+iy}{1-z} \quad \text{und} \quad \varphi_\infty(x,y,z) \;=\; \frac{x-iy}{1+z}.$$

Der Kartenwechsel ist holomorph: Für $u = \varphi_0(x,y,z) = \frac{x+iy}{1-z} \in \varphi_0(U_0 \cap U_\infty) = \mathbb{C}^\times$ berechnet man

$$\begin{aligned}\varphi_\infty(\varphi_0^{-1}(u)) \;=\; \varphi_\infty(x,y,z) \;=\; \frac{x-iy}{1+z} \;=\; \frac{x^2+y^2}{(x+iy)(1+z)} \;&=\; \frac{1-z^2}{(x+iy)(1+z)} \\ &=\; \frac{1-z}{x-iy} \;=\; 1/u,\end{aligned}$$

der Kartenwechsel ist also

$$\varphi_{0\infty}: \quad \mathbb{C}^\times \;=\; \varphi_0(U_0 \cap U_\infty) \;\xrightarrow{\sim}\; \mathbb{C}^\times \;=\; \varphi_\infty(U_0 \cap U_\infty), \quad u \mapsto 1/u.$$

Wir nennen die so erhaltene Riemannsche Fläche die *Riemannsche Zahlkugel* und schreiben

$$S \;=\; \mathbb{C} \cup \{\infty\} \;=\; \mathbb{P}^1(\mathbb{C}),$$

wobei die Inklusion $\mathbb{C} \hookrightarrow \mathbb{P}^1(\mathbb{C})$ sich auf die erste Karte φ_0 bezieht.

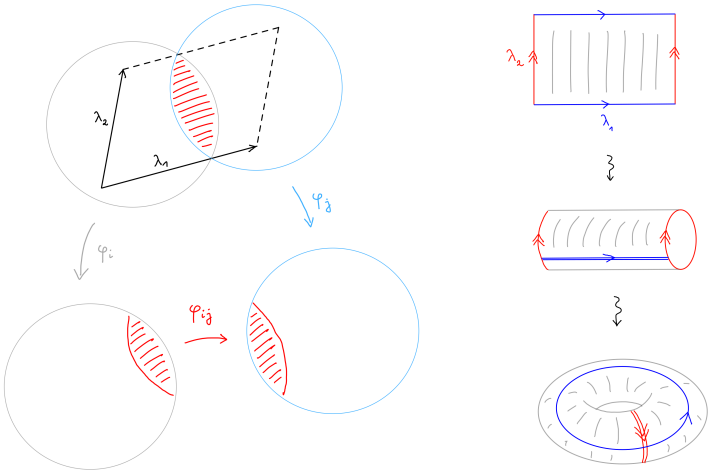
c) Sei $\Lambda = \mathbb{Z}\lambda_1 \oplus \mathbb{Z}\lambda_2 \subseteq \mathbb{C}$ ein *Gitter*, d.h. eine von zwei $\mathbb{R}$-linear unabhängigen Vektoren aufgespannte additive Untergruppe der komplexen Ebene. Dann trägt die Quotientengruppe

$$E \;:=\; \mathbb{C}/\Lambda$$

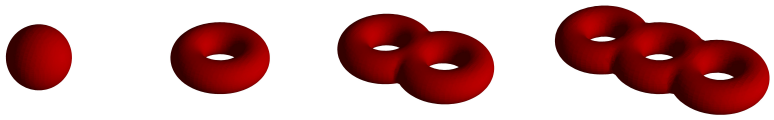
eine Struktur einer Riemannschen Fläche: Sei $0 < \varepsilon < \min\{|\lambda_1|/2, |\lambda_2|/2\}$. Für jedes $z_0 \in \mathbb{C}$ ist die Abbildung

$$V_{z_0} \;:=\; \{z \in \mathbb{C} \mid |z - z_0| < \varepsilon\} \;\xrightarrow{\sim}\; U_{z_0} \;:=\; \{z \mod \Lambda \mid z \in V_{z_0}\}$$

bijektiv, definiert also eine komplexe Karte; die Kartenwechsel sind hier eine Verschiebung in der komplexen Ebene, also biholomorph. Riemannsche Flächen dieser Form heißen *elliptische Kurven*. Als topologischer Raum sind sie alle homöomorph zu einem Torus:



d) Allgemeiner kann man zeigen, dass die kompakten Riemannschen Flächen als reelle Mannigfaltigkeiten genau die kompakten orientierbaren Flächen im Sinn der reellen Analysis sind:



Die Orientierbarkeit folgt daraus, dass biholomorphe Abbildungen wegen der Cauchy-Riemann DGL orientierungserhaltend sind.

