Algebra

Dr. Stefan Kühnlein

Institut für Algebra und Geometrie, Karlsruher Institut für Technologie (KIT)
2012[1]

[1]Stand vom 22.03.2012

Die Vorlesung „Algebra“ schließt an die Vorlesung „Einführung in die Algebra und Zahlentheorie“ an.

Wir werden verschiedentlich auf diese verweisen, was im Skript mit „EAZ...“ geschieht.

Dabei greifen wir im ersten Kapitel noch einmal elementare Fragen der Gruppen- und Ringtheorie auf, die der Kürze des Sommersemesters zum Opfer gefallen waren, und wenden uns dann im zweiten Kapitel der Galoistheorie zu. Dies war früher typischer Weise das Ende der Vorlesung „Algebra I“. Dabei wurden Anwendungen der Galoistheorie oft etwas in den Hintergrund gedrängt, da das Semesterende nahe bevorstand. Dies könnte jetzt durch die frühere Lage im Semester etwas befriedigender werden.

Im dritten Kapitel lernen wir noch einmal neue Facetten der Ringtheorie kennen, die in der kommutativen Algebra eine systematischere und weiter reichende Behandlung erfahren. Als spezielle Klasse von Ringen lernen wir dann noch Dedekindringe kennen, die in Zahlentheorie und Algebraischer Geometrie eine fundamentale Rolle spielen. Eng damit verknüpft ist der Begriff einer diskreten Bewertung auf einem Körper.

Nach Ende der Vorlesungen hat Christian Steinhart mir noch eine Liste mit Korrekturvorschlägen zukommen lassen, die ich teilweise eingearbeitet habe. Ich danke ihm herzlich für das offensichtlich sehr genaue Lesen dieses Skriptums.

Karlsruhe im März 2012

Inhaltsverzeichnis

Kapitel 1

Mehr von Gruppen und Ringen

1.1 Einfache Gruppen

Definition 1.1.1 Total banal

Wir erinnern uns zunächst daran, dass eine Gruppe *einfach* heißt, wenn sie nichttrivial ist und außer der trivialen Gruppe und sich selbst keine weiteren Normalteiler besitzt.

Um einmal ein nichtabelsches Beispiel zu sehen, beweisen wir einen Hilfssatz.

Hilfssatz 1.1.2 A_n **ist meistens einfach**

Es sei $n \geq 5$ *eine natürliche Zahl.*

Dann ist die alternierende Gruppe A_n *einfach.*

Beweis. Wir machen vollständige Induktion nach n. Für $n = 5$ haben wir die Aussage in EAZ als Konsequenz der Sylowsätze gesehen. Ein nichttrivialer Normalteiler mit durch 3 oder 5 teilbarer Ordnung enthält alle 3-Zykel, und diese erzeugen A_5. Eine normale 2-Gruppe gibt es nicht in A_5.

Sei nun $n \geq 6$ und A_{n-1} einfach. Weiter sei $N \lhd A_n$ ein Normalteiler, der nicht nur die Identität enthält. Wie immer identifizieren wir A_{n-1} mit dem Stabilisator von n in A_n.

Wir wählen ein $\sigma \in N$, das nicht die Identität ist, und ein $a \in \{1, \ldots, n\}$, mit $b := \sigma(a) \neq a$. Weiter seien $c, d \in \{1, \ldots, n\}$ von a und b verschieden. Dann liegt der Dreizykel $\zeta = (b\ c\ d)$ in A_n, und

$$(\zeta\sigma\zeta^{-1})(a) = c.$$

Da N ein Normalteiler ist und c fast beliebig war, operiert N also transitiv auf $\{1, \ldots n\}$.

Nun sei $\tau \in N$ ein Element mit $\tau(n) = 1$. Da τ zu A_n gehört, ist es keine Transposition, es gibt also ein a mit $1 < a < n$ und $b = \tau(a) \neq a$. Wir wählen $1 < c, d < n$ von a verschieden und setzen $\zeta = (a\ c\ d) \in A_n$. Dann gilt

$$(\zeta^{-1}\tau\zeta)(n) = 1 \quad \text{und} \quad (\zeta^{-1}\tau\zeta)(d) = b,$$

also ist $\tilde{\tau} := (\zeta^{-1}\tau\zeta) \in N$ ein von τ verschiedenes Element (das Urbild von b ist ein anderes), und $\tau^{-1}\tilde{\tau} \in H := N \cap A_{n-1}$ ist nichttrivial. Wegen der Induktionsvoraussetzung ist H als nichttrivialer Normalteiler von A_{n-1} die ganze Gruppe A_{n-1}, und da N transitiv auf $\{1, \ldots, n\}$ operiert, gibt es für jedes $\pi \in A_n$ ein $\nu \in N$ mit $\pi\nu^{-1}(n) = n$, also

$$\pi\nu^{-1} \in A_{n-1} \subseteq N, \quad \text{also} \quad \pi \in A_{n-1}\nu \subseteq N.$$

Es folgt $A_n \subseteq N$ wie gewünscht. ◯

Definition 1.1.3 Kompositionsreihe

Es sei G eine Gruppe.

Eine *Normalreihe der Länge* k (mit $k \in \mathbb{N}$) für G ist eine Folge von Untergruppen

$$\{e_G\} =: G_0 \lhd G_1 \lhd G_2 \cdots \lhd G_{k-1} \lhd G_k := G,$$

sodass jedes G_{i-1} im darauffolgenden G_i normal ist.

Vorsicht: Das heißt noch lange nicht, dass G_1 zum Beispiel in G normal sein müsste!

Eine Normalreihe wie eben heißt eine *Kompositionsreihe*, wenn die Faktorgruppen

$$G_i/G_{i-1},\ 1 \leq i \leq k,$$

alle einfach sind. Definitionsgemäßhat eine Kompositionsreihe also immer endliche Länge.

Beispiel 1.1.4 und Nichtbeispiel

Wenn G abelsch ist, dann ist jede aufsteigende Folge von Untergruppen, die bei $\{e_G\}$ anfängt und bei G aufhört, eine Normalreihe.

Eine Gruppe mit pq Elementen ($p < q$ Primzahlen) hat immer eine q-Sylowgruppe Q als Normalteiler. Diese ist einfach und die Faktorgruppe (mit p Elementen) ist auch einfach, also erhalten wir die Kompositionsreihe

$$\{e_G\} \lhd Q \lhd G$$

der Länge 2.

$\mathbb{Z}$ besitzt keine Kompositionsreihe, denn das G_1 darin müsste einfach sein, und es gibt keine einfache Untergruppe von $\mathbb{Z}$.

Aber jede endliche Gruppe hat eine Kompositionsreihe. Für Gruppen der Ordnung 1 ist das klar (Länge 0). Wenn G größere Ordnung hat, dann ist G entweder einfach (und wir erhalten eine Kompositionsreihe der Länge 1) oder G hat nichttriviale Normalteiler. Von diesen gibt es dann aber auch einen maximalen, und man sieht leicht ein, dass die entsprechende Faktorgruppe einfach ist. Dann greift ein Induktionsargument.

Eine Kompositionsreihe für die symmetrische Gruppe S_4 zum Beispiel sieht so aus:

$$\{e\} \lhd \{e, (12)(34)\} \lhd V_4 \lhd A_4 \lhd S_4$$

Dabei ist $V_4 = \{e, (12)(34), (13)(24), (14)(23)\}$ die *Klein*[1]*sche Vierergruppe*. Die Faktorgruppen sind jeweils zyklische Gruppen der Ordnungen 2,2,3, und 2.

Es gibt nun einen interessanten Satz über Kompositionsreihen.

Satz 1.1.5 von Jordan[2]-Hölder[3]

Es sei G eine Gruppe mit zwei Kompositionsreihen:

$$\{e_G\} =: G_0 \lhd G_1 \lhd G_2 \cdots \lhd G_{k-1} \lhd G_k := G,$$

$$\{e_G\} =: H_0 \lhd H_1 \lhd H_2 \cdots \lhd H_{l-1} \lhd H_l := G,$$

Dann gilt $k = l$, und bis auf die Reihenfolge und Isomorphie stimmen die einfachen Faktorgruppen G_i/G_{i-1} und H_j/H_{j-1} überein.

Beweis. Der Beweis ist klar, wenn $k = 0$ oder $k = 1$ gilt, denn im ersten Fall ist $G = \{e_G\}$, und im zweiten Fall ist G einfach.

Um gleich das allgemeine Induktionsprinzip zu verstehen, machen wir den Fall $k = 2$ individuell. Hier ist G nicht einfach, und damit auch $l \geq 2$.

Wenn hier $H_{l-1} = G_1$ gilt, dann sind wir fertig.

Ansonsten ist $H_{l-1} \cap G_1$ ein Normalteiler in G_1, denn H_{l-1} ist normal in G. Da G_1 einfach ist, ist H_{l-1} nicht darin enthalten (sonst wäre das ja trivial, da $G_1 \neq H_{l-1}$, und damit G einfach).

[1] Christian Felix Klein, 1848-1925
[2] Camille Marie Ennemond Jordan, 1838-1922
[3] Ludwig Otto Hölder, 1859-1937

Aber auch G_1 ist nicht in H_{l-1} enthalten, denn es ist ein maximaler Normalteiler und von H_{l-1} verschieden. Es folgt

$$H_{l-1} \cap G_1 = \{e_G\}.$$

Daher ist $H_{l-1} \cdot G_1$ ein größerer Normalteiler in G als G_1, und folglich gleich G.

Wir erhalten nach dem Homomorphiesatz

$$G/G_1 \cong (G_1 H_{l-1})/G_1 \cong H_{l-1},$$

also ist diese Gruppe einfach, und damit $l = 2$ sowie (aus Analogiegründen)

$$G_1 \cong G/H_1,\ G/G_1 \cong H_1.$$

Damit ist der Fall $k = 2$ erschlagen.

Im Weiteren sei $k \geq 3$ und die Behauptung wahr für alle kleineren Werte für k. Insbesondere ist dann auch $l \geq k$, sonst mache ich schnell aus dem l ein k und wende die Induktionsvoraussetzung an.

Ich fasse $N := G_{k-1} \cap H_{l-1}$ fest ins Auge. Als Durchschnitt zweier Normalteiler ist das eine normale Untergruppe. Hierfür treten in grober Näherung zwei Möglichkeiten auf:

Fall 1: $N = \{e_G\}$.

In diesem Fall ist $G_{k-1} \neq H_{l-1}$, da sonst beide trivial wären, obwohl

$k \geq 3$. Es folgt wie eben $G_{k-1} H_{l-1} = G$ und mit dem Homomorphiesatz $G/H_{l-1} \cong G_{k-1}$.

Demnach ist G_{k-1} einfach und daher $k = 2$, was nicht stimmt. Damit lege ich den Fall ad acta.

Fall 2: $N \neq \{e_G\}$.

Hier enthält die Folge

$$\{e_G\} \lhd G_1 \cap N \lhd G_2 \cap N \lhd \cdots \lhd G_{k-1} \cap N = N$$

nach Wegstreichen der Doppelungen eine Kompositionsreihe von N, genauso wie auch

$$\{e_G\} \lhd H_1 \cap N \lhd H_2 \cap N \lhd \cdots \lhd H_{l-1} \cap N = N$$

Da die Länge offensichtlich kürzer ist als k folgt mit der Induktionsvoraussetzung, dass die beiden Kompositionsreihen von N dieselbe Länge und (bis auf die Reihenfolge) dieselben Faktorgruppen besitzen.

Die naheliegende Folge von N nach G ist

$$N \lhd G_1N \lhd G_2N \lhd \dots G_kN \lhd G$$

Faktorbildung nach N liefert

$$\{e_{G/N}\} \lhd G_1/(N \cap G_1) \lhd G_2/(N \cap G_2) \lhd \cdots \lhd G/N,$$

und das enthält wieder eine Kompositionsreihe für G/N. Sie ist kürzer als die von G, und wir können wieder per Induktionsvoraussetzung sehen, dass sie und die entsprechende Folge für die H_j dieselbe Länge und dieselben Faktorgruppen besitzen.

Um am Ende noch buchhalterisch einzusehen, dass das auch wirklich etwas für die ursprünglichen Kompositionsreihen liefert, halten wir noch das folgende fest:

Eine „Doppelung“ in der ersten, per Durchschnitt entstandenen, Kompositionsreihe von N tritt da auf, wo $G_{i-1} \cap N = G_i \cap N$ gilt. Aber dann ist $G_{i-1}/(N \cap G_i)$ ein echter Normalteiler in $G_i/(N \cap G_i)$, und ich sehe

$$\big(G_i/(N \cap G_i)\big)/\big(G_{i-1}/(N \cap G_i)\big) \cong G_i/G_{i-1}$$

Also entsprechen die Doppelungen der einen Reihe echten Schritten in der anderen, und dies gilt auch umgekehrt. Daher haben die zwei Kompositionsreihen von G tatsächlich dieselbe Länge, und die Quotienten stimmen bis auf die Reihenfolge überein. ◯

Folgerung 1.1.6 Fundamentalsatz der Arithmetik

Es sei $n \in \mathbb{N}$ gegeben. Die Gruppe $G = \mathbb{Z}/n\mathbb{Z}$ hat eine Kompositionsreihe. Die auftretenden Faktorgruppen sind abelsch und daher als einfache abelsche Gruppen von Primzahlordnung. Das impliziert, dass n ein Produkt von Primzahlen ist, und dass die hier auftretenden Primfaktoren nebst der Häufigkeit ihres Erscheinens eindeutig sind.

Bemerkung 1.1.7 Moduln

Auch für Moduln über einem Ring R gibt es den Begriff des einfachen Moduls; das ist ein nichttrivialer Modul M, der außer $\{0\}$ und M keine Untermoduln hat.

Wieder kann man definieren, was eine Kompositionsreihe ist; und wieder gilt der Satz von Jordan-Hölder über die Eindeutigkeit der in Kompositionsreihen eines festen Moduls M auftretenden *Kompositionsfaktoren*. Der Beweis ist sogar etwas einfacher, weil man nicht so darauf aufpassen muss, was worin normal ist und so weiter. Man kann nach jedem Untermodul den Faktormodul bilden.

Bemerkung 1.1.8 Der große Satz

Die Suche nach einem Überblick über die Gesamtheit aller endlichen einfachen Gruppen kulminierte in den 70er Jahren des vergangenen Jahrhunderts in einer (sehr sicher) endgültigen Liste, in der es einige „Serien“ solcher Gruppen gibt und darüber hinaus noch endlich viele sogenannte sporadische Gruppen.

Der Beweis der Vollständigkeit dieser Liste ist sehr aufwendig, und es gibt immer noch Bestrebungen, diesen Beweis kürzer zu machen.

1.2 Auflösbarkeit

Definition 1.2.1 Auflösbar

Es sei G eine Gruppe.

Dann heißt G *auflösbar*, wenn eine Normalreihe

$$\{e_G\} =: G_0 \lhd G_1 \lhd G_2 \cdots \lhd G_{k-1} \lhd G_k := G,$$

existiert, für die alle Quotienten G_i/G_{i-1} abelsch sind.

Diese Klasse von Gruppen verallgemeinert also die Klasse der abelschen Gruppen.

Man muss hier übrigens sehr aufpassen, die G_i sind nicht als in G normal vorausgesetzt. Wenn sogar dies möglich ist und zusätzlich G_i/G_{i-1} im Zentrum von G/G_{i-1} liegt, dann heißt G *nilpotent*.

Die Klasse der nilpotenten Gruppen umfasst immer noch die abelschen Gruppen, ist aber viel kleiner als die der auflösbaren Gruppen.

Beispiel 1.2.2 Matrizengruppen

Es sei K ein Körper und $G = \mathrm{GL}_n(K)$ die Gruppe der invertierbaren $n \times n$-Matrizen mit Einträgen aus K.

Außerdem sei $n \geq 2$.

Dann ist die Gruppe der invertierbaren oberen Dreiecksmatrizen auflösbar, aber nicht nilpotent. Die Gruppe der unipotenten oberen Dreiecksmatrizen (das heißt: nur Einsen auf der Diagonale) ist nilpotent.

Hilfssatz 1.2.3 Divide et impera

Es sei G eine Gruppe. Dann sind äquivalent:

i) G ist auflösbar.

ii) Jede Untergruppe und jede Faktorgruppe von G ist auflösbar.

iii) G besitzt einen Normalteiler N, sodass N und G/N auflösbar sind.

Bemerkung 1.2.4 p-Gruppen

Es sei p eine Primzahl und P eine p-Gruppe, also eine Gruppe, deren Kardinalität eine Potenz von p ist.

Wie immer operiert P auf sich selbst durch Konjugation:

$$\bullet : P \times P \to P, (g, x) \mapsto gxg^{-1}.$$

Die Bahnen dieser Operation haben als Länge eine Potenz von p, und die Bahn des neutralen Elements hat Länge 1. Da insgesamt die Summe der Bahnlängen die Ordnung von P ist, muss im Fall $P \neq \{1\}$ die Anzahl der Fixpunkte der Operation durch p teilbar sein. Diese Fixpunkte bilden aber gerade das Zentrum von P, und das zeigt:

$$P \neq \{1\} \Rightarrow Z(P) \neq \{1\}.$$

Insbesondere hat P einen nichttrivialen abelschen Normalteiler.

P hat eine Kompositionsreihe, und die Kompositionsfaktoren sind einfache p-Gruppen; diese sind wegen des eben gesehenen Arguments abelsch und damit zyklisch von Ordnung p. Somit ist P auflösbar, und es gibt eine normale Untergruppe von Index p, wenn $P \neq \{1\}$.