Die Topologie kompakter Riemannscher Flächen ist damit geklärt; die komplexe Analysis ist aber viel reichhaltiger! Um sagen zu können, wann zwei Riemannsche Flächen nicht nur als topologische Räume, sondern auch aus Sicht der komplexen Analysis gleich aussehen, benötigen wir einige weitere Begriffe:

Definition 8.3. Sei S eine Riemannsche Fläche und $U \subseteq S$ eine offene Teilmenge; eine Funktion $f : U \to \mathbb{C}$ heißt *holomorph*, wenn für jede in einem gegebenen Atlas der Riemannschen Fläche enthaltene Karte $\varphi_i : U_i \xrightarrow{\sim} V_i$ von $U_i \subseteq S$ nach $V_i \subseteq \mathbb{C}$ die Funktion

$$f \circ \varphi^{-1} : \quad \varphi^{-1}(U \cap U_i) \longrightarrow \mathbb{C}$$

holomorph ist. Eine Abbildung $p : X \to S$ zwischen zwei Riemannschen Flächen heißt *holomorph* oder ein *Morphismus von Riemannschen Flächen*, wenn für jede

Karte $\varphi_i : U_i \to V_i$ von S die Funktion $p^{-1}(U_i) \longrightarrow V_i$ holomorph ist. Ein bijektiver Morphismus von Riemannschen Flächen heißt *Isomorphismus* oder *biholomorph*; die beiden Riemannschen Flächen heißen dann zueinander isomorph.

Beispiel 8.4. Es gilt:

a) Sei $U \subseteq \mathbb{C}$ ein Gebiet. Dann haben wir eine Bijektion

$$\mathscr{M}(U) := \{\text{meromorphe Funktionen auf } U\} \xrightarrow{\sim} \{\text{Morphismen } f : U \to \mathbb{P}^1(\mathbb{C})\}$$

wobei wir für $f \in \mathscr{M}(U)$ den Wert $f(x) = \infty$ setzen, falls f einen Pol in x hat.

b) Unter einer *meromorphen Funktion* auf einer Riemannschen Fläche X verstehen wir einen Morphismus $f : X \to \mathbb{P}^1(\mathbb{C})$. Wie in der komplexen Ebene sieht man, dass die Menge der meromorphen Funktionen einen Körper $\mathscr{M}(X)$ bildet, der sogenannte *Funktionenkörper* von X. Beispielsweise ist

$$\mathscr{M}(\mathbb{P}^1(\mathbb{C})) \simeq \mathbb{C}(x)$$

der Körper der rationalen Funktionen in einer Variablen x (Übungsaufgabe).

c) Sei $\Lambda \subset \mathbb{C}$ ein Gitter. Dann ist die Quotientenabbildung

$$\mathbb{C} \to \mathbb{C}/\Lambda \quad \text{ein Morphismus von Riemannschen Flächen.}$$

Die lokale Beschreibung holomorpher Funktionen führt zu der folgenden lokalen Beschreibung von Morphismen Riemannscher Flächen:

Lemma 8.5. *Sei $f : Y \to X$ ein Morphismus von Riemannschen Flächen. Dann existieren für jeden Punkt $p \in Y$ offene Umgebungen $V \subseteq Y$ von p und $U \subseteq X$ von $q = f(p)$ sowie Karten*

$$\begin{aligned} \psi: &\quad V \xrightarrow{\sim} D \quad \textit{mit} \quad \psi(p) = 0, \\ \varphi: &\quad U \xrightarrow{\sim} D \quad \textit{mit} \quad \varphi(q) = 0, \end{aligned}$$

sodass das folgende Diagramm kommutiert:

$$\begin{array}{ccccc} Y & \longleftarrow & V & \xrightarrow[\sim]{\psi_p} & D \\ {\scriptstyle f}\downarrow & & \downarrow & & \downarrow{\scriptstyle z\mapsto z^{e_p}} \\ X & \longleftarrow & U & \xrightarrow[\sim]{\phi} & D \end{array}$$

Dabei ist $e_p \in \mathbb{N}_0$ eindeutig bestimmt und heißt Verzweigungsindex *von f in p.*

Beweis. Durch Übergang zu Karten folgt dies aus dem lokalen Abbildungsverhalten holomorpher Funktionen in Korollar 5.7. □

Die obige Beschreibung gilt zunächst nur lokal in einer Umgebung eines Punktes im Definitionsbereich. Für eine Beschreibung auf dem vollen Urbild $f^{-1}(U)$ einer Umgebung $U \subseteq X$ benötigen wir eine weitere Eigenschaft, die es uns z.B. verbietet, willkürlich Punkte aus dem Definitionsbereich herauszunehmen:

Definition 8.6. Eine stetige Abbildung $f : Y \to X$ lokalkompakter Hausdorffscher Räumen heißt *eigentlich*, wenn für jede kompakte Menge $K \subseteq X$ das Urbild $f^{-1}(K)$ kompakt ist (dies ist z.B. automatisch, wenn Y kompakt ist).

Proposition 8.7. *Es sei $f : Y \to X$ ein nicht konstanter eigentlicher Morphismus von Riemannschen Flächen. Dann hat jedes $q \in X$ eine offene Umgebung $U \subseteq X$, deren Urbild eine disjunkte Vereinigung*

$$f^{-1}(U) \;=\; \bigsqcup_{p \in f^{-1}(q)} V_p$$

offener Teilmengen $V_p \subseteq Y$ ist, sodass Karten

$$\begin{aligned} \psi_p : &\quad V_p \xrightarrow{\sim} D \quad \textit{mit} \quad \psi_p(p) = 0, \\ \varphi : &\quad U \xrightarrow{\sim} D \quad \textit{mit} \quad \varphi(q) = 0, \end{aligned}$$

existieren, welche das folgende Diagramm kommutativ machen:

$$\begin{array}{ccccc} Y & \hookleftarrow & V_p & \xrightarrow[\sim]{\psi_p} & D \\ \downarrow & & \downarrow & & \downarrow{\scriptstyle z \mapsto z^{e_p}} \\ X & \hookleftarrow & U & \xrightarrow[\sim]{\varphi} & D \end{array}$$

Insbesondere ist der Grad $\deg(f) := \sum_{p \in f^{-1}(q)} e_p$ *unabhängig vom Punkt $q \in X$.*

Beweis. Für $q \in X$ ist die Faser $f^{-1}(q) \subset Y$ nach dem Identitätssatz eine diskrete Teilmenge. Da f eigentlich ist, muß diese Faser aber zugleich kompakt sein, besteht also nur aus endlich vielen Punkten. Wir können um jeden dieser Punkte $p \in f^{-1}(q)$ eine Umgebung V_p mit den Eigenschaften aus Lemma 8.5 finden. Da es nur um endlich viele Punkte geht, können wir zudem erreichen, dass alle diese Umgebungen das gleiche Bild $U = f(V_p) \subseteq X$ besitzen. Dann ist $\sqcup_{p \in f^{-1}(q)} V_p \subseteq f^{-1}(U)$, und da f eigentlich ist, muß hier sogar Gleichheit gelten, da sie per Konstruktion für die Faser über dem Punkt q gilt (die Details seien als Übungsaufgabe überlassen). □

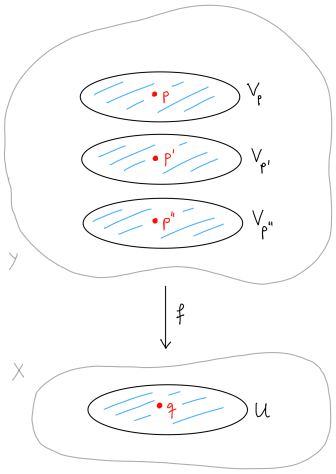
Wir bezeichnen einen nicht konstanten eigentlichen Morphismus $f : Y \to X$ von Riemannschen Flächen auch als *verzweigte Überlagerung*. Im Fall, dass $e_p = 1$ für alle $p \in Y$ gilt, handelt es sich um eine unverzweigte Überlagerung:

Definition 8.8. Eine stetige Abbildung $f : Y \to X$ von topologischen Räumen heißt eine *unverzweigte Überlagerung*, wenn sie die folgende Eigenschaft besitzt: Für jedes $q \in X$ gibt es eine Umgebung $U \subseteq X$ von q, sodass ihr Urbild eine disjunkte Vereinigung

$$f^{-1}(U) \;=\; \bigsqcup_{p \in f^{-1}(q)} V_p$$

offener Teilmengen $V_p \subseteq Y$ ist, auf denen die Abbildung f sich einschränkt zu einem Homöomorphismus

$$f : \quad V_p \xrightarrow{\sim} U.$$



Die Überlagerung heißt *endlich*, wenn $|f^{-1}(q)| < \infty$ ist für alle $q \in X$.

Aus Proposition 8.7 folgt, dass jede verzweigte Überlagerung $f : Y \to X$ von Riemannschen Flächen sich über dem Komplement der endlichen Menge

$$S := \{f(p) \in X \mid e_p > 1\} \subset X$$

zu einer unverzweigten Überlagerung einschränkt. Wir können umgekehrt auch neue Riemannsche Flächen auf diese Weise *konstruieren*:

Proposition 8.9. *Sei X eine Riemannsche Fläche, und es sei $S \subset X$ eine diskrete Menge von Punkten. Sei Y_0 ein topologischer Raum, und es sei eine unverzweigte endliche Überlagerung*

$$f_0 : \quad Y_0 \longrightarrow X_0 = X \setminus S$$

gegeben. Dann existiert bis auf Isomorphismus genau eine Riemannsche Fläche Y mit einer Einbettung $Y_0 \hookrightarrow Y$ als offene Teilmenge und einer Fortsetzung von f_0 zu einer verzweigten Überlagerung $f : Y \to X$.

Beweis. Da $f_0 : Y_0 \to X_0$ als unverzweigte Überlagerung insbesondere ein lokaler Homöomorphismus ist, existiert genau eine Struktur einer Riemannschen Fläche auf Y_0, sodass f_0 ein Morphismus Riemannscher Flächen wird.

Wir wählen nun für jeden der Punkte $q \in S$ eine offene Umgebung $U \subseteq X$ mit einer Karte

$$\varphi : \quad U \xrightarrow{\sim} D := \{z \in \mathbb{C} \mid |z| < 1\} \quad \text{mit} \quad \varphi(q) = 0.$$

Dann ist

$$\varphi \circ f_0 : \quad f_0^{-1}(U \setminus \{q\}) \longrightarrow U \setminus \{q\} \xrightarrow{\sim} \dot{D} := D \setminus \{0\}$$

eine unverzweigte Überlagerung der punktierten Kreisscheibe. In der Topologie zeigt man, dass jede unverzweigte zusammenhängende Überlagerung von $\dot{D}$ von der Form

$$\dot{D} \longrightarrow \dot{D}, \quad z \mapsto z^e$$

mit $e \in \mathbb{N}$ ist, sich also ausdehnt zur verzweigten Überlagerung $D \to D, z \mapsto z^e$. Durch Einkleben endlich vieler Kreisscheiben können wir also die ursprünglich gegebene unverzweigte Überlagerung $f_0^{-1}(U \setminus q) \to U \setminus \{q\}$ fortsetzen zu einer verzweigten Überlagerung von U. Indem wir dies für jeden der Punkte $q \in S$ machen, erhalten wir die gewünschte Fortsetzung $f : Y \to X$. □