Diese Aussagen werden wir für $p = 2$ später bei den Anwendungen der Galoistheorie (Fundamentalsatz der Algebra sowie Konstruierbarkeit regelmäßiger n-Ecke mit Zirkel und Lineal) verwenden.

1.3 Einfache Moduln – maximale Ideale

Definition 1.3.1 Einfacher Modul

Es seien R ein Ring und M ein R-Modul.

Dann heißt M *einfach*, wenn $M \neq \{0\}$ gilt und jeder Untermodul $U \subset M$ entweder $\{0\}$ ist oder M.

Beispiel 1.3.2 Vektorräume

a) Der $\mathbb{Z}$-Modul $\mathbb{Q}$ ist nicht einfach und enthält auch nicht einmal einen einfachen Untermodul. Auch kein Quotient von $\mathbb{Q}$ ist einfach. Denn einfache $\mathbb{Z}$-Moduln sind genau die einfachen abelschen Gruppen, also die Gruppen von Primzahlordnung.

b) Ist $R = K$ ein Körper, so ist ein einfacher K-Modul ein K-Vektorraum V, der außer $\{0\}$ und V keine Untervektorräume besitzt, selbst aber nichttrivial ist. Das sind also genau die eindimensionalen Vektorräume. Insbesondere sind je zwei einfache K-Moduln hier isomorph.

Bemerkung 1.3.3 einfach $\Rightarrow$ einfach erzeugt

Es sei M ein einfacher R-Modul. Dann gibt es ein Element $m \in M$, das nicht 0 ist. Die Abbildung

$$\lambda : R \to M,\ \lambda(r) := r \cdot m,$$

ist ein Modulhomomorphismus, und daher ist $R \cdot m = \text{Bild}(\lambda)$ ein R-Untermodul von M. Da er $m = \lambda(1)$ enthält, ist er nicht 0, und wegen der Einfachheit von M folgt $R \cdot m = M$.

M ist also einfach erzeugt.

Die Umkehrung ist offensichtlich nicht der Fall, es gibt einfach erzeugte Moduln, die nicht einfach sind.

Aber wir können M wegen des Homomorphiesatzes schreiben als

$$M \cong R/\text{Kern}(\lambda),$$

wobei $\text{Kern}(\lambda) = \{r \in R \mid rm = 0\}$ der *Annulator* von m in R ist. (Das definiert man unabhängig von der Einfachheit von M so.)

Das ist ein Linksideal von R.

Ist nun $\text{Kern}(\lambda) \subset I \subset R$ für ein weiteres Linksideal I, so folgt $I/\text{Kern}(\lambda) \cong \lambda(I) \subset M$, und da M einfach ist, folgt $I = \text{Kern}(\lambda)$ oder $I = R$.

Definition 1.3.4 Maximale Ideale

Es sei R ein Ring. Ein Ideal $I \subset R$ heißt *maximales Ideal*, wenn $I \neq R$ gilt und zwischen I und R kein Ideal $\neq I$, $\neq R$ liegt.

Analog definiert man maximale Links- bzw. maximale Rechtsideale.

Beispiel 1.3.5 Hauptidealringe, einfache Moduln

a) Wenn R ein Hauptidealring ist, dann sind die maximalen Ideale genau die, die von irreduziblen Elementen erzeugt werden.

b) $I \subset R$ ist genau dann ein maximales Linksideal, wenn R/I ein einfacher R-Modul ist.

Eine größere Klasse von Idealen findet sich in der folgenden Definition:

Definition 1.3.6 Primideale

Es seien R ein kommutativer Ring und I ein Ideal in R.

Dann heißt I ein *Primideal*, wenn $I \neq R$ gilt und zusätzlich für alle $a, b \in R$:

$$ab \in I \Rightarrow a \in I \text{ oder } b \in I.$$

Hilfssatz 1.3.7 maximale Ideal sind prim

Es seien R ein kommutativer Ring und $I \subset R$ ein Ideal.

Dann gelten:

a) I ist genau dann ein Primideal, wenn R/I nullteilerfrei ist.

b) I ist genau dann maximal, wenn R/I ein Körper ist.

Beweis. Übungsaufgabe. ◯

Interessant ist nun die Frage, ob es immer maximale Ideale gibt. Tatsächlich gilt:

Hilfssatz 1.3.8 maximale Ideale existieren (meistens)

Es seien R ein kommutativer Ring und $a \in R$ keine Einheit.

Dann gibt es ein maximales Ideal $I \subset R$, das a enthält.

Beweis. Wir betrachten die Menge $\mathcal{S}$ aller Ideale $\neq R$, die a enthalten.

$\mathcal{S}$ ist nicht leer, denn das von a erzeugte Hauptideal liegt darin. Hierbei benutzen wir, dass a keine Einheit ist und R kommutativ.

Wir ordnen $\mathcal{S}$ durch Inklusion.

Nun sei $(I_k)_{k\in K}$ eine Familie in $\mathcal{S}$, sodass für je zwei Elemente $k, l \in K$ ein $m \in K$ mit der Eigenschaft

$$I_k \subseteq I_m \text{ und } I_l \subseteq I_m$$

existiert, zum Beispiel eine aufsteigende Folge.

Die Vereinigung

$$J := \bigcup_{k\in K} I_k$$

ist dann auch ein Ideal, denn es ist eine Untergruppe, und jedes $x \in J$ liegt schon in einem I_k, und darin liegen dann auch alle $rx, r \in R$, die damit auch in J liegen.

Aber J ist nicht der ganze Ring R, denn sonst läge $1 \in J$, und das müsste dann auch schon in einem I_k liegen, das damit ganz R wäre... ein Widerspruch!

Also gehört J zu $\mathcal{S}$, und wir sehen, dass jedes induktiv geordnete System in $\mathcal{S}$ eine obere Schranke in $\mathcal{S}$ besitzt. Das erlaubt uns, das Lemma von Zorn zu verwenden, das da sagt: Es gibt ein maximales Element M in $\mathcal{S}$.

Wir müssen noch zeigen, dass M in R ein maximales Ideal ist, nicht nur maximales Element von $\mathcal{S}$. Das ist aber klar, denn jedes M umfassende Ideal enthält a, ist also entweder ein Element von $\mathcal{S}$ oder ist schon ganz R. ◯

Der Satz zeigt insbesondere, dass in jedem Ring $\neq \{0\}$ maximale Ideale existieren, denn wir können $a = 0$ verwenden.

Kapitel 2

Körpererweiterungen

In diesem Kapitel geht es darum, Fragen nach Erweiterungen von Körpern zu diskutieren. Was ein Körper ist, wissen wir schon.

2.1 Algebraizität

Definition 2.1.1 Algebraisch und transzendent

Es sei K ein Körper und L ein Körper, der K umfasst. Wir nennen dann $K \subseteq L$ eine *Körpererweiterung.*

a) Ein Element $\alpha \in L$ heißt *algebraisch über* K*,* falls es ein Polynom $f \in K[X],\ f \neq 0,$ gibt, sodass $f(\alpha) = 0.$

b) Ein Element $\alpha \in L,$ das nicht über K algebraisch ist, heißt *transzendent über* K*.*

c) L heißt algebraisch über K, wenn jedes Element von L über K algebraisch ist.

d) Es sei $\alpha \in L$ über K algebraisch. Dann ist das *Verschwindungsideal*

$$V(\alpha) := \{f \in K[X] \mid f(\alpha) = 0\}$$

nicht das Nullideal im Polynomring. Der normierte Erzeuger von $V(\alpha)$ heißt das *Minimalpolynom* von α.

Den kleinsten Teilkörper von L, der K und ein gegebenes Element α von L enthält, bezeichnen wir mit $K(\alpha)$. Man sagt, dass er durch *Adjunktion* von α zu K entsteht.

Genauso gibt es für jede Teilmenge A von L den kleinsten Teilkörper, der K und A umfasst. Er wird natürlich mit $K(A)$ notiert.

Beispiel 2.1.2 Beides kommt vor

$\mathbb{C}$ ist ein Erweiterungskörper von $\mathbb{Q}$. Da es nur abzählbar viele von 0 verschiedene Polynome in $\mathbb{Q}[X]$ gibt und jedes davon nur endlich viele Nullstellen in $\mathbb{C}$ hat, gibt es in $\mathbb{C}$ auch nur abzählbar viele algebraische Elemente. Zum Beispiel ist $\mathbb{Q}(\sqrt{2})$ eine algebraische Körpererweiterung. Da andererseits $\mathbb{C}$ überabzählbar ist, muss es dort auch transzendente Elemente geben, im Sinne des Lebesgue-Maßes sind diese sogar weit in der Überzahl, denn abzählbare Mengen sind Nullmengen.

Konkret sind zum Beispiel die Eulersche Zahl e[1] oder die Kreiszahl π transzendent, wie ein Satz von Lindemann[2] sagt, mit dem gegen Ende des 19. Jahrhunderts gezeigt wurde, dass die Quadratur des Kreises mit Zirkel und Lineal nicht möglich ist.

Es ist zumeist sehr schwer, von einer gegebenen Zahl zu entscheiden, ob sie algebraisch oder transzendent ist. Die Transzendenztheorie ist eine Teildisziplin der Zahlentheorie, die genau hierfür Werkzeuge entwickelt.

Bemerkung 2.1.3 Zur Notation

Es hat sich eingebürgert, für einen Erweiterungskörper L von K zu sagen, L *über* K sei eine Körpererweiterung. Oft findet sich hier auch die Notation L/K, die ich insofern gerade auch für den Neuling für missverständlich halte, als das mit dem Bilden der Faktorgruppe verwechselt werden kann. Ich bevorzuge hier die weniger missverständliche Notation $K \subseteq L$, wenngleich die andere heute aus der Literatur in diesem und vielen ähnlich gelagerten Kontexten nicht wegzudenken ist.

Ein Erweiterungskörper $K \subseteq L$ ist insbesondere eine K-Algebra. Wie in EAZ 2.3.8 bezeichnen wir mit $\mathrm{Aut}(L|K)$ die Gruppe aller K-linearen Automorphismen des Körpers L. Ist $\sigma \in \mathrm{Aut}(L|K)$ und $\alpha \in L$ algebraisch über K, so ist $\sigma(\alpha)$ ebenfalls eine Nullstelle des Minimalpolynoms von α über K. Das schränkt die Möglichkeiten von Automorphismen drastisch ein, wir werden das später noch eingehend ausnutzen.

Hilfssatz 2.1.4 Algebraische Erweiterung

Es sei $K \subseteq L$ eine Körpererweiterung. Dann gelten:

a) Ein $\alpha \in L$ ist genau dann über K algebraisch, wenn die Dimension von $K(\alpha)$ als K-Vektorraum endlich ist.

b) Die Menge aller über K algebraischen $\alpha \in L$ ist ein Teilkörper von L.

[1] Charles Hermite, 1822-1901
[2] Carl Louis Ferdinand von Lindemann, 1852-1939

c) Sind $K \subseteq L$ und $L \subseteq M$ algebraische Körpererweiterungen, so ist auch die Erweiterung $K \subseteq M$ algebraisch.

Beweis.

a) Wenn α über K algebraisch ist, dann ist die Auswertungsabbildung

$$K[X] \ni f \mapsto f(\alpha) \in L$$

nicht injektiv, und ihr Kern ist ein nichttriviales Primideal in $K[X]$. Es wird vom Minimalpolynom M von α erzeugt, und wir wissen, dass die K-Dimension von $K[X]/MK[X]$ gleich dem Grad von M ist, also endlich. Andererseits ist nach dem Homomorphiesatz das Bild der Auswertungsabbildung isomorph zu $K[X]/MK[X]$ und hat daher auch dieselbe Dimension über K. Da die nichttrivialen Primideale im Hauptidealring $K[X]$ gleichzeitig die maximalen Ideale sind, ist dieses Bild also ein Körper und muss gleich $K(\alpha)$ sein.

Ist umgekehrt die K-Dimension von $K(\alpha)$ endlich, so kann die Auswertungsabbildung $K[X] \ni f \mapsto f(\alpha) \in L$ nicht injektiv sein, und ihr Kern enthält ein nichttriviales Element, was gerade die Definition der Algebraizität von α ist.

Alternativ sind $1, \alpha, \alpha^2, \ldots, \alpha^d$ mit $d = \dim_K(K(\alpha))$ nicht linear unabhängig, es gibt also eine nichttriviale Relation zwischen ihnen. Diese entspricht einem von Null verschiedenen Polynom, das α als Nullstelle hat.

b) Wir müssen zeigen, dass mit zwei algebraischen Elementen $\alpha, \beta \in L$ auch $-\alpha$, $\alpha + \beta$, $\alpha \cdot \beta$ und gegebenenfalls α^{-1} über K algebraisch sind.

Dazu sei $K(\alpha, \beta)$ der kleinste Teilkörper von L, der K und α und β enthält. Da β über K algebraisch ist, ist es auch über $K(\alpha)$ algebraisch. $\{1, \alpha, \alpha^2, \ldots, \alpha^{d-1}\}$ ist eine K-Basis von $K(\alpha)$ und $\{1, \beta, \ldots, \beta^{e-1}\}$ eine $K(\alpha)$-Basis von $K(\alpha, \beta)$. Dann ist offensichtlich

$$\{\alpha^i \beta^j \mid 0 \leq i \leq d-1, 0 \leq j \leq e-1\}$$

eine K-Basis von $K(\alpha, \beta)$, und damit alle Elemente dieses Körpers in einem über K endlichdimensionalen Körper enthalten. Daher sind sie algebraisch. Zu diesen Elementen gehören auch $\alpha\beta$ und $\alpha + \beta$, $-\alpha$ und – falls $\alpha \neq 0$ – auch α^{-1}.

c) Es sei $\alpha \in M$. Wir müssen begründen, dass α über K algebraisch ist.

Dazu betrachten wir das Minimalpolynom von α über L und schreiben es als

$$f = \sum_{i=0}^{n} c_i X^i, \quad c_i \in L.$$

Da die Koeffizienten alle über K algebraisch sind, ist wegen a) und b)

$$Z := K(c_0, \ldots, c_n)$$

eine endlichdimensionale K-Algebra. Da auch $Z(\alpha)$ endliche Dimension über Z hat, hat insgesamt $Z(\alpha)$ endliche Dimension über K. Da $K(\alpha) \subseteq Z(\alpha)$ gilt, kann es über K nicht unendliche Dimension haben, und damit ist α auch über K algebraisch. ◯

Definition 2.1.5 Körpergrad

Es sei $K \subseteq L$ eine Körpererweiterung. Die Dimension von L als K-Vektorraum nennt man auch den *Grad von L über K*. Man notiert diesen mit $[L : K]$.

Es ist also α genau dann algebraisch, wenn $[K(\alpha) : K] < \infty$.

Man sagt auch, L sei eine endliche Erweiterung von K, wenn der Grad endlich ist. Sind $K \subseteq L \subseteq M$ endliche Körpererweiterungen, so gilt

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

Wenn B eine K-Basis von L ist und C eine L-Basis von M, dann ist $\{bc \mid b \in B, c \in C\}$ eine K-Basis von M.

Der Grad von $K(\alpha)$ über K ist gleich dem Grad des Minimalpolynoms von α über K.

Definition 2.1.6 Algebraisch unabhängig

Wieder sei $K \subseteq L$ eine Körpererweiterung. Eine Teilmenge $A \subseteq L$ heißt *über K algebraisch unabhängig*, wenn für jede endliche Teilmenge $\{\alpha_1, \ldots, \alpha_n\} \subseteq A$ aus n Elementen ($n \in \mathbb{N}$) der K-Algebrenhomomorphismus

$$K[X_1, \ldots, X_n] \to L, f \mapsto f(\alpha_1, \ldots, \alpha_n)$$

injektiv ist. Konkreter: α_1 ist transzendent über K, α_2 ist transzendent über $K(\alpha_1)$, α_3 ist transzendent über $K(\alpha_1, \alpha_2)$, usw...

Wenn A algebraisch unabhängig ist und L über $K(A)$ algebraisch, dann heißt A auch eine *Transzendenzbasis* von L über K.

Bemerkung 2.1.7 Wieder einmal der Zorn

Eine einelementige Menge $A = \{\alpha\} \subseteq L$ ist algebraisch unabhängig genau dann, wenn α über K transzendent ist.

Ist L also algebraisch über K, so ist demnach jede algebraisch unabhängige Teilmenge leer, und damit die leere Menge eine Transzendenzbasis.

$\{X\}$ ist eine Transzendenzbasis des Körpers $K(X)$ der rationalen Funktionen über K.

Allgemein kann man mit dem Zornschen Lemma zeigen, dass es für jede Körpererweiterung eine Transzendenzbasis gibt, und dass je zwei Transzendenzbasen dieselbe Kardinalität haben.

Hilfssatz 2.1.8 Fundamentalkonstruktion

Es seien K Körper und $f \in K[X]$ ein normiertes Polynom. Dann gibt es einen Erweiterungskörper L von K, über dem f in Linearfaktoren zerfällt.

Beweis. Wir führen den Beweis induktiv nach dem Grad von f, und zwar für alle Körper gleichzeitig.

Für $\deg(f) = 0$ ist nichts zu zeigen, denn dann ist $f = 1$ schon ein leeres Produkt.

Auch für Grad 1 ist die Behauptung klar.

Spaßes halber führen wir noch den Fall $\deg(f) = 2$ explizit aus. Wenn f eine Nullstelle $\alpha \in K$ hat, dann gilt

$$f = (X - \alpha)(X - \beta),$$

wobei $-(\alpha + \beta)$ der Faktor vor X in f ist.

Hat f noch keine Nullstelle in K, so ist f irreduzibel, und $L = K[X]/fK[X]$ ist wegen (EAZ, 3.2.14) ein Körper. Die Restklasse von X in diesem Körper ist eine Nullstelle von f, und damit zerfällt f über L in zwei Linearfaktoren.

Nun sei der Grad von f größer als 2.

Wenn f über K nicht irreduzibel ist, dann ist es Produkt von zwei normierten Faktoren f_1, f_2 kleineren Grades. Es gibt nach Induktionsvoraussetzung einen Körper L_1, über dem f_1 in Linearfaktoren zerfällt, und wieder nach Induktionsvoraussetzung existiert ein Erweiterungskörper L_2 von L_1, über dem auch f_2 in Linearfaktoren zerfällt. Dieser tut, was wir wollten.

Wenn f hingegen irreduzibel ist, dann ist $L_1 := K[X]/fK[X]$ ein Körper (selber Verweis wie oben!), in dem die Restklasse α von X eine Nullstelle von f ist. (Diese Konstruktion heißt oft die Konstruktion von Kronecker[3].)

Also können wir hier f zerlegen als

$$f = (X - \alpha) \cdot f_2,$$

wobei der Grad von f_2 kleiner ist als der von f. Es gibt also nach Induktionsvoraussetzung einen Erweiterungskörper L_2 von L_1, in dem f_2 in Linearfaktoren zerfällt, und dieser tut, was wir wollten. ◯

Definition 2.1.9 Algebraischer Abschluss

Ein Körper K heißt *algebraisch abgeschlossen*, wenn er keine echten algebraischen Erweiterungskörper besitzt. Das ist äquivalent dazu, dass jedes normierte

[3] Leopold Kronecker, 1823-1891

Polynom in $K[X]$ schon da in Linearfaktoren zerfällt, und auch dazu, dass jedes nichtkonstante Polynom in $K[X]$ mindestens eine Nullstelle in K hat.

Ein algebraischer Erweiterungskörper von K, der algebraisch abgeschlossen ist, heißt ein *algebraischer Abschluss von K.* Wir werden später sehen, dass er bis auf einen K-Algebrenisomorphismus eindeutig bestimmt ist.

Satz 2.1.10 Existenz des algebraischen Abschlusses

Es sei K ein Körper. Dann existiert ein algebraischer Abschluss von K.

Beweis. Wir konstruieren als erstes einen Körper K_1, in dem jedes Polynom aus $K[X]$ mindestens eine Nullstelle hat. Im Allgemeinen muss das noch nicht ein algebraischer Abschluss sein.

Um K_1 zu konstruieren, betrachten wir den Polynomring R in den Variablen X_p, wobei der Index p die Menge $\mathbb{P}_{K[X]}$ der irreduziblen normierten Polynome in $K[X]$ durchläuft. In R gibt es das Ideal I, das von den Elementen $p(X_p),\ p \in \mathbb{P}_{K[X]},$ erzeugt wird.

Dieses Ideal ist ein echtes Ideal. Ansonsten läge die 1 darin, und das hieße, dass 1 sich schreiben lässt als

$$1 = \sum_{i=1}^{n} g_i \cdot p_i(X_{p_i}), \quad g_i \in R \text{ geeignet.}$$

Hierbei sind $p_1, \ldots, p_n \in \mathbb{P}_{K[X]}$ paarweise verschieden.

Nach 2.1.8 wissen wir, dass es einen Erweiterungskörper L von K gibt, über dem $p_1 \cdot \ldots \cdot p_n$ in Linearfaktoren zerfällt. Für jedes i zwischen 1 und n sei $a_i \in L$ eine Nullstelle von p_i. Dann gibt es einen K-Algebrenhomomorphismus Φ von R nach L, der die X_{p_i} auf a_i abbildet $(1 \leq i \leq n)$ und alle anderen X_p auf 0. Hierbei nutzen wir die Arithmetik (universelle Abbildungseigenschaft) im Polynomring aus.

Es gilt dann

$$\Phi(1) = \Phi(\sum_{i=1}^{n} g_i \cdot p_i(X_{p_i})) = \sum_{i=1}^{n} \Phi(g_i) \cdot \Phi(p_i(X_{p_i})) = \sum_{i=1}^{n} \Phi(g_i) \cdot 0 = 0,$$

was ein Widerspruch ist. Daher gehört 1 nicht zu I.

Mit dem Argument aus 1.3.8 sieht man, dass in R ein maximales Ideal M existiert, das I enthält.

Wegen 1.3.7 ist $K_1 := R/M$ ein Körper, der auf natürliche Weise auch K enthält, und in dem die Restklasse von X_p modulo M eine Nullstelle des Polynoms p ist. Daher hat jedes irreduzible Polynom $p \in \mathbb{P}_{K[X]}$ eine Nullstelle in K_1, und

da nach (EAZ, 3.2.10) jedes nichtkonstante Polynom in $K[X]$ zu einem Produkt von Elementen aus $\mathbb{P}_{K[X]}$ assoziiert ist, hat es in K_1 mindestens eine Nullstelle.

Ausgehend von K_1 kann man dann einen Körper K_2 finden, in dem jedes nichtkonstante Polynom in $K_1[X]$ eine Nullstelle hat, und so weiter: Wir finden einen „Turm“

$$K \subseteq K_1 \subseteq K_2 \subseteq \dots$$

sodass jedes nichtkonstante Polynom mit Koeffizienten im Körper K_i eine Nullstelle in K_{i+1} hat.

Die Vereinigung all dieser Körper ist dann wieder ein Körper K_∞, und wenn $f \in K_\infty[X]$ ein nichtkonstantes Polynom ist, dann liegen seine Koeffizienten schon in einem K_i, also findet sich eine Nullstelle auch in $K_{i+1} \subseteq K_\infty$. Daher ist K_∞ algebraisch abgeschlossen.

Die Menge aller über K algebraischen Elemente in K_∞ ist dann ein algebraischer Abschluss von K. ◯

2.2 Irreduzibles

Hier wollen wir uns einiges über irreduzible Polynome überlegen. Wir fangen mit einem Hilfssatz an.

Hilfssatz 2.2.1 Eisensteinkriterium[4]

Es seien R ein kommutativer nullteilerfreier Ring und $P \subseteq R$ ein Primideal.

Weiter sei $f = \sum_{i=0}^{d} r_i X^i \in R[X]$ ein nichtkonstantes Polynom, dessen Leitkoeffizient r_d nicht in P liegt, alle anderen Koeffizienten aber schon. Schließlich sei r_0 kein Produkt von zwei Elementen aus P.

Dann ist f kein Produkt von zwei Faktoren in $R[X]$, die kleineren Grad haben.

Beweis. Wir nehmen im Gegenteil an, f sei ein Produkt von zwei Faktoren g und h kleineren Grades. Insbesondere ist dann der Grad von f mindestens 2. Wir schreiben

$$g = \sum s_j X^j, \quad h = \sum t_k X^k.$$

Aus $gh = f$ folgt $s_0 t_0 = r_0 \in P$. Da P ein Primideal ist, ist einer der Faktoren in P. Da r_0 kein Produkt von zwei Faktoren aus P ist, ist genau einer der Faktoren in P. Ohne Einschränkung sei $s_0 \in P$, $t_0 \notin P$.

Als nächstes bekommen wir $s_0 t_1 + s_1 t_0 = r_1 \in P$. Daher ist $s_1 t_0 \in P$, und wegen $t_0 \notin P$ folgt $s_1 \in P$.

[4] Ferdinand Gotthold Max Eisenstein, 1823-1852

Wir machen rekursiv so weiter und sehen, dass für $l < d$ mit

$$s_l t_0 = r_l - (s_0 t_l + s_1 t_{l-1} + \cdots + s_{l-1} t_1) \in P$$

stets folgt, dass auch $s_l \in P$. Daher liegt der Leitkoeffizient von g in P, denn der Grad von g ist kleiner als d. Da der Leitkoeffizient von f das Produkt der Leitkoeffizienten von g und h ist, liegt auch dieser in P, was explizit ausgeschlossen war.

Das führt unsere Annahme zum Widerspruch. ◯

Beispiel 2.2.2 Ganzzahliges

Insbesondere für $R = \mathbb{Z}$ ist dieses Kriterium sehr hilfreich. Zum Beispiel fallen Polynome wie $X^n - p,\ p \in \mathbb{P},$ darunter.

Man sieht jetzt sofort, dass es über $\mathbb{Z}$ irreduzible Polynome beliebig hohen Grades gibt.

Was uns noch fehlt ist die Erkenntnis, wann solche Polynome auch über $\mathbb{Q}$ irreduzibel sind, denn dann können wir auch viele Körpererweiterungen von $\mathbb{Q}$ konstruieren.

Dazu brauchen wir noch einmal den Begriff des Inhalts.

Definition 2.2.3 Noch einmal der Inhalt

Es sei R ein Hauptidealring. Der *Inhalt* $\mathrm{Inh}(f)$ eines Polynoms $f \in R[X], f \neq 0$, ist definiert als der Inhalt seiner Koeffizienten (EAZ, 3.4.5), also ein Erzeuger des Ideals, das von den Koeffizienten von f erzeugt wird. Wie schon früher ist auch diesmal der Inhalt nur bis auf Assoziiertheit definiert, also bis auf Multiplikation mit einer Einheit aus R.

Ein normiertes Polynom in $R[X]$ hat zum Beispiel immer Inhalt 1.

Ist K der Quotientenkörper von R und $f \in K[X]$ ein Polynom $\neq 0$, so gibt es ein $0 \neq r \in R$ mit $rf \in R[X]$. Wir definieren den Inhalt von f dann als

$$\mathrm{Inh}(f) := r^{-1}\mathrm{Inh}(rf).$$

Das ist ein Erzeuger des R-Untermoduls von K, der von den Koeffizienten von f erzeugt wird.

Für $R = \mathbb{Z}$ ist der Inhalt von $f = \frac{3}{7}X^2 + X - 5$ genau $\frac{1}{7}$, denn 3 und 7 sind teilerfremd.

Bemerkung 2.2.4 Inhalt 1

Wenn $f \in K[X]$ Inhalt 1 hat, dann liegt es schon in $R[X]$.

Für jedes $f \in K[X], f \neq 0,$ ist

$$\mathrm{Inh}(f)^{-1} \cdot f \in R[X]$$

ein Polynom von Inhalt 1.

Hilfssatz 2.2.5 Lemma von Gauß

Es seien R ein Hauptidealring mit Quotientenkörper K und $f, g \in K[X]$ von Null verschieden. Dann gilt

$$\mathrm{Inh}(fg) = \mathrm{Inh}(f) \cdot \mathrm{Inh}(g).$$

Beweis. Wegen der eben gemachten Bemerkung können wir annehmen, dass f, g Inhalt 1 haben, also Koeffizienten in R, die teilerfremd sind.

Sei $f = \sum r_i X^i, g = \sum_j s_j X^j$.

Wir müssen zeigen, dass kein irreduzibles Element von R alle Koeffizienten von fg teilt. Sei $p \in R$ irreduzibel. Dann existieren

$$m := \min\{i : p \text{ teilt nicht } r_i\}, n := \min\{j : p \text{ teilt nicht } s_j\}.$$

Dann teilt aber p auch nicht den Koeffizienten

$$\sum_{i+j=m+n} r_i s_j$$

von fg, denn alle Summanden außer $r_m s_n$ sind durch p teilbar. ◯

Eine wichtige Folgerung hieraus ist der folgende Hilfssatz.

Hilfssatz 2.2.6 Ein Irreduzibilitätskriterium

Es sei R ein Hauptidealring mit Quotientenkörper K und $f \in R[X]$ ein nichtkonstantes Polynom, das in $R[X]$ kein Produkt von Faktoren kleineren Grades ist.

Dann ist f in $K[X]$ irreduzibel.

Beweis. Es sei $f = gh$ mit $g, h \in K[X]$. Dann gilt wegen 2.2.5

$$\frac{1}{\mathrm{Inh}(f)} f = \frac{1}{\mathrm{Inh}(gh)} gh = \frac{1}{\mathrm{Inh}(g)} g \cdot \frac{1}{\mathrm{Inh}(h)} h,$$

und das ist eine Zerlegung der linken Seite in zwei ganzzahlige Faktoren.

Daher ist auch

$$f = \frac{\mathrm{Inh}(f)}{\mathrm{Inh}(g)} g \cdot \frac{1}{\mathrm{Inh}(h)} h$$

eine Zerlegung von f in zwei ganzzahlige Faktoren. Nach Voraussetzung erzwingt dies, dass g oder h denselben Grad hat wie f, und das andere Polynom ist konstant. ◯

Beispiel 2.2.7 Wie versprochen sehen wir jetzt irreduzible rationale Polynome beliebig hohen Grades, nämlich solche der Gestalt

$$X^d + p \cdot f(X),$$

wobei p ein Primzahl ist und $f \in \mathbb{Z}[X]$ ein Polynom vom Grad $< d$, dessen konstanter Term nicht durch p teilbar ist.

Wegen 2.2.1 sind diese über $\mathbb{Z}$ nicht in Faktoren vom Grad $< d$ zerlegbar, und daher auch über $\mathbb{Q}$ irreduzibel.

Bemerkung 2.2.8 faktorielle Ringe – eine Skizze

Vieles von dem, was wir in diesem Abschnitt über Hauptidealringe gelernt haben, geht ganz ähnlich für so genannte *faktorielle Ringe*.

Das sind kommutative, nullteilerfreie Ringe R, in denen jedes Element $\neq 0$ zu einem Produkt von Primelementen assoziiert ist.

Dieses Produkt ist dann im Wesentlichen eindeutig, was wiederum die Definition des größten gemeinsamen Teilers ermöglicht (anders als wir das in EAZ für Hauptidealringe gemacht haben!). Mit diesem kann man dann Inhalte von Polynomen definieren und das Lemma von Gauß sowie sein Korollar zeigen.

Interessanter Weise ist der Polynomring in einer (und induktiv in endlich vielen) Variablen über einem faktoriellen Ring wieder faktoriell.

Wir werden später daran interessiert sein, wann ein irreduzibles Polynom in $K[X]$ im algebraischen Abschluss von K nur einfache Nullstellen besitzt, wann es also in paarweise verschiedene Linearfaktoren zerfällt.

Wie in der Analysis kann man das mit der Ableitung überprüfen. Da uns aber hier kein Grenzwertprozess zur Verfügung steht, müssen wir die Ableitung von Polynomen rein algebraisch definieren. Es liegt eigentlich auf der Hand, wie das geht.

Definition/Bemerkung 2.2.9 Die Ableitung

Es sei K ein Körper. Die Abbildung

$$D : K[X] \to K[X], \quad D(\sum_{i=0}^{d} c_i X^i) := \sum_{i=1}^{d} i c_i X^{i-1},$$

heißt die *Ableitung*. Statt $D(f)$ werden wir auch in der Algebra häufig f' schreiben.

D ist derjenige Endomorphismus des K-Vektorraums $K[X]$, der auf der Basis $\{X^i \mid i \in \mathbb{N}_0\}$ durch $X^i \mapsto iX^{i-1}$ festgelegt wird.

Für die Multiplikation gilt die Leibnizregel[5]:

$$D(fg) = D(f)g + fD(g).$$

Denn: Beide Seiten der Gleichung sind K-bilinear in (f, g), und ausgewertet auf Paaren von Basisvektoren X^i, X^j gilt

$$D(X^{i+j}) = (i+j)X^{i+j-1} = iX^{i-1}X^j + X^i jX^{j-1} = D(X^i)X^j + X^i D(X^j),$$

also stimmen linke und rechte Seite obiger Gleichung für alle Paare von Basisvektoren überein, und das langt für die Gleichheit zweier bilinearer Abbildungen.

Man kann die Ableitung zu einem Endomorphismus von $K(X)$ fortsetzen durch

$$D(\frac{f}{g}) = \frac{D(f)g - D(g)f}{g^2}.$$

Diese Formel wird von der Quotientenregel der Analysis nahegelegt. D erfüllt dann auf ganz $K(X)$ die Leibnizregel.

Hilfssatz 2.2.10 mehrfache Nullstellen

Es seien $f \in K[X]$ ein Polynom und $\alpha \in K$ eine Nullstelle davon. Dann ist f genau dann ein Vielfaches von $(X-\alpha)^2$, wenn $f'(\alpha) = 0$ gilt.

Beweis. Wenn $(X-\alpha)^2$ ein Teiler von f ist, dann gilt mit $f = (X-\alpha)^2 h$:

$$\begin{aligned} D(f) &= D((X-\alpha)^2)h + (X-\alpha)^2 D(h) \\ &= 2(X-\alpha)h + (X-\alpha)^2 D(h) \\ &= (X-\alpha)\cdot[2h + (X-\alpha)D(h)], \end{aligned}$$

also ist α eine Nullstelle von f'.

Ist umgekehrt α eine Nullstelle von f' und von f, so folgt mit $f = (X-\alpha)h$

$$f' = (X-\alpha)D(h) + h,$$

also

$$h = f' - (X-\alpha)D(h) \in (X-\alpha)K[X].$$

Demnach ist $X-\alpha$ ein Teiler von h und damit $(X-\alpha)^2$ ein Teiler von f. ◯

Folgerung 2.2.11 irreduzible Polynome ohne mehrfache Nullstellen

Es seien $f \in K[X]$ irreduzibel und α eine Nullstelle von f in einem Erweiterungskörper L von K.

Dann ist α genau dann eine einfache Nullstelle von f, wenn $f' \neq 0$.

[5]Gottfried Wilhelm Leibniz, 1646-1716

Beweis. Das irreduzible Polynom f sei ohne Einschränkung normiert. Es ist dann das Minimalpolynom von α über K.

Die Nullstelle α von f ist genau dann einfach, wenn sie keine Nullstelle von f' ist. Da aber auch f' schon in $K[X]$ liegt und kleineren Grad als f hat, kann $f'(\alpha) = 0$ nur für $f' = 0$ gelten, denn kein anderes Polynom kleineren Grades als f ist Vielfaches von f. ◯

Definition/Bemerkung 2.2.12 Perfekte Körper

Ein Körper K heißt *perfekt*, wenn kein irreduzibles Polynom aus $K[X]$ in einem Erweiterungskörper mehrfache Nullstellen hat.

Das ist also äquivalent dazu, dass für kein irreduzibles Polynom $f \in K[X]$ die Ableitung f' das Nullpolynom ist.

Zum Beispiel stimmt das für Körper der Charakteristik 0, denn hier ist der Grad der Ableitung immer um 1 kleiner als der des hineingesteckten Polynoms.

Auch endliche Körper sind perfekt, denn eine Nullstelle eines irreduziblen Polynoms $f \in F[X]$ liegt in einem etwas größeren endlichen Körper mit (z.B.) q Elementen. Jedes Element dieses Körpers ist eine Nullstelle von $X^q - X$, und damit zerfällt dieses in paarweise verschiedene Faktoren. Das muss dann auch für seinen Faktor f gelten.

Im Gegensatz dazu ist zum Beispiel der Körper $K(T)$ der rationalen Funktionen in einer Variablen T über einem Körper K nicht perfekt, wenn die Charakteristik von K ungleich 0 ist. Ist diese nämlich $p \neq 0$, so ist das Polynom

$$X^p - T \in K(T)[X]$$

nach Eisenstein und Gauß irreduzibel, aber seine Ableitung bezüglich X ist 0.

Allgemein ist über einem Körper der Charakteristik p die Ableitung eines Polynoms genau dann 0, wenn an ihm nur Potenzen von X^p beteiligt sind.

2.3 Der Hauptsatz der Galoistheorie

Wir werden hier Ringhomomorphismen zwischen algebraischen Erweiterungskörpern eines Körpers K ansehen, die K-linear sind.

Hilfssatz 2.3.1 Surjektivität

Es sei $K \subseteq L$ eine algebraische Körpererweiterung und $\sigma : L \to L$ ein K-Algebrenendomorphismus.

Dann ist σ sogar ein Automorphismus.

Beweis. Da der Kern von σ ein Ideal in L ist, das nicht die 1 enthält, ist er $\{0\}$, und damit σ injektiv. Zu zeigen ist noch die Surjektivität.

Dazu sei $\alpha \in L$ und $f \in K[X]$ das Minimalpolynom von α. Der Endomorphismus σ permutiert die Nullstellen von f in L, denn das Bild einer Nullstelle ist eine Nullstelle, σ ist injektiv, und es gibt nur endlich viele Nullstellen. Daher liegt in L eine Nullstelle β von f, die unter σ auf α abgebildet wird. ◯

Um nun die algebraischen Erweiterungen von K besser sortieren zu können, ist es hilfreich zu wissen, dass es ein großes Auffangbecken dafür gibt. Dieses kennen wir schon: Es ist der algebraische Abschluss von K.

Hilfssatz 2.3.2 Eindeutigkeit des algebraischen Abschlusses

a) Es sei F^{alg} ein algebraisch abgeschlossener Körper.

Wenn $K \subseteq L$ eine algebraische Körpererweiterung ist, und $\varphi_0 : K \to F^{\text{alg}}$ ein Ringhomomorphismus, dann lässt φ_0 sich zu einem Ringhomomorphismus von L nach F^{alg} fortsetzen.

b) Je zwei algebraische Abschlüsse eines Körpers K sind zueinander isomorph.

Beweis.

a) Es sei $\mathcal{S}$ die Menge aller Paare (E, φ), wobei E ein Körper zwischen K und L ist und $\varphi : E \to F^{\text{alg}}$ eine Fortsetzung von φ_0 zu einem Ringhomomorphismus.

Die Menge $\mathcal{S}$ ist nicht leer, denn das Paar (K, φ_0) gehört dazu.

Auf $\mathcal{S}$ definieren wir eine Ordnungsrelation durch

$$(E, \varphi) \leq (\tilde{E}, \tilde{\varphi}) \iff E \subseteq \tilde{E} \text{ und } \tilde{\varphi}|_E = \varphi.$$

Bezüglich dieser Ordnungsrelation besitzt $\mathcal{S}$ ein maximales Element.

Ist nämlich

$$((E_i, \varphi_i))_{i \in I},$$

eine Familie von Elementen in $\mathcal{S}$, die mit je zweien auch ein gemeinsames größeres enthält, so ist auch die Vereinigung E_∞ der E_i ein Teilkörper von L, und durch

$$\psi : E_\infty \to F^{\text{alg}}, \psi(x) = \varphi_i(x) \text{ wenn } x \in E_i$$

wird eine wohldefinierte Abbildung auf E_∞ mit Werten in F^{alg} gegeben, die φ_0 fortsetzt. Daher ist (E_∞, ψ) eine obere Schranke unserer Folge. Wir dürfen damit das Lemma von Zorn verwenden, welches uns die Existenz eines maximalen Elements zusichert.

Es sei $(E, \varphi) \in \mathcal{S}$ maximal. Dann gilt $E = L$.

Denn: Es sei $\alpha \in L$ und f das Minimalpolynom von α über E. Der Körper $E' = E(\alpha)$ ist isomorph zu $E[X]/(f)$.

Wir setzen φ fort zu einem Ringhomomorphismus $\Phi : E[X] \to F^{\text{alg}}[X]$ mit der Eigenschaft $\Phi(X) = X$.

Wenn dann β eine Nullstelle von $\Phi(f)$ in F^{alg} ist, so ist

$$E[X] \ni h \mapsto \Phi(h)(\beta) \in F^{\text{alg}}$$

ein Ringhomomorphismus, in dessen Kern das irreduzible Polynom f liegt. Also ist der Kern das von f erzeugte Hauptideal, und damit ist das Bild zu $E[X]/(f)$ isomorph. Damit lässt sich φ nach $E(\alpha)$ fortsetzen, und wegen der Maximalität von (E, φ) ist $E(\alpha) = E$, also $\alpha \in E$.

Das zeigt $E = L$.

b) Es seien $\overline{K}$ und K^{alg} zwei algebraische Abschlüsse von K. Wegen a) gibt es K-Algebrenhomomorphismen $\varphi : \overline{K} \to K^{\text{alg}}$ und $\psi : K^{\text{alg}} \to \overline{K}$.

$\varphi \circ \psi$ ist also ein Endomorphismus von K^{alg} und damit wegen unseres letzten Hilfssatzes surjektiv. Damit ist auch φ surjektiv. Da es sowieso injektiv ist, ist es ein Isomorphismus. ◯

Folgerung 2.3.3 Viele Automorphismen

Es sei $K \subseteq K^{\text{alg}}$ ein algebraischer Abschluss des Körpers K.

a) Jeder Automorphismus von K lässt sich zu einem von K^{alg} fortsetzen.

b) Sind $\alpha \in K^{\text{alg}}$, $f \in K[X]$ sein Minimalpolynom und $\beta \in K^{\text{alg}}$ eine weitere Nullstelle von f, so gibt es einen K-Automorphismus von K^{alg}, der α nach β abbildet.

Beweis.

a) Das folgt für $L = K^{\text{alg}} = F^{\text{alg}}$ sofort aus 2.3.2a).

b) Hier sei $L = K(\alpha)$. Dieser Körper ist vermöge der Auswertung von Polynomen bei α und des Homomorphiesatzes isomorph zu $K[X]/(f)$.

Dasselbe gilt auch für $K(\beta) \cong K[X]/(f)$. Daher gibt es einen K-Isomorphismus φ_0 von $K(\alpha)$ nach $K(\beta) \subseteq K^{\text{alg}}$, der α auf β abbildet. Dieser lässt sich wieder mit 2.3.2a) fortsetzen zu einem Automorphismus von K^{alg}. ◯

Folgerung 2.3.4 Endliche Körper

Es sei p eine Primzahl. Dann gibt es für jede natürliche Zahl d einen Körper mit $q = p^d$ Elementen. Je zwei dieser Körper sind zueinander isomorph.

Beweis. Es sei L ein algebraischer Abschluss von $\mathbb{F}_p$.

Die Abbildung

$$\varphi : L \to L,\ x \mapsto x^p,$$

ist ein Automorphismus von L. Man nennt ihn oft den Frobenius-Automorphismus. Ihre d-te Potenz ist

$$\varphi^d : L \to L,\ x \mapsto x^q,\ q = p^d.$$

Die Menge aller Fixpunkte dieser Abbildung ist ein Teilkörper von L.

Diese Fixpunktmenge ist

$$F := \{x \in L \mid x^q - x = 0\}.$$

Sie hat höchstens q Elemente, da das die Nullstellen eines Polynoms vom Grad q sind.

Da die Ableitung von $X^q - X$ gerade $p^d X^{q-1} - 1 = -1$ ist, hat die Ableitung keine Nullstelle mit $X^q - X$ gemeinsam, und damit hat dieses Polynom wegen 2.2.10 tatsächlich in L q paarweise verschiedene Nullstellen. Daher hat F genau q Elemente.

Wenn K irgendein Körper mit q Elementen ist, dann sind alle Elemente von K Nullstellen von $X^q - X$ (wegen Lagrange für die Einheitengruppe), und das Bild der Einbettung von K nach L, die es wegen des eben gezeigten Satzes gibt, ist der eingangs konstruierte Körper mit q Elementen. ◯

Bemerkung 2.3.5 mehr dazu

Es sei $q = p^d > 1$ eine Potenz der Primzahl p. Der bis auf Isomorphismus eindeutig bestimmte Körper mit q Elementen heißt dann $\mathbb{F}_q$. Er ist der Faktorring von $\mathbb{F}_p[X]$ nach einem irreduziblen Polynom vom Grad d, das sich sicher unter den Teilern von $X^q - X$ findet.

Es ist klar, dass $\mathbb{F}_{p^d} \subseteq \mathbb{F}_{p^e}$ genau dann gilt, wenn d ein Teiler von e ist.

Man kann jetzt umgekehrt diese endlichen Körper nehmen und den algebraischen Abschluss von $\mathbb{F}_p$ konstruieren. Dazu sei für $n \in \mathbb{N}$ der Körper $F_n := \mathbb{F}_{p^{n!}}$ gegeben. Dann gilt

$$F_1 \subseteq F_2 \subseteq F_3 \subseteq \ldots$$

und wir erhalten den Abschluss von $\mathbb{F}_p$ als Vereinigung dieser endlichen Körper. Dass das ein Körper ist, ist klar. Da jedes Element α, das über der Vereinigung algebraisch ist, auch über $\mathbb{F}_p$ algebraisch ist, ist $\mathbb{F}_p(\alpha)$ ein endlicher Körper, der damit schon in einem der F_n liegen muss.

Man erhält also grob gesagt den algebraischen Abschluss von $\mathbb{F}_p$, indem man Einheitswurzeln von immer höherer Ordnung dazunimmt.

Hilfssatz 2.3.6 Anzahl der Automorphismen

Es sei $K \subseteq L$ eine endliche Körpererweiterung, $n := [L : K]$.

Dann gilt $\#\mathrm{Aut}(L|K) \leq n$.

Beweis. Es sei $L = K(\alpha_1, \ldots, \alpha_d)$. Weiter sei $\sigma \in \mathrm{Aut}(L|K)$. Für $1 \leq i \leq n$ setzen wir

$$K_i := K(\alpha_1, \ldots, \alpha_i) = K_{i-1}(\alpha_i),$$

wobei wir auch $K_0 := K$ definieren.

Schließlich sei $m_i \in K_{i-1}[X]$ das jeweilige Minimalpolynom von α_i. Wenn dieses Grad γ_i hat, so folgt aus der Multiplikativität der Körpergrade

$$n = \gamma_1 \cdot \gamma_2 \cdot \ldots \cdot \gamma_d.$$

Da $\sigma(\alpha_1)$ eine Nullstelle von $m_1 \in K[X]$ ist, gibt es hierfür höchstens γ_1 Möglichkeiten. Wenn eine davon fixiert ist, dann liegt σ auf K_1 fest. Dann ist $\sigma(\alpha_2)$ eine Nullstelle von $\sigma(m_2)$, was auch Grad γ_2 hat, und damit gibt es für $\sigma(\alpha_2)$ noch höchstens γ_2 Möglichkeiten.

Man verfährt sukzessive so weiter und findet für $\sigma(\alpha_i)$ höchstens γ_i Möglichkeiten, wenn $\sigma(\alpha_1), \ldots, \sigma(\alpha_{i-1})$ schon festgelegt sind.

Da σ durch die Bilder der Erzeuger festgenagelt wird, gibt es für σ insgesamt nicht mehr als

$$\gamma_1 \cdot \gamma_2 \cdot \ldots \cdot \gamma_d = n$$

Möglichkeiten, wie behauptet. ◯

Satz 2.3.7 mehr als ein Hilfssatz

Es sei $L := K(\alpha_1, \ldots, \alpha_d)$ ein Erweiterungskörper von K vom Grad n.

Weiter sei f_i für $1 \leq i \leq d$ das Minimalpolynom von α_i über K.

Dann sind äquivalent:

i) $\#\mathrm{Aut}(L|K) = n$

ii) *Jedes f_i zerfällt über L in paarweise verschiedene normierte Linearfaktoren.*

iii) *Für jedes $\alpha \in L$ zerfällt das Minimalpolynom $f \in K[X]$ von α in $L[X]$ in paarweise verschiedene normierte Linearfaktoren.*

Beweis.

Wir zeigen zunächst die Äquivalenz von i) und ii).

i) $\Rightarrow$ ii)

Im Beweis von 2.3.6 sieht man, dass sicher dann die Anzahl der Automorphismen von L über K kleiner als n ist, wenn das Minimalpolynom von α_1 in L weniger als γ_1 Nullstellen hat – egal, ob dies an höherer Vielfachheit liegt oder einfach an mangelnder Existenz.

Wenn also i) erfüllt ist, dann hat f_1 genau γ_1 paarweise verschiedene Nullstellen und zerfällt damit in paarweise verschiedene normierte Linearfaktoren.

Da man hier auch die Reihenfolge von $\alpha_1, \ldots, \alpha_d$ vertauschen kann, gilt die Behauptung für alle f_i.

ii) $\Rightarrow$ i)

Wie im Beweis des letzten Satzes sei $K_i := K(\alpha_1, \ldots, \alpha_i)$.

Es sei $\sigma : K_i \to L$ eine K-lineare Einbettung, $i < d$. Dann lässt σ sich zu einer Einbettung von K_{i+1} nach L fortsetzen.

Denn: Das Minimalpolynom m_{i+1} von α_{i+1} über K_i teilt f_{i+1} (da selbiges auch in $K_i[X]$ liegt und α_{i+1} als Nullstelle hat). Auch $\sigma(m_{i+1})$ (hierbei wird σ auf die Koeffizienten von m_{i+1} angewandt) teilt f_{i+1}, denn aus $f_{i+1} = m_{i+1} \cdot h_{i+1}$ folgt $f_{i+1} = \sigma(f_{i+1}) = \sigma(m_{i+1}) \cdot \sigma(h_{i+1})$.

Daher hat auch $\sigma(m_{i+1})$ in L γ_{i+1} paarweise verschiedene Nullstellen. Wenn β eine davon ist, dann wird durch

$$\tau : K_i[X] \to L, h \mapsto \sigma(h)(\beta)$$

ein Ringhomomorphismus gegeben, der auf K_i dasselbe macht wie σ, und in dessen Kern m_{i+1} liegt. Daher definiert τ eine Fortsetzung von σ nach $K_{i+1} \cong K_i[X]/(m_{i+1})$.

Da wir hierfür also γ_{i+1} Möglichkeiten haben, folgt die Behauptung i) durch sukzessives Fortsetzen der Inklusion von $K_0 = K$ nach L auf K_1, $K_2, \ldots, K_d$.

Die Äquivalenz von ii) und iii) ist nun klar, denn unter Voraussetzung von iii) hat man ja auch die Minimalpolynome $f_1, \ldots, f_n$ mit abgedeckt, und unter Voraussetzung von ii) auch das von irgendeinem α, denn das kann man zum Erzeugendensystem dazunehmen, ohne den Körpergrad oder die Anzahl der Automorphismen zu verändern. Wir gehen also vom alten ii) zu i) und dann zurück zu ii) für die Erzeuger $\alpha, \alpha_1, \ldots, \alpha_d$. ◯

Definition 2.3.8 Galoiserweiterung

Es sei $K \subseteq L$ eine algebraische Körpererweiterung.

a) Es sei $f \in K[X]$ ein Polynom. Dann heißt L ein *Zerfällungskörper* von f, wenn f in $L[X]$ in Linearfaktoren zerfällt und L über K von deren Nullstellen erzeugt wird.

Das ist also der kleinste Erweiterungskörper von K, über dem f in Linearfaktoren zerfällt.

Analog kann man den Zerfällungskörper einer Familie von Polynomen definieren.

b) Die Erweiterung $K \subseteq L$ heißt *normal*, wenn für jedes $\alpha \in L$ das Minimalpolynom aus $K[X]$ über L in Linearfaktoren zerfällt.

c) Ein Element $\alpha \in L$ heißt *separabel über* K, wenn sein Minimalpolynom keine mehrfache Nullstelle in L besitzt. Anders gesagt (siehe 2.2.11): Die Ableitung des Minimalpolynoms ist nicht 0.

d) Die Erweiterung $K \subseteq L$ heißt *separabel*, wenn alle $\alpha \in L$ über K separabel sind.

e) Die Erweiterung $K \subseteq L$ heißt *galoissch*, wenn sie separabel und normal ist.

Wenn $K \subseteq L$ galoissch ist, dann heißt die Gruppe $\mathrm{Aut}(L|K)$ auch die *Galoisgruppe* von L über K, und wir schreiben dafür in der Regel $\mathrm{Gal}(L|K)$.

Bemerkung 2.3.9 Permutationen

Es sei $K \subseteq L$ eine endliche Körpererweiterung vom Grad $[L : K] = n$.

Nach 2.3.7 ist $K \subseteq L$ genau dann galoissch, wenn die Automorphismengruppe genau n Elemente enthält.

Wenn in dieser Situation $f \in K[X]$ ein Polynom mit Zerfällungskörper L ist, dann permutiert $\mathrm{Gal}(L|K)$ die Nullstellen von f. Ist f irreduzibel, so werden die Nullstellen sogar transitiv permutiert, denn wir können eine beliebige davon nehmen und als α_1 im Beweis von 2.3.7 wählen. Im Allgemeinen wird das Bild der Galoisgruppe aber nicht die volle symmetrische Gruppe der Nullstellen sein.

Beispiel: Es sei $f = X^a - 1 \in \mathbb{Q}[X],\ a \in \mathbb{N}$. Ist

$$\zeta = \cos\frac{2\pi}{a} + \mathrm{i}\sin\frac{2\pi}{a} \in \mathbb{C}$$

eine (geeignete) Nullstelle davon, so ist $L := \mathbb{Q}(\zeta)$ der Zerfällungskörper von f, denn alle Nullstellen von f sind Potenzen von ζ.

Das Polynom f ist zwar für $a > 1$ niemals irreduzibel (es gibt die Nullstelle 1), jedoch ist der Grad des Minimalpolynoms von ζ über $\mathbb{Q}$ gleich $\varphi(a)$ (Eulersche φ-Funktion) und kann damit beliebig groß werden.

Andererseits liefert ein Automorphismus von L über $\mathbb{Q}$ einen Gruppenautomorphismus von $\langle\zeta\rangle$, was eine zyklische Gruppe der Ordnung a ist, und das ist eine Permutation, die durch Potenzieren mit einer Einheit in $\mathbb{Z}/a\mathbb{Z}$ kommt. Daher ist die Automorphismengruppe $\mathrm{Gal}(\mathbb{Q}(\zeta)|\mathbb{Q})$ isomorph zu einer Untergruppe von

$(\mathbb{Z}/a\mathbb{Z})^\times$, also sicher abelsch, die symmetrische Gruppe auf den a-ten Einheitswurzeln aber meistens nicht.

Ein Satz von Kronecker und Weber[6] sagt, dass jeder galoissche Erweiterungskörper von $\mathbb{Q}$ mit abelscher Galoisgruppe in einem solchen *Kreisteilungskörper* $\mathbb{Q}(\zeta)$ enthalten ist. Das kann man mit Methoden der algebraischen Zahlentheorie beweisen und ist ein Ausgangspunkt für die sogenannte Klassenkörpertheorie.

Hilfssatz 2.3.10 Der Fixkörper

Es sei $K \subseteq L$ eine endliche Galoiserweiterung und $G = \mathrm{Gal}(L|K)$.

Dann gilt

$$K = L^G := \{x \in L | \forall \sigma \in G : \sigma(x) = x\}.$$

Beweis. Es ist klar, dass L^G ein Körper ist, der K enthält. Laut Definition von L^G gilt dann aber auch $G \subseteq \mathrm{Aut}(L|L^G)$.

Daher muss der Grad von L über L^G mindestens $\#G$ sein, aber das ist wegen 2.3.7 schon der Grad von L über K, was $K = L^G$ erzwingt. ◯

Hilfssatz 2.3.11 Kriterium für die Normalität

Es sei $K \subseteq L$ eine algebraische Körpererweiterung. Dann sind äquivalent:

i) L ist normal über K.

ii) L ist der Zerfällungskörper einer Familie von Polynomen.

iii) Für jede algebraische Erweiterung $L \subseteq M$ und jedes $\sigma \in \mathrm{Aut}(M|K)$ gilt $\sigma(L) \subseteq L$.

Beweis. i) ⇒ ii)

Wenn L normal ist und von $A \subseteq L$ erzeugt wird, dann ist es der Zerfällungskörper der Familie in $K[X]$, die aus den Minimalpolynomen der Elemente von A besteht.

ii) ⇒ iii)

Es sei L der Zerfällungskörper von $\mathcal{F} \subseteq K[X]$. Dann ist $L = K(A)$, wobei A die Menge der Nullstellen der Polynome in $\mathcal{F}$ ist.

Weiter seien $L \subseteq M$ und σ wie in iii). Dann gilt für $\alpha \in A$, dass $\sigma(\alpha)$ eine Nullstelle des Minimalpolynoms von α über K ist. Da dieses aber ein Teiler eines Elements von $\mathcal{F}$ ist, zerfällt es schon über L in Linearfaktoren, und daher gilt auch $\sigma(\alpha) \in A$. Da L von A erzeugt wird, folgt $\sigma(L) \subseteq L$.

[6] Heinrich Weber, 1842-1913

iii) $\Rightarrow$ i)

Wie benutzen die Voraussetung aus iii) für den algebraischen Abschluss L^{alg} von L. Weiter seien $\alpha \in L$ und $\beta \in L^{\text{alg}}$ eine Nullstelle des Minimalpolynoms von α über K.

Wegen 2.3.3 gibt es einen K-Automorphismus von L^{alg}, der α auf β abbildet. Nach Voraussetzung liegt also auch β in L, und damit zerfallen alle Minimalpolynome der Elemente aus L schon über L. ◯

Bemerkung 2.3.12 normale Hülle

a) Es sei $K \subseteq L$ eine algebraische Erweiterung. Im algebraischen Abschluss gibt es dann den Körper, der von allen Nullstellen der Minimalpolynome aller $\alpha \in L$ erzeugt wird. Dieser ist der kleinste über K normale Erweiterungskörper von L und heißt die *normale Hülle* von L über K.

b) Ist $K \subseteq L$ schon normal und $K \subseteq E \subseteq L$ ein Körper zwischen K und L, so ist auch $E \subseteq L$ normal, denn L ist immer noch ein Zerfällungskörper. $K \subseteq E$ muss natürlich nicht normal sein.

Auch wenn $L \subseteq M$ eine normale Erweiterung von L ist, muss $K \subseteq M$ nicht normal sein.

Ist zum Beispiel $K = \mathbb{Q}$, $\alpha = \sqrt{2} \in \mathbb{R}$ und $\beta = \sqrt{\alpha} \in \mathbb{R}$, so sind zwar $K \subseteq K(\alpha)$ und $K(\alpha) \subseteq K(\alpha, \beta)$ normal, da es quadratische Erweiterungen sind, aber $K \subseteq K(\alpha, \beta) = K(\beta)$ ist nicht normal, da nur die reellen Nullstellen des Minimalpolynoms $X^4 - 2$ von β in diesem Körper liegen. Die normale Hülle über $\mathbb{Q}$ ist $\mathbb{Q}(\beta, \mathrm{i})$.

Hilfssatz 2.3.13 Separabilität

Es sei $K \subseteq L$ eine algebraische Erweiterung, $L = K(\alpha_1, \ldots, \alpha_n)$.

Dann ist $K \subseteq L$ genau dann separabel, wenn die Minimalpolynome $f_1, \ldots, f_n$ von $\alpha_1, \ldots, \alpha_n$ keine mehrfachen Nullstellen haben.

Beweis. Dass die Minimalpolynome bei einer separablen Erweiterung keine mehrfachen Nullstellen haben ist klar. Wir müssen umgekehrt zeigen, dass es genügt, diese Aussage nur für die Minimalpolynome $f_1, \ldots, f_n$ zu testen.

Weiter sei $L \subseteq Z$ ein Zerfällungkörper der Minimalpolynome $f_1, \ldots, f_n$. Dieser hat einen endlichen Grad d über K, und wegen 2.3.7 und laut Voraussetzung hat er genau d Automorphismen über K. Also ist Z über K galoissch, und damit jedes α darin separabel. ◯

Definition 2.3.14 primitives Element

Es sei $K \subseteq L$ eine endliche Körpererweiterung.

Ein Element $\alpha \in L$ heißt ein *primitives Element* der Erweiterung, wenn $L = K(\alpha)$.

Wenn solch ein primitives Element existiert, dann ist das sehr angenehm. Wir sehen gleich, dass es gar nicht so selten vorkommt.

Hilfssatz 2.3.15 Satz vom primitiven Element

Es sei $K \subseteq L$ eine endliche Körpererweiterung.

a) *Genau dann gibt es ein primitives Element für $K \subseteq L$, wenn es nur endlich viele Körper E zwischen K und L gibt.*

b) *Wenn $K \subseteq L$ galoissch ist, so gibt es ein primitives Element.*

c) *Wenn $K \subseteq L$ separabel ist, so gibt es ein primitives Element.*

Beweis.

a) Wenn $L = K(\alpha)$ gilt, so ist zu zeigen, dass es nur endlich viele Körper zwischen K und L gibt. Dazu sei $f \in K[X]$ das Minimalpolynom von α und S die Menge aller normierten Teiler von f in $L[X]$.

Die Menge S ist endlich. Für einen Körper E zwischen K und L sei $g \in E[X]$ das Minimalpolynom von α über E. Dies ist natürlich ein Element von S. Wenn $e_0, e_1, \dots$ die Koeffizienten von g sind, so ist $K(e_0, e_1, \dots) \subseteq E$ ein Teilkörper, über dem α dasselbe Minimalpolynom besitzt, wie über E. Also hat $L = K(\alpha) = E(\alpha)$ über beiden Körpern denselben Grad, und damit stimmen diese überein, da der eine im anderen enthalten ist.

Die Zuordnung von E zu g ist also injektiv, und damit gibt es nur endlich viele Kandidaten für E.

Für die andere Richtung ist es bequem, K als unendlich vorauszusetzen. Der Fall endlicher Körper wurde in EAZ 4.2.1 und 4.2.2 behandelt.

Wenn nun $E_1, \dots, E_r$ alle echten Teilkörper von L sind, die K enthalten, dann kann die Vereinigung der E_i nicht ganz L sein[7]. Es gibt also ein

$$\alpha \in L \setminus (E_1 \cup E_2 \cup \dots \cup E_r),$$

und dieses liegt in keinem echten Teilkörper von L, also ist $L = K(\alpha)$.

b) Wenn E ein Körper zwischen K und L ist, dann ist auch $E \subseteq L$ galoissch, und $H := \mathrm{Gal}(L|E) \subseteq \mathrm{Gal}(L|K)$ hat genau $[L : E]$ Elemente. Wegen 2.3.10

[7]Das ist ein Vektorraumargument, oder eher noch eines über affine Räume.

gilt dann $E = L^H$, man kann also E aus H zurückgewinnen, und damit ist die Zuordnung von E zu H injektiv.

Da es nur endlich viele Untergruppen von $\mathrm{Gal}(L|K)$ gibt, gibt es auch nur endlich viele Zwischenkörper, und damit nach a) ein primitives Element.

c) Wenn $K \subseteq L$ separabel ist, dann ist die normale Hülle von L galoissch über K und besitzt wegen a) und b) nur endlich viele Zwischenkörper. Die Zwischenkörper zwischen K und L sind davon wieder nur eine Teilmenge, also gibt es auch hier nur endlich viele, und damit haben wir wegen a) auch in L ein primitives Element. ◯

Wir sind nun in der Lage, den Hauptsatz der Galoistheorie zu beweisen.

Satz 2.3.16 Hauptsatz der Galoisteorie

Es sei $K \subseteq L$ eine endliche Galoiserweiterung, $G := \mathrm{Gal}(L|K)$. Weiter seien

$$\mathcal{Z} := \{E \mid K \subseteq E \subseteq L,\ E \text{ ist Körper}\}$$

die Menge der Zwischenkörper der Erweiterung und

$$\mathcal{U} := \{H \mid H \leq G \text{ ist Untergruppe}\}$$

die Menge der Untergruppen von G.

a) Die Zuordnungen

$$\mathrm{F} : \mathcal{U} \to \mathcal{Z},\ \mathrm{F}(H) := L^H,$$

und

$$\mathrm{A} : \mathcal{Z} \to \mathcal{U},\ \mathrm{A}(E) := \mathrm{Aut}(L|E),$$

sind zueinander invers.

b) $H \subseteq G$ ist genau dann eine normale Untergruppe, wenn $K \subseteq L^H$ eine normale Erweiterung ist.

In diesem Fall gilt $\mathrm{Aut}(L^H|K) \cong G/H$.

Beweis.

a) Da für jeden Körper $E \in \mathcal{Z}$ die Erweiterung $E \subseteq L$ galoissch ist, folgt aus 2.3.10 die Beziehung $\mathrm{F} \circ \mathrm{A} = \mathrm{Id}_{\mathcal{Z}}$.

Wir zeigen nun für $H \in \mathcal{U}$ auch noch

$$H = \mathrm{A}(\mathrm{F}(H)).$$

Sei dazu $E = \mathrm{F}(H) = L^H$ der Fixkörper von H. Zu zeigen ist $H = \mathrm{Aut}(L|E)$. Wir setzen $d := \#H$. Da $H \subseteq \mathrm{Aut}(L|E)$ gilt wegen 2.3.6

$$d \leq \mathrm{Aut}(L|E) \leq [L : E].$$

Wegen des Satzes vom primitiven Element gibt es ein $\pi \in L$, sodass $L = K(\pi)$. Natürlich ist dann auch $L = E(\pi)$. Wir betrachten nun das Polynom

$$f := \prod_{h \in H} (X - h(\pi)) \in L[X].$$

Wir schreiben es als

$$f = \sum_{i=0}^{d} c_i X^i, \quad c_i \in L.$$

Für $g \in H$ gilt dann

$$\sum_{i=0}^{d} g(c_i) X^i = \prod_{h \in H} (X - gh(\pi)) = f,$$

denn hier stehen dieselben Faktoren wie in f. Daher ändert sich kein Koeffizient von f, egal welches $g \in H$ man darauf anwendet, also liegen alle c_i in $E = L^H$. Das zeigt, dass $f \in E[X]$ gilt. Sein Grad ist d, und da es π als Nullstelle hat, ist der Grad des Minimalpolynoms von π über E $\leq d$.

Damit folgt auch $[L : E] \leq d$ und mit der obigen Ungleichung also

$$[L : E] = d = \#H.$$

Daher finden wir

$$H = \mathrm{Aut}(L|L^H).$$

b) Wenn $E \in \mathcal{Z}$ normal über K ist, dann gilt wegen 2.3.11 für alle $g \in G$ und alle $x \in E$: $g(x) \in E$.

Daraus folgt für alle $h \in \mathrm{Aut}(L|E)$:

$$ghg^{-1}(x) = g(g^{-1}(x)) = x,$$

denn h lässt $g^{-1}(x) \in E$ fest. Das zeigt

$$ghg^{-1} \in \mathrm{Aut}(L|E),$$

also ist dies ein Normalteiler.

Ist andererseits $H \in \mathcal{U}$ normal in G, so ist sein Fixkörper $E = L^H$ normal über K.

Denn: Ist $\beta \in E$, $g \in G$ und $h \in H$, so folgt wegen $g^{-1}hg \in H$, dass

$$g^{-1}hg(\beta) = \beta, \quad \text{also} \quad hg(\beta) = g(\beta),$$

und das zeigt $g(\beta) \in L^H$. Da aber G transitiv auf den Nullstellen des Minimalpolynoms von β über K operiert (siehe 2.3.9), liegen alle Nullstellen dieses

Minimalpolynoms in E, und damit ist E der Zerfällungskörper der Minimalpolynome seiner Elemente.

Zu guter Letzt sei H normal und $E = L^H$ sein Fixkörper. Dann liefert die Einschränkung nach E einen Homomorphismus

$$\rho : \mathrm{Gal}(L|K) \to \mathrm{Gal}(E|K),$$

denn G bewegt die Elemente von E nicht aus E heraus.

Der Kern von ρ ist gerade H, und aus

$$\#G = [L : K] = [L : E] \cdot [E : K] = \#H \cdot [E : K]$$

folgt dann, dass das Bild von ρ Ordnung $[E : K]$ hat und damit die ganze Galoisgruppe $\mathrm{Gal}(E|K)$ ist. Das zeigt die Surjektivität von ρ, und der Homomorphiesatz vermittelt den gewünschten Isomorphismus. ◯

Satz 2.3.17 Der Satz von Artin

Es seien L ein Körper und $G \subseteq \mathrm{Aut}(L)$ eine endliche Gruppe von Automorphismen von L. Weiter sei

$$K := L^G = \{\alpha \in L \mid \forall \sigma \in G : \sigma(\alpha) = \alpha\}$$

der Fixkörper von G.

Dann ist $L^G \subseteq L$ galoissch vom Grad $\#G$.

Beweis. Es sei $\alpha \in L$ beliebig. Weiter sei

$$H := \{\sigma \in G \mid \sigma(\alpha) = \alpha\}$$

der Stabilisator von α in G. Dieser habe in G Index d, und $g_1H, \ldots, g_dH$ seien die Nebenklassen.

Dann ist

$$f := \prod_{j=1}^{d} (X - g_j(\alpha)) \in L[X]$$

ein Polynom, das α als Nullstelle hat. Es hat in L die d einfachen Nullstellen $g_j(\alpha)$, $1 \le j \le d$. Diese bilden den G-Orbit von α.

Nun zeigen wir, dass $f \in K[X]$ gilt. Dazu schreiben wir uns

$$f = \sum_{i=0}^{d} c_i X^i, \quad c_i \in L$$

hin. Wir müssen $c_i \in K$ nachweisen. Es sei $\sigma \in G$. Dann ist

$$\{g_1(\alpha), \ldots, g_d(\alpha)\} = \{\sigma g_1(\alpha), \ldots, \sigma g_d(\alpha)\},$$

aber $\sigma g_j(\alpha)$ ist Nullstelle von $\sum(\sigma c_i)X^i$, da

$$\sum(\sigma(c_i))(\sigma(g_j(\alpha)))^i = \sigma(\sum_{i=0}^{d} c_i(g_j(\alpha))^i) = \sigma(f(g_j(\alpha))) = 0.$$

Die beiden normierten Polynome f und $\sum \sigma(c_i)X^i$ vom Grad d haben also die selben d Nullstellen, und stimmen daher überein.

Da dies für alle $\sigma \in G$ gilt, sind die Koeffizienten von f alle in K.

Es folgt, dass $K \subseteq L$ galoissch ist, denn alle Minimalpolynome zerfallen über L in Linearfaktoren und haben keine mehrfachen Nullstellen.

Zudem zeigt es, dass $K \subseteq L$ eine endliche Erweiterung ist, denn ansonsten gäbe es – wegen der Algebraizität – endliche Galoiserweiterungen von K in L, die über K beliebig hohen Grad besitzen. Da diese jeweils von einem primitiven Element erzeugt werden, widerspricht das der Tatsache, dass der Grad dessen Minimalpolynoms nicht größer als $\#G$ sein kann.

Wäre nun $G \neq \mathrm{Gal}(L|K)$, so wäre es eine echte Untergruppe der Galoisgruppe, und damit der Fixkörper – nach dem Hauptsatz – eine echte Erweiterung von K. Das widerspricht der Definition von K und zeigt

$$G = \mathrm{Gal}(L|K).$$

Damit ist $\#G$ der Grad von $K \subseteq L$. ◯

2.4 Beispiele und Anwendungen

Da wir nachher mehrfach auf die folgende Situation stoßen, fangen wir mit einem Hilfssatz an.

Hilfssatz 2.4.1 Ein Körperturm

Es sei $K \subseteq L$ eine Galoiserweiterung vom Grad p^d, wobei p eine Primzahl ist. Dann gibt es eine Folge von Körpererweiterungen

$$K := K_0 \subset K_1 \subset \ldots \subset K_{d-1} \subset K_d = L,$$

wobei $K_i \subseteq K_{i+1}$ jeweils Grad p hat.

Beweis. Die Galoisgruppe G von $K \subseteq L$ ist eine p-Gruppe. Es gibt daher eine Kompositionsreihe, deren Kompositionsfaktoren einfache p-Gruppen sind. Diese sind wegen 1.2.4 zyklische Gruppen der Ordnung p. Sei

$$\{e\} = G_d \leq G_{d-1} \leq \ldots \leq G_1 \leq G_0 = G$$

solch eine Kompositionsreihe. Dann hat G_i genau p^{d-i} Elemente.

Dann ist der Fixkörper $K_i := L^{G_i}$ ein Teilkörper von L, und für den Körpergrad gilt, da $K_i \subseteq L$ galoissch ist und G_i die Galoisgruppe:

$$[L : K_i] = p^{d-i}, \quad \text{also} \quad [K_i : K] = p^i.$$

Das zeigt die Behauptung.

Es gilt sogar jeweils, dass $K_i \subseteq K_{i+1}$ normal ist. ◯

Satz 2.4.2 Fundamentalsatz der Algebra

Der Körper $\mathbb{C}$ ist algebraisch abgeschlossen.

Beweis. Es sei $\mathbb{C} \subseteq K$ eine endliche Körpererweiterung. Wir müssen zeigen, dass $K = \mathbb{C}$ gilt.

Dazu sei L die normale Hülle von K über $\mathbb{R}$ (auch von $\mathbb{R}$ ist K eine endliche Erweiterung). Es sei G die Galoisgruppe von L über $\mathbb{R}$. Diese ist endlich. Daher gibt es in G eine 2-Sylowgruppe S.

Dann ist der Körpergrad von L über L^S die maximale Zweierpotenz in $[L : \mathbb{R}]$, also ist $\mathbb{R} \subseteq L^S$ eine Erweiterung von ungeradem Grad. Wenn $\alpha \in L^S$ ein primitives Element dieser Erweiterung bezeichnet, so hat sein Minimalpolynom über $\mathbb{R}$ ungeraden Grad.

Nach dem Zwischenwertsatz hat dieses Polynom also eine reelle Nullstelle, und kann daher nur irreduzibel sein, wenn $\alpha \in \mathbb{R}$. Es folgt $\mathbb{R} = L^S$, und damit hat L über $\mathbb{C}$ eine Zweierpotenz als Grad.

Wäre nun $\mathbb{C} \neq L$, so läge nach dem Hilfssatz 2.4.1 eine quadratische Erweiterung von $\mathbb{C}$ in L. Solch eine Erweiterung aber gibt es nicht, denn jede komplexe Zahl besitzt eine komplexe Quadratwurzel.

Das zeigt $L = \mathbb{C}$, und damit auch $K = \mathbb{C}$. ◯

Folgerung 2.4.3 Der algebraische Abschluss von $\mathbb{Q}$

Eine mögliche Wahl für den ursprünglich so mühsam konstruierten algebraischen Abschluss von $\mathbb{Q}$ lässt sich nun besser greifbar angeben:

$$\mathbb{Q}^{\text{alg}} = \{\alpha \in \mathbb{C} \mid \alpha \text{ algebraisch über } \mathbb{Q}\}.$$

Bemerkung 2.4.4 Konstruktionen mit Zirkel und Lineal

Schon seit Urzeiten interessiert man sich für Konstruktionen ebener geometrischer Objekte mit Zirkel und Lineal. Um dies algebraisch fassen zu können interpretiert man die Ebene als $\mathbb{C}$. Nun normiert man weiter einen Punkt als 0 und einen als 1. Dann kann man alle rationalen Zahlen mit Zirkel und Lineal konstruieren. Für die ganzen ist das klar, und den Rest erledigt der Strahlensatz.

Sind zu 0 und 1 noch weitere Punkte gegeben, so lässt sich deren Summe konstruieren (Konstruktion eines Parallelogramms) und auch deren Produkt (Abtragen eines Winkels und zentrische Streckung). Auch die Division ist durchführbar, also ist die Menge aller Punkte, die man so konstruieren kann, ein Teilkörper von $\mathbb{C}$.

Andererseits löst nach dem Satz von Pythagoras jeder Konstruktionsschritt mit Zirkel und Lineal eine Polynomgleichung von Grad 2. Das motiviert hoffentlich die folgende Definition.

Definition 2.4.5 Konstruierbarkeit

Es sei $K \subseteq \mathbb{C}$ ein Teilkörper. Eine komplexe Zahl z heißt *über K konstruierbar*, wenn $K(z)$ aus K durch sukzessives Adjungieren von Quadratwurzeln entsteht, wenn es also Zwischenkörper

$$K = K_0 \subseteq K_1 \subseteq K_2 \subseteq \ldots \subseteq K_r = K(z)$$

gibt, sodass $K_i \subseteq K_{i+1}$ für alle $0 \leq i \leq r-1$ Grad 2 hat.

Hilfssatz 2.4.6 Ein galoistheoretisches Kriterium

Es sei $K \subseteq \mathbb{C}$ ein Teilkörper und $z \in \mathbb{C}$. Dann ist z genau dann über K konstruierbar, wenn es über K algebraisch ist und der Zerfällungskörper seines Minimalpolynoms über K eine Zweierpotenz als Grad hat.

Beweis. Zunächst sei vorausgesetzt, dass z über K konstruierbar ist.

Wir zeigen scheinbar allgemeiner: Es sei $K \subseteq L$ eine galoissche Körpererweiterung vom Grad 2^n und $f \in L[X]$ ein irreduzibles quadratisches Polynom. Weiter sei α eine Nullstelle von f und M die normale Hülle von $L(\alpha)$ über K. Dann ist der Grad von M über K eine Zweierpotenz.

Denn: M entsteht aus L durch die Hinzunahme der Wurzeln der Polynome $\sigma(f)$, wobei σ die Galoisgruppe von L über K durchläuft. Da diese jedes Mal eine Erweiterung vom Grad 1 oder 2 ist, erhält man insgesamt wegen der Multiplikativität der Körpergrade eine Zweierpotenz als Erweiterungsgrad.

Dies zeigt, dass die normale Hülle von $K(z)$ über K eine Zweierpotenz als Grad hat.

Umgekehrt sei nun die normale Hülle von $L = K(z)$ über K eine Erweiterung vom Zweierpotenzgrad. Dann liefert 2.4.1 genau das, was wir brauchen, denn es impliziert, dass jedes Element der normalen Hülle sich mit Zirkel und Lineal konstruieren lässt. Dies gilt insbesondere für z, und damit ergibt sich $K(z)$ aus K durch sukzessive quadratishe Erweiterungen. ◯

Beispiel 2.4.7 Kreisteilungspolynome

Wir erinnern an die Kreisteilungspolynome $\Phi_n(X) \in \mathbb{Z}[X]$, die wir in EAZ, 4.2.5, eingeführt haben. Sie werden rekursiv durch die folgende Vorgabe definiert:

$$\Phi_1 := X - 1, \quad \Phi_n := \frac{X^n - 1}{\prod\limits_{d|n,\ d\neq n} \Phi_d}.$$

Die Nullstellen von Φ_n in $\mathbb{C}$ sind die Einheiten von Ordnung n. Das ist auch der Grund, weshalb die Φ_d alle paarweise teilerfremde Teiler von $X^n - 1$ sind. Die Polynomdivision geht wegen des Gauß-Lemmas in $\mathbb{Z}[X]$ auf, da die Nullstellen des Nenners passen und dieser normiert und ganzzahlig ist.

Wir finden

$$\Phi_2 = X + 1,\ \Phi_3 = X^2 + X + 1,\ \Phi_4 = X^2 + 1,\ \Phi_5 = X^4 + X^3 + X^2 + X + 1 \ldots$$

Aus der Übung kennen wir schon die Polynome

$$\Phi_p = \frac{X^p - 1}{X - 1}$$

für Primzahlen p und wissen, dass sie irreduzibel sind. Das wollen wir jetzt für alle Kreisteilungspolynome zeigen.

Dazu sei $\zeta \in \mathbb{C}$ eine Nullstelle von Φ_n. Das Minimalpolynom von ζ sei $f \in \mathbb{Q}[X]$. Dann sagt uns das Gauß-Lemma 2.2.5, dass f in Wirklichkeit schon in $\mathbb{Z}[X]$ liegt. Denn:

$$X^n - 1 = f \cdot h = \frac{f}{\mathrm{Inh}(f)} \cdot \mathrm{Inh}(f)h$$

ist eine Zerlegung in zwei ganzzahlige Faktoren, und der Leitkoeffizient von $X^n - 1$ ist das Produkt von deren Leitkoeffizienten. Also sind diese ganzzahligen Faktoren (bis aufs Vorzeichen) normiert.

Weiter sei nun p eine Primzahl, die n nicht teilt. Dann ist auch ζ^p eine Nullstelle von Φ_n. Es sei $g \in \mathbb{Z}[X]$ das Minimalpolynom von ζ^p.

Wir zeigen nun $f = g$.

Annahme: $f \neq g$.

Da beide Polynome irreduzible, ganzzahlige, normierte Teiler von $X^n - 1$ sind, gibt es (wieder mit Gauß) ein normiertes Polynom $h \in \mathbb{Z}[X]$ mit

$$X^n - 1 = fgh.$$

Wir betrachten die Koeffizienten modulo p und erhalten so Polynome $\tilde{f}, \tilde{g}, \tilde{h} \in \mathbb{F}_p[X]$ mit

$$X^n - 1 = \tilde{f}\tilde{g}\tilde{h}.$$

Da $g(\zeta^p) = 0$ gilt, teilt f das Polynom $g(X^p)$. Dies geht wieder ganzzahlig und stimmt daher auch nach Reduktion modulo p:

$$\tilde{f}|\tilde{g}(X^p) = (\tilde{g}(X))^p.$$

Das heißt aber auch, dass X^n-1 im algebraischen Abschluss von $\mathbb{F}_p$ eine doppelte Nullstelle hat. Die Ableitung jedoch ist nX^{n-1} und hat (da $n \notin p\mathbb{Z}$) nur die Nullstelle 0, die keine Nullstelle von $X^n - 1$ ist. Also gibt es diese doppelte Nullstelle nicht und bringt somit unsere Annahme zu Fall.

Das zeigt, dass $f = g$ gilt.

Wenn nun ξ irgendeine Nullstelle von Φ_n ist, so gilt $\xi = \zeta^k$, $k \in \mathbb{N}$ geeignet, denn ζ erzeugt die Gruppe der n-ten Einheitswurzeln in $\mathbb{C}$. Da auch ξ Ordnung n hat, ist k zu n teilerfremd.

Wir schreiben $k = p_1 \cdot p_2 \cdot \ldots \cdot p_r$ mit Primzahlen p_i.

Dann ist aber f das Minimalpolynom von ζ^{p_1}, also auch das von $(\zeta^{p_1})^{p_2} = \zeta^{p_1 p_2}$, also auch das von $\ldots \zeta^k$.

Daher hat f Grad $\#((\mathbb{Z}/n\mathbb{Z})^\times) = \deg(\Phi_n)$, und es folgt, dass dieses Polynom irreduzibel ist.

Das zeigt uns, dass $L := \mathbb{Q}(\zeta)$ eine Erweiterung von $\mathbb{Q}$ vom Grad $\varphi(n)$ ist, und alle Nullstellen von Φ_n liegen schon in L. Das ist also eine normale Erweiterung und damit ($\mathbb{Q}$ ist ja perfekt) auch galoissch. Die Galoisgruppe ist wegen 2.3.9 isomorph zu einer Untergruppe von $(\mathbb{Z}/n\mathbb{Z})^\times$. Da sie dieselbe endliche Kardinalität hat, ist sie zur ganzen Einheitengruppe von $\mathbb{Z}/n\mathbb{Z}$ isomorph.

Insbesondere sagt nun 2.4.6, dass das regelmäßige n-Eck genau dann (über $\mathbb{Q}$) mit Zirkel und Lineal konstruierbar ist, wenn $\varphi(n)$ eine Zweierpotenz ist. Dies ist (wie man sich noch überlegen müsste) genau dann der Fall, wenn n von der Gestalt

$$n = 2^e \cdot p_1 \cdot \ldots \cdot p_r,$$

wobei $p_1, \ldots, p_r$ paarweise verschiedene Primzahlen der Gestalt $2^f + 1$ sind. Solche Primzahlen heißen Fermatzahlen. Es ist bis heute ungeklärt, ob es unendlich viele davon gibt. Aber einige kennt man:

$$3,\ 5,\ 17,\ 257,\ 65537, \ldots$$

Beispiel 2.4.8 Gallien...

Eine der klassischen Fragen der Geometrie ist, ob man jeden gegebenen Winkel mit Zirkel und Lineal dreiteilen kann. Die Antwort hierauf ist nun klar: das geht nicht.

Als Beispiel nehmen wir den Winkel $120^\circ = 2\pi/3$, den man natürlich konstruieren kann, da er zum regelmäßigen Dreieck gehört. Wenn man ihn dreiteilen könnte, dann hätte man ein regelmäßiges Neuneck mit Zirkel und Lineal konstruiert, aber das geht nicht, da $\varphi(9) = 6$ keine Zweierpotenz ist.

Leider lassen sich immer noch nicht alle potentiellen Trisektierer von diesem Beispiel abschrecken, und es gibt immer wieder ernstgemeinte Lösungsversuche für die Dreiteilung eines gegebenen Winkels mit Zirkel und Lineal.

Beispiel 2.4.9 Die Quadratur des Kreises

Es ist nicht möglich, ausgehend von $\mathbb{Q}$ mit Zirkel und Lineal ein Quadrat zu konstruieren, dessen Flächeninhalt π ist.

Dazu muss man wissen, dass π nicht die Nullstelle eines rationalen Polynoms mit einer Zweierpotenz als Grad ist.

Es langt also insbesondere auch zu zeigen, dass π transzendent ist, was wir schon einmal in 2.1.2 als Faktum festgehalten hatten.

Nach diesem Zwischenspiel verlassen wir die Geometrie wieder.

Definition 2.4.10 Radikalerweiterungen

Es sei K ein Körper der Charakteristik 0. Eine endliche Körpererweiterung $K \subseteq L$ heißt eine *Radikalerweiterung*, wenn ein $\alpha \in L$ und ein $n \in \mathbb{N}$ existieren, sodass

$$L = K(\alpha), \quad \alpha^n \in K.$$

Die Erweiterung heißt *durch Radikale auflösbar*, wenn es Zwischenkörper

$$K = K_0 \subseteq K_1 \subseteq K_2 \subseteq \cdots \subseteq K_r = L$$

gibt, sodass jeweils $K_i \subseteq K_{i+1}$ eine Radikalerweiterung ist.

Ein Polynom $f \in K[X]$ ist durch Radikale lösbar, wenn sein Zerfällungskörper über K durch Radikale auflösbar ist.

NB: Wenn man das in Charakteristik ungleich 0 machen will, so muss man noch Artin-Schreier[8] Erweiterungen zulassen und erhält dann ein ganz ähnliches Resultat wie das folgende.

[8] Otto Schreier, 1901-1929

Bemerkung 2.4.11 Lösungsformeln

Es ist das Ausgangsproblem der Algebra, für ein gegebenes Polynom $f \in K[X]$ eine Formel für die Nullstellen zu finden. Diese Formel soll algebraisch funktionieren, womit man meint, dass für eine Nullstelle α von f stets gilt: $K \subseteq K(\alpha)$ ist eine Radikalerweiterung.

Das heißt konkret: α lässt sich ausgehend von den Koeffizienten von f durch sukzessives Ziehen von n-ten Wurzeln und Auswerten von rationalen Funktionen angeben.

Zum Beispiel ist für $f = aX^2 + bX + c$ die bekannte Formel

$$x_{1/2} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

solch eine Vorschrift, denn man bildet erst den Ausdruck $b^2 - 4ac$, das ist eine rationale Funktion, zieht daraus die Quadratwurzel und bildet dann nochmals eine rationale Funktion.

Für kubische Polynome ist die bekannte Lösungsformel auch von diesem Typ, und auch für Polynome vom Gad 4 gibt es solch eine Formel.

Die naheliegende Frage war, ob es für jedes Polynom solch eine Lösungsformel geben kann. In unserer jetzigen Terminologie heißt das:

Ist jede endliche Galoiserweiterung durch Radikale auflösbar?

Hilfssatz 2.4.12 Noch ein Galoistheoretisches Argument

Es sei $K \subseteq L$ eine endliche Galoiserweiterung vom Grad n, die Charakteristik von K sei 0.

Dann ist $K \subseteq L$ genau dann durch Radikale auflösbar, wenn die Galoisgruppe $G = \mathrm{Gal}(L|K)$ auflösbar ist.

Beweis. Um gleich einfacher argumentieren zu können, machen wir erst einen Reduktionsschritt.

Da n-te Einheitswurzeln immer durch Radikale erreichbar sind, ist die Frage einer Lösungsformel unabhängig davon, ob man erst zu K noch Einheitswurzeln hinzunimmt oder nicht.

Auf der anderen Seite sei M der Körper, der aus L durch Adjunktion einer n-ten Einheitswurzel ζ entsteht. Dieser ist dann auch über K normal. Es gilt

$$\mathrm{Gal}(L|K) \cong \mathrm{Gal}(M|K)/\mathrm{Gal}(M|L),$$

aber $\mathrm{Gal}(M|L)$ ist abelsch und daher sind die beiden anderen Gruppen wegen 1.2.3 simultan auflösbar oder nicht.

Andererseits sind auch die Erweiterungen $K \subseteq K(\zeta) \subseteq M$ alle galoissch und wieder $\mathrm{Gal}(K(\zeta)|K)$ abelsch, also $\mathrm{Gal}(M|K)$ und $\mathrm{Gal}(M|K(\zeta))$ simultan auflösbar oder nicht.

Zusammen genommen ist $\mathrm{Gal}(L|K)$ genau dann auflösbar, wenn $\mathrm{Gal}(M|K(\zeta))$ dies ist.

Wir dürfen also ohne Einschränkung annehmen, dass K ein n-te Einheitswurzel enthält. Weder die Frage nach der Auflösbarkeit durch Radikale noch die Frage nach der Auflösbarkeit der Galoisgruppe wird davon berührt.

Wir nehmen zunächst an, die Galoisgruppe G sei auflösbar. Dann hat eine Kompositionsreihe

$$\{e\} := G_r \subset G_{r-1} \subset \cdots \subset G_1 \subset G_0 = G$$

von G einfache abelsche Gruppen als Kompositionsfaktoren, und diese sind zyklisch von Primzahlordnung. Für die Fixkörper $K_i := L^{G_i}$ gilt demnach, dass $K_i \subset K_{i+1}$ eine Galoiserweiterung von Primzahlgrad p ist. Da diese Primzahl p ein Teiler von n ist, liegt in K eine primitive p-te Einheitswurzel. Eine Übungsaufgabe zeigt dann, dass K_{i+1} durch Adjunktion einer p-ten Wurzel eines Elements aus K_i zu K_i erzeugt wird.

Daher ist $K \subseteq L$ durch Radikale auflösbar.

Ist andererseits die Erweiterung durch Radikale auflösbar, so ist jede dieser Radikalerweiterungen schon galoissch (da die richtigen Einheitswurzeln schon in K liegen). Wir erhalten durch den Hauptsatz der Galoistheorie eine Normalreihe in G mit zyklischen Faktorgruppen, und damit ist G auflösbar. ◯

Bemerkung 2.4.13 Nichtauflösbare Gleichungen

Jetzt ist es schon fast nicht mehr schwer, Polynome anzugeben, deren Zerfällungskörper nicht durch Radikale auflösbar ist. Wir wissen ja, dass die alternierende Gruppe A_n für $n \geq 5$ einfach und nichtkommutativ ist, also ist S_n in diesem Fall nicht auflösbar. Es langt also, ein Polynom anzugeben, dessen Zerfällungskörper als Galoisgruppe eine Gruppe isomorph zu $S_n,\ n \geq 5,$ hat.

Für $n = 5$ mit $\mathbb{Q}$ als Grundkörper ist das eine Übungsaufgabe.

Eine andere, mehr geometrische Situation ist die, dass man für einen Körper k den Polynomring $R = k[T_1, \ldots, T_n]$ betrachtet oder besser noch dessen Quotientenkörper $L = k(T_1, \ldots, T_n)$.

Auf diesem operiert die symmetrische Gruppe S_n durch Vertauschung der Variablen, und damit sitzt S_n in der Automorphismengruppe von L. Mit dem Satz von Artin (2.3.17) ist dann S_n die Galoisgruppe von L über dem Fixkörper $K := L^{S_n}$. Daher ist das Minimalpolynom eines primitiven Elements für diese Erweiterung nicht durch Radikale auflösbar.

Das erklärt, weshalb man sich umsonst die Zähne daran ausgebissen hat, Lösungsformeln für Polynome vom Grad 5 und größer zu finden.

Um das ganze noch etwas substanzieller zu beschreiben ist es vielleicht nicht falsch, den Fixkörper noch auszurechnen. Dazu betrachten wir das Minimalpolynom von T_1 über K. Das ist zwar kein primitives Element, aber wir kennen das Minimalpolynom m, denn seine Nullstellen sind ja die Bahn von T_1 unter der Galoisgruppe, also $T_1, \ldots, T_n$. Das Minimalpolynom ist also

$$m = (X - T_1) \cdot (X - T_2) \cdot \ldots \cdot (X - T_n).$$

Wenn man dies ausmultipliziert, so ergibt sich

$$m = \sum_{i=0}^{n} (-1)^i \sigma_i(T_1, \ldots, T_n) X^{n-i}.$$

Die Koeffizienten hierbei sind die *elementarsymmetrischen Polynome*, die durch

$$\sigma_i(T_1, \ldots, T_n) := \sum_{1 \le j_1 < j_2 < \cdots < j_i \le n} T_{j_1} \cdot \ldots \cdot T_{j_i}$$

definiert sind. Speziell sind

$$\begin{aligned}
\sigma_0(T_1, \ldots, T_n) &= 1, \\
\sigma_1(T_1, \ldots, T_n) &= T_1 + \ldots + T_n \\
\sigma_2(T_1, \ldots, T_4) &= T_1T_2 + T_1T_3 + T_1T_4 + T_2T_3 + T_2T_4 + T_3T_4 \\
\sigma_n(T_1, \ldots, T_n) &= T_1 \cdot \ldots \cdot T_n.
\end{aligned}$$

Die elementarsymmetrischen Polynome erzeugen über k einen Teilkörper von L, über dem $T_1, \ldots, T_n$ algebraisch sind und ein gemeinsames Minimalpolynom vom Grad n haben. Damit ist der Erweiterungsgrad von L über $k(\sigma_1, \ldots, \sigma_n)$ höchstens $n!$, und da die σ_i alle im Fixkörper der S_n-Operation auf L liegen, ist

$$K = k(\sigma_1, \ldots, \sigma_n)$$

Insbesondere sind die elementarsymmetrischen Polynome eine Transzendenzbasis von L über k, denn der Transzendenzgrad ist ja n.

Beispiel 2.4.14 Rationales Beispiel

Über $\mathbb{Q}$ sollte man natürlich auch ein Beispiel eines Polynoms mit nicht auflösbarer Galoisgruppe finden.

Konkret sei

$$f = X^5 + 5X^4 + 4X + 1 \in \mathbb{Z}[X].$$

Dieses Polynom ist über $\mathbb{F}_5$ irreduzibel. Daher ist es auch über $\mathbb{Z}$ nicht in Faktoren zerlegbar und somit wegen Gauß auch über $\mathbb{Q}$ irreduzibel. Es hat drei reelle

Nullstellen, und zwei Nullstellen sind nicht reell. Die komplexe Konjugation operiert auf den Nullstellen also über eine Transposition.

Nun betrachten wir die Galoisgruppe des Zerfällungskörpers von f als Untergruppe in der symmetrischen Gruppe auf den Nullstellen des Polynoms. Da sie transitiv auf den Nullstellen von f operiert, enthält sie einen Fünfzykel. Eine Transposition liegt auch darin. Wegen EAZ 3.5.6 muss dann aber die Galoisgruppe schon die ganze symmetrische Gruppe sein.

Es ist noch immer nicht von allen endlichen Gruppen bekannt, ob sie Galoisgruppen für eine Galoiserweiterung mit Grundkörper $\mathbb{Q}$ sind. Die Untersuchung dieser und ähnlich gelagerter Fragen nennt man inverse Galoistheorie.

Satz 2.4.15 Abelsche Galoisgruppen

Jede endliche abelsche Gruppe G ist isomorph zur Galoisgruppe einer Galoiserweiterung $\mathbb{Q} \subseteq K$.

Beweis. Es sei G eine endliche abelsche Gruppe.

Nach dem Hauptsatz über endlich erzeugte abelsche Gruppen ist G also ein direktes Produkt von zyklischen Gruppen. Wir schreiben

$$G = \prod_{i=1}^{r} \mathbb{Z}/k_i\mathbb{Z},\ 2 \leq k_i \in \mathbb{N}.$$

Wegen EAZ, 4.2.7, gibt es Primzahlen

$$p_1 < p_2 < \cdots < p_r,$$

sodass jeweils k_i ein Teiler von $p_i - 1$ ist.

Nun setzen wir

$$n := p_1 \cdot \ldots \cdot p_r,\quad \zeta = \cos(2\pi/n) + \mathrm{i}\sin(2\pi/n).$$

Dann ist $L := \mathbb{Q}(\zeta)$ eine Galoiserweiterung von $\mathbb{Q}$ mit Galoisgruppe

$$(\mathbb{Z}/n\mathbb{Z})^\times \cong \mathbb{F}_{p_1}^\times \times \ldots \times \mathbb{F}_{p_r}^\times,$$

wobei wir 2.4.7 und den Chinesischen Restsatz bemühen. Nun ist $\mathbb{F}_{p_i}^\times$ aber zyklisch von Ordnung $p_i - 1$, also gibt es eine Untergruppe $H_i \subseteq \mathbb{F}_{p_i}^\times$ von Ordnung $(p_i - 1)/k_i$, und es gilt

$$\mathbb{F}_{p_i}^\times / H_i \cong \mathbb{Z}/k_i\mathbb{Z}.$$

Dann ist aber wegen des Hauptsatzes der Galoistheorie

$$(\mathbb{Z}/n\mathbb{Z})^\times / (H_1 \times \ldots \times H_r) \cong G$$

die Galoisgruppe von $K := L^{(H_1 \times \ldots \times H_r)}$ über $\mathbb{Q}$. ◯

Bemerkung 2.4.16 Einbettungen

Es sei $K \subseteq L$ separabel vom Grad n. Dann gibt es ein primitives Element α für diese Erweiterung, $L = K(\alpha)$, und das Minimalpolynom von α hat in der normalen Hülle $\widetilde{L}$ von L n paarweise verschiedene Nullstellen.

Dann gibt es aber auch genau n K-Algebrenhomomorphismen von L nach $\widetilde{L}$, die durch

$$a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} \mapsto a_0 + a_1\beta + \cdots + a_{n-1}\beta^{n-1}$$

gegeben sind, wobei β die Nullstellen des Minimalpolynoms von α durchläuft.

Diese sind linear unabhängig über $\widetilde{L}$. Das sieht man aus dem folgenden Hilfssatz.

Hilfssatz 2.4.17 Lemma von Artin

Es seien Γ eine Gruppe und F ein Körper. Dann ist die Menge

$$\mathrm{Hom}_{\mathrm{Gruppen}}(\Gamma, F^\times) \subseteq \mathrm{Abb}(\Gamma, F)$$

linear unabhängig.

Beweis. Wenn nicht, dann gäbe es eine kleinste natürliche Zahl n und n paarweise verschiedene solche Homomorphismen

$$\chi_i : \Gamma \to F^\times,\ 1 \leq i \leq n,$$

sodass für ein von Null verschiedenes Tupel $(f_1, \ldots, f_n) \in F^n$ die Gleichheit

$$f_1\chi_1 + f_2\chi_2 + \cdots + f_n\chi_n = 0 \qquad (*)$$

gilt. Da n kleinstmöglich ist, sind alle f_i nicht 0.

Da die χ_i paarweise verschieden sind, gibt es ein $\gamma \in \Gamma$ mit

$$\chi_1(\gamma) \neq \chi_n(\gamma).$$

Dieses γ merken wir uns. Da die χ_i multiplikative Homomorphismen sind, gilt für alle $g \in \Gamma$:

$$\chi_i(\gamma g) = \chi_i(\gamma)\chi_i(g).$$

Wir werten $(*)$ bei γg aus und sehen dann (da g beliebig ist):

$$f_1\chi_1(\gamma)\chi_1 + \chi_2(\gamma)f_2\chi_2 + \ldots \chi_n(\gamma)f_n\chi_n = 0.$$

Andererseits können wir die Gleichung $(*)$ auch nehmen und mit $\chi_1(\gamma)$ multiplizieren:

$$f_1\chi_1(\gamma)\chi_1 + \chi_1(\gamma)f_2\chi_2 + \ldots \chi_1(\gamma)f_n\chi_n = 0.$$

Zieht man die so erhaltenen Gleichungen voneinander ab, so folgt

$$(\chi_2(\gamma) - \chi_1(\gamma))f_2\chi_2 + \cdots + (\chi_n(\gamma) - \chi_1(\gamma))f_n\chi_2.$$

Da hier die Anzahl der Summanden kleiner ist als n, müssen alle Vorfaktoren 0 sein. Es folgt

$$(\chi_n(\gamma) - \chi_1(\gamma))f_n = 0,$$

aber das wiederum erzwingt wegen der Wahl von γ, dass $f_n = 0$.

Ein Widerspruch. ◯

Mit diesem Lemma beweisen wir jetzt einen Fall des Satzes von der normalen Basis. Für den anderen Fall brauchen wir ein anderes Argument.

Folgerung 2.4.18 Satz von der Normalbasis

Es sei $K \subseteq L$ eine endliche Galoiserweiterung mit Galoisgruppe G.

Dann gibt es ein $\beta \in L$, sodass $\{\tau(\beta) \mid \tau \in G\}$ eine K-Basis von L ist.

Beweis. Wir unterscheiden zwei Fälle, die nicht disjunkt sind, aber doch alles überdecken.

Fall 1: G ist zyklisch. Es sei $\sigma \in G$ ein Erzeuger, n sei der Grad der Erweiterung, und daher also auch die Ordnung von σ.

Die Abbildungen

$$\sigma^i : L \to L, \quad 0 \leq i \leq n-1,$$

sind linear unabhängig über L, denn ihre Einschränkungen auf $L^\times$ sind das nach dem Lemma 2.4.17 von Artin. Daher ist $X^n - 1$ das Minimalpolynom von σ aufgefasst als K-Vektorraumendomorphismus von L.

Wir statten L mit einer Struktur als $K[X]$-Modul aus, indem wir definieren:

$$(K[X], L) \ni (f, l) \mapsto (f(\sigma))(l) \in L.$$

Der Elementarteilersatz sagt uns, dass es normierte Polynome $f_1, \ldots, f_r \in K[X]$ gibt mit

$$f_1 \mid f_2 \mid \cdots \mid f_r \quad \text{und} \quad L \cong K[X]/(f_1) \times \cdots \times K[X]/(f_r).$$

Da f_r ein Vielfaches der anderen ist, ist f_r das Minimalpolynom von σ, also $f_r = X^n - 1$. Da dann aber schon $K[X]/(f_r)$ Dimension n hat, sind die anderen Polynome $f_1, \ldots, f_{r-1}$ alle 1.

Das heißt:

$$L \cong K[X]/(X^n - 1).$$

(Isomorphismus von $K[X]$-Moduln.)

Bezüglich der Basis $\{1, X, X^2 \dots X^{n-1}\}(\text{mod } X^n - 1)$ beschreibt sich die Multipikation mit X durch die Matrix

$$\begin{pmatrix} 0 & 0 & \dots & 0 & 1 \\ 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \dots & 0 & 1 & 0 \end{pmatrix}.$$

Diese beschreibt dann aber auch die Multiplikation mit σ auf L bezüglich einer geeigneten Basis. Nennt man den ersten Basisvektor β, so tut der, was er soll.

Das beendet den ersten Fall. Insbesondere beinhaltet dieser den Fall endlicher Körper und wir haben alles gezeigt, wenn der folgende Fall 2 auch erfolgreich behandelt ist.

Fall 2: K ist unendlich. Wieder sei n der Grad der Erweiterung. Nach dem Satz 2.3.15 vom primitiven Element gibt es ein $\alpha \in L$, sodass $L = K(\alpha)$.

Wir numerieren die Elemente aus G durch und nennen sie $\sigma_1, \dots \sigma_n$. Dabei soll $\sigma_1 = \text{Id}_L$ gelten.

Weiter setzen wir

$$a_i := \sigma_i(\alpha) \in L$$

und

$$g_j := \prod_{i \neq j} \frac{X - a_i}{a_j - a_i} \in L[X].$$

Dieses Polynom ist 0 bei $x = a_i,\ i \neq j$, und 1 bei $x = a_j$.

Da der Grad nicht größer ist als $n - 1$, gilt

$$g_1 + g_2 + \dots + g_n = 1. \qquad (*)$$

Das ist ein Spezialfall der Interpolationsformel von Lagrange.

Jeder Automorphismus $\sigma \in G$ wirkt auch auf den Polynomen in $L[X]$, durch Anwendung auf die Koeffizienten. Hierbei gilt für alle $h \in L[X],\ x \in L$:

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

Insbesondere sieht man an den Werten bei den a_i, dass

$$\sigma_j(g_1) = g_j.$$

Es sei $f := \prod_{i=1}^{n}(X - a_i)$.

Dann ist f das Produkt der verschiedenen Linearfaktoren von $g_i g_j$, also ein Teiler dieses Produkts. Daher ist f wegen $(*)$ auch ein Teiler von

$$g_i^2 - g_i = -\sum_{j \neq i}(g_i g_j).$$

Für die Matrix

$$A := (\sigma_i(g_j))_{i,j} \in L[X]^{n \times n}$$

ergibt sich daher aus $(*)$, dass

$$A \cdot A^\top \equiv I_n \pmod{f}.$$

Diese Kongruenzbedingung ist eintragsweise zu verstehen.

Insbesondere ist die Determinante von $A \cdot A^\top$ modulo f gleich 1, also ein von 0 verschiedenes Polynom, und damit auch die von A selbst.

Da K unendlich ist, gibt es ein $u \in K$, sodass

$$\det((\sigma_i(g_j(u)))_{i,j}) \neq 0.$$

Mit $g_j(u) = \sigma_j(g_1(u))$ folgt für $\beta := g_1(u)$, dass

$$\det(\sigma_i(\sigma_j(\beta))) \neq 0.$$

Ist nun $(\lambda_1, \ldots, \lambda_n)^\top \in K^n$ mit

$$\sum \lambda_j \sigma_j(\beta) = 0,$$

so gilt auch für jedes i

$$\sum \lambda_j \sigma_i \sigma_j(\beta) = \sigma_i(\sum \lambda_j \sigma_j(\beta)) = 0,$$

also

$$(\sigma_i(\sigma_j(\beta)))_{i,j} \cdot (\lambda_1, \ldots, \lambda_n)^\top = 0,$$

aber das erzwingt wegen der Regularität der beteiligten Matrix $\lambda_1 = \ldots = \lambda_n = 0$, und damit sind die Elemente $\sigma_j(\beta)$, $1 \leq j \leq n$, über K linear unabhängig. ◯

Kapitel 3

Noch mehr Ringtheorie

3.1 Noethersche Ringe und Moduln

Hier lernen wir einen hilfreichen Endlichkeitsbegriff kennen.

Definition 3.1.1 Der Emmy-Award

a) Es seien R ein kommutativer Ring und M ein R-Modul. Dann heißt M *noethersch*[1], falls jeder R-Untermodul von M endlich erzeugt ist.

Der Ring R selbst heißt *noethersch*, wenn jedes Ideal in R endlich erzeugt ist, wenn er also ein noetherscher R-Modul ist.

b) Wenn R nicht kommutativ ist, dann unterscheiden sich im Allgemeinen Links-R-Moduln (mit der Eigenschaft $(rs)m = r(sm)$) und Rechts-R-Moduln (mit der Eigenschaft $(rs)m = s(rm)$). Entsprechend gibt es linksnoethersche Ringe und rechtsnoethersche Ringe, wir wollen das aber nicht ausführlicher diskutieren.

Beispiel 3.1.2 alles sieht so noethersch aus!

a) Der Ring $\mathbb{Z}$ der ganzen Zahlen ist noethersch, wie überhaupt jeder Hauptidealring noethersch ist. Körper sowieso.

b) Ist R ein noetherscher Ring und $\Phi : R \longrightarrow S$ ein surjektiver Ringhomomorphismus, so ist auch S noethersch. Denn für jedes Ideal I in S ist $\Phi^{-1}(I)$ ein Ideal in R und somit endlich erzeugt. Die Bilder eines Erzeugendensystems von $\Phi^{-1}(I)$ unter Φ erzeugen aber $\Phi(\Phi^{-1}(I)) = I$.

c) Jede endlichdimensionale K-Algebra A über einem Körper K ist noethersch. Die Ideale in A sind ja insbesondere Untervektorräume, und als solche endlichdimensional über K. Also sind sie erst Recht als A-Moduln endlich erzeugt. Für

[1] Amalie Emmy Noether, 1882-1935

so eine Algebra ist auch jeder endlich erzeugte Modul ein noetherscher A-Modul, und zwar aus demselben Grund.

Aber auch der Polynomring über einem Körper ist noethersch, er ist ja ein Hauptidealring.

Definition 3.1.3 exakte Sequenzen

Es seien R ein Ring und $M_i, i \in \mathbb{Z}$, ein paar R-Moduln. Weiterhin sei für jedes $i \in \mathbb{Z}$ ein R-Modulhomomorphismus

$$\Phi_i : M_i \longrightarrow M_{i+1}$$

gegeben. Dann heißt die Sequenz

$$\ldots \xrightarrow{\Phi_{i-1}} M_i \xrightarrow{\Phi_i} M_{i+1} \xrightarrow{\Phi_{i+1}} M_{i+2} \ldots$$

eine *exakte Sequenz* von R-Moduln, wenn das Folgende für alle i gilt:

$$\text{Kern}(\Phi_{i+1}) = \text{Bild}(\Phi_i).$$

Anstelle von $\mathbb{Z}$ kann hier auch der Durchschnitt von $\mathbb{Z}$ mit einem reellen Intervall als Indexmenge dienen, wobei die Bedingung dann nur für alle i zu prüfen ist, für die sowohl i als auch $i+1$ als Index vorkommen.

Eine exakte Sequenz der Gestalt

$$0 \longrightarrow M \xrightarrow{\Phi} N \xrightarrow{\Psi} Q \longrightarrow 0$$

heißt eine *kurze exakte Sequenz (keS)*. Das ist gleichbedeutend damit, dass Φ injektiv ist, $\text{Kern}(\Psi) = \text{Bild}(\Phi)$ gilt, und Ψ surjektiv ist. Man könnte dann auch M durch den isomorphen Modul $\Phi(M)$ ersetzen, Φ durch die Einbettung, Q durch $N/\Phi(M)$ und Ψ durch die kanonische Abbildung.

Zum Beispiel ist für zwei Moduln M und Q die Sequenz

$$0 \longrightarrow M \xrightarrow{m \mapsto (m,0)} M \times Q \xrightarrow{(m,q) \mapsto q} Q \longrightarrow 0$$

eine kurze exakte Sequenz.

Hilfssatz 3.1.4 Sequenzen von noetherschen Moduln

Es seien R ein Ring und M, N, Q drei R-Moduln. Weiterhin sei

$$0 \longrightarrow M \xrightarrow{\Phi} N \xrightarrow{\Psi} Q \longrightarrow 0$$

eine kurze exakte Sequenz von R-Moduln.

Dann ist N genau dann noethersch, wenn sowohl M als auch Q noethersch sind.

Beweis. Zunächst sei N noethersch. Wenn $U \subseteq M$ ein Untermodul ist, dann ist U isomorph zu $\Phi(U)$, das ist ein Untermodul von N, also endlich erzeugt, und damit ist auch U endlich erzeugt, also M noethersch.

Wenn V ein Untermodul von Q ist, dann ist $V = \Psi(\Psi^{-1}(V))$, da Ψ surjektiv ist. Da N noethersch ist, wird $\Psi^{-1}(V)$ von endlich vielen Elementen $n_1, \ldots, n_k$ erzeugt, aber dann ist V von $\Psi(n_1), \ldots, \Psi(n_k)$ erzeugt, und damit auch Q noethersch.

Sind umgekehrt M und Q noethersch und U ein Untermodul von N, dann ist $\Phi^{-1}(U)$ ein Untermodul von M und damit endlich erzeugt. Es seien $m_1, \ldots, m_r$ endlich viele Erzeuger von $\Phi^{-1}(U)$. Weiterhin ist $\Psi(U)$ ein Untermodul von Q und damit endlich erzeugt. Es seien $q_1, \ldots, q_s$ Erzeuger von $\Psi(U)$ und $u_1, \ldots, u_s$ Urbilder von ihnen unter Ψ.

Nun sei $u \in U$. Dann lässt sich $\Psi(u)$ schreiben als

$$\Psi(u) = \sum_{i=1}^{s} r_i q_i,$$

und damit liegt

$$u - \sum_{i=1}^{s} r_i u_i \in \mathrm{Kern}(\Psi) \cap U = \Phi(\Phi^{-1}(U)).$$

Es gibt also $a_1, \ldots, a_r \in R$, sodass

$$u - \sum_{i=1}^{s} r_i u_i = \sum_{j=1}^{r} a_j \Phi(m_j).$$

Damit haben wir ein endliches Erzeugendensystem von U gefunden, nämlich

$$\{\Phi(m_1), \ldots, \Phi(m_r), u_1, \ldots, u_s\}.$$

Da dies für jeden Untermodul U von N geht, ist N noethersch. ◯

Hilfssatz 3.1.5 Vererbungslehre

Es sei R ein linksnoetherscher Ring und M ein endlich erzeugter R-Linksmodul. Dann ist M noethersch.

Beweis. Es seien $m_1, \ldots, m_d$ Erzeuger von M. Dann ist die Abbildung

$$\Phi : R^d \longrightarrow M, \quad \Phi((a_i)) := a_1 m_1 + a_2 m_2 + \cdots + a_d m_d,$$

ein surjektiver Morphismus von Links-R-Moduln. Dann ist aber nach 3.1.4 M noethersch, wenn R^d dies ist, was wiederum induktiv aus 3.1.4 folgt, es gibt ja eine offensichtliche kurze exakte Sequenz

$$0 \longrightarrow R \longrightarrow R^{d+1} \longrightarrow R^d \longrightarrow 0.$$

◯

Satz 3.1.6 Hilberts[2] Basissatz

Es sei R ein kommutativer noetherscher Ring. Dann ist auch der Polynomring $R[X]$ noethersch.

Beweis. Es sei $I \subseteq R[X]$ ein Ideal. Wir müssen zeigen, dass es endlich erzeugt ist.

Für $n \in \mathbb{N}_0$ definieren wir

$$C_n := \{r \in R \mid \exists f \in I : f = rX^n + \sum_{i=0}^{n-1} a_i X^i, a_i \in R\}.$$

Insbesondere ist $C_n = \{0\}$, wenn es kein Polynom vom Grad n in I gibt.

Die Multiplikation mit X führt I in sich über. Dies zeigt, dass

$$C_n \subseteq C_{n+1}.$$

Außerdem ist C_n für jedes n ein Ideal in R.

Damit ist auch die (aufsteigende) Vereinigung $C_0 \cup C_1 \cup C_2 \cup \cdots =: C$ ein Ideal in R. Da C als Ideal in R endlich erzeugt ist und diese endlich vielen Erzeuger schon in einem der C_n liegen müssen, gibt es ein $N \in \mathbb{N}$, sodass gilt:

$$\forall n \geq 0 : \quad C_N = C_{N+1} = \cdots = C_{N+n}.$$

Wir wählen ein großes $K \in \mathbb{N}$, sodass für $0 \leq i \leq N$ das Ideal C_i von Elementen $\alpha_{i,1}, \ldots, \alpha_{i,K}$ erzeugt wird. Weiter wählen wir für jedes solche i und $1 \leq j \leq K$ ein Polynom

$$f_{i,j} \in I : \quad f_{i,j} = \alpha_{i,j} X^i + \text{niedrigere Terme}.$$

Dann gilt: Die Menge $\{f_{i,j} \mid 0 \leq i \leq N, 1 \leq j \leq K\}$ ist ein Erzeugendensystem des Ideals I.

Um das einzusehen machen wir vollständige Induktion nach dem Grad von $f \in I$. Wenn f Grad ≤ 0 hat, dann ist es eine Konstante, liegt also in C_0, das als R-Modul von den Elementen $f_{0,j} = \alpha_{0,j}, 1 \leq j \leq K$, erzeugt wird.

Hat f Grad $d > 0$, so ist entweder $d \leq N$, und f lässt sich durch Subtraktion einer geeigneten R-Linearkombination der $f_{d,j}$, $1 \leq j \leq K$, zu einem Polynom kleineren Grades machen, das in I liegt und damit – nach Induktionsvoraussetzung – im $R[X]$-Modulerzeugnis der $f_{i,j}$.

Oder f hat Grad $d > N$; dann lässt sich f durch Subtraktion des X^{d-N}-fachen einer R-Linearkombination der $f_{N,j}$, $1 \leq j \leq K$, zu einem Polynom in I von kleinerem Grad machen, und damit auch zu einer $R[X]$-Linearkombination der $f_{i,j}$. ◯

[2]David Hilbert, 1862-1943

Folgerung 3.1.7 endlich erzeugte kommutative R-Algebren

Es sei R ein kommutativer noetherscher Ring und A eine (als Ring) endlich erzeugte kommutative R-Algebra. Dann ist auch A noethersch.

Beweis. Es sei

$$\{a_1, \ldots, a_d\} \subseteq A$$

ein Erzeugendensystem, das heißt

$$A = \{ \sum_{i_1,\ldots,i_d} r_{i_1,\ldots,i_d} a_1^{i_1} \cdot \cdots \cdot a_d^{i_d} \mid r_{i_1,\ldots,i_d} \in R, \text{ endliche Summe}\}.$$

Dann ist der Homomorphismus

$$\Phi : R[X_1, \ldots X_d] \longrightarrow A, \quad f(X_1, \ldots, X_d) \mapsto f(a_1, \ldots a_d),$$

ein surjektiver Ringhomomorphismus.

Da aber R noethersch ist, ist es (dank Hilbert) auch $R[X_1]$, und damit auch $R[X_1][X_2] = R[X_1, X_2]$, und damit ... auch $R[X_1, \ldots X_d]$. Wegen 3.1.2b) ist auch A selbst noethersch. ◯

Definition/Bemerkung 3.1.8 Kettenbedingung

Im Beweis von Hilberts Basissatz haben wir benutzt (und begründet), dass eine aufsteigende Kette von Idealen in einem noetherschen Ring stationär wird. Genauer:

a) Es sei R ein Ring und M ein R-Modul. Weiter sei

$$U_1 \subseteq U_2 \subseteq U_3 \subseteq \ldots$$

eine aufsteigende Folge von Untermoduln. Dann sagt man, diese Folge werde *stationär*, wenn es ein $N \in \mathbb{N}$ gibt mit:

$$\forall k \geq N : U_k = U_N.$$

Der Modul erfüllt die *aufsteigende Kettenbedingung*, wenn jede aufsteigende Folge von Untermoduln stationär wird.

b) Analog gibt es die *absteigende Kettenbedingung*, die besagt, dass jede absteigende Folge von Untermoduln stationär wird.

c) Diese zwei Bedingungen lassen sich direkt auf beliebige geordnete Mengen übertragen. Statt zu sagen, sie erfüllten die aufsteigende Kettenbedingung, sagt man auch: sie sind *noethersch.* Statt zu sagen, sie erfüllten die absteigende Kettenbedingung, sagt man auch: sie sind *artinsch*[3].

[3] Emil Artin ist uns jetzt schon oft begegnet. Er war ein Schüler von Emmy Noether.

Eine geordnete Menge ist genau dann noethersch, wenn jede nichtleere Teilmenge ein maximales Element enthält.

Denn: Es sei $(M, \leq)$ noethersch und $S \subseteq M$ nichtleer. Nehmen wir an, es gebe in S kein maximales Element. Es sei $s_1 \in S$ irgendein Element. Wenn sukzessive $s_1 < s_2 < s_3 < \cdots < s_n \in S$ gewählt sind, dann ist auch s_n in S nicht maximal, und es gibt ein $s_{n+1} > s_n$. Auf diese Art konstruiert man eine unendliche, echt aufsteigende Kette in M, die es aber nach Voraussetzung nicht gibt. Also muss es ein maximales Element in S geben.

Wenn umgekehrt jede nichtleere Menge in M ein maximales Element besitzt und $m_1 \leq m_2 \leq \ldots$ eine aufsteigende Folge ist, dann besitzt auch

$$S := \{m_i \mid i \in \mathbb{N}\}$$

ein