Beispiel 8.10. Sei $f \in \mathbb{C}[x,y]$ ein irreduzibles Polynom mit $\partial f/\partial y \not\equiv 0$. Wir betrachten die Nullstellenmenge

$$Z := \{p \in \mathbb{C}^2 \mid f(p) = 0\} \subset \mathbb{C}^2.$$

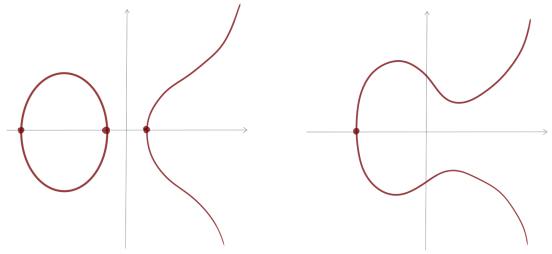
Der Satz über implizite Funktionen zeigt, dass die Projektion $pr_1 : Z \to \mathbb{C}, (x,y) \mapsto x$ in jedem Punkt $p \in Z$ mit $(\partial f/\partial y)(p) \neq 0$ ein lokaler Diffeomorphismus ist. Es sei nun

$$S := \{pr_1(p) \mid p \in Z, (\partial f/\partial y)(p) = 0\} \cup \{\infty\} \subset X := \mathbb{P}^1(\mathbb{C}).$$

Proposition 8.9 lässt sich auf $f_0 : Y_0 := Z \setminus pr^{-1}(S) \longrightarrow X_0 := X \setminus S$ anwenden und liefert eine kompakte Riemannsche Fläche mit einer verzweigten Überlagerung

$$f : \quad Y \longrightarrow X = \mathbb{P}^1(\mathbb{C}).$$

Wir nennen Y die Riemannsche Fläche zur algebraischen Kurve $f(x,y) = 0$.



Man kann zeigen:

- Für die Funktionenkörper gilt $\mathscr{M}(Y) \simeq \mathbb{C}(x)[y]/(f) \supseteq \mathscr{M}(X) = \mathbb{C}(x)$.
- Jede kompakte Riemannsche Fläche entsteht so. In dieser Aussage steckt aber echte Analysis: Um zu sehen, dass für jede kompakte Riemannsche Fläche ein nicht konstanter Morphismus zu $\mathbb{P}^1(\mathbb{C})$ existiert, muß man eine nicht konstante meromorphe Funktion konstruieren!

Tatsächlich erhalten wir eine Äquivalenz von Kategorien

$$\{\text{verzweigte Überlagerungen von } \mathbb{P}^1(\mathbb{C})\} \xrightarrow{\sim} \{\text{endliche Erweiterungen von } \mathbb{C}(x)\}$$

Damit können wir die in der Algebra entwickelte Galoiskorrespondenz anwenden, um verzweigte Überlagerungen kompakter Riemannscher Flächen zu studieren:

Definition 8.11. Sei $f : Z \to X$ eine verzweigte Überlagerung. Ein *Automorphismus* der Überlagerung ist ein biholomorpher Morphismus $\varphi : Z \to Z$ mit $f \circ \varphi = f$. Die Gruppe

$$\mathrm{Aut}(Z/X) := \{\varphi : Z \xrightarrow{\sim} Z \mid f \circ \varphi = f\}$$

heißt *Automorphismengruppe* der Überlagerung.

Satz 8.12 (Galoiskorrespondenz für Riemannsche Flächen). *Es sei $f : Z \longrightarrow X$ eine endliche verzweigte Überlagerung von kompakten Riemannschen Flächen mit Automorphismengruppe $G = \mathrm{Aut}(Z/X)$. Dann gilt:*

a) Es ist $\mathscr{M}(X) \hookrightarrow \mathscr{M}(Z), g \mapsto g \circ f$ eine Körpererweiterung vom Grad $d = \deg(f)$.

b) Die folgenden Bedingungen sind äquivalent:

- *Es ist $|G| = \deg(f)$.*
- *Es ist $X \simeq Z/G$ (als topologischer Quotientenraum).*
- *Die Körpererweiterung $\mathscr{M}(X) \hookrightarrow \mathscr{M}(Z)$ ist Galois.*

c) Wenn diese Bedingungen gelten, haben wir eine Bijektion zwischen

- *Untergruppen $H = \mathrm{Aut}(Z/Y) \leq G = \mathrm{Aut}(Z/X)$,*
- *Zwischenkörpern $\mathscr{M}(X) \subseteq \mathscr{M}(Y) \subseteq \mathscr{M}(Z)$,*
- *Faktorisierungen $f : Z \to Y \to X$.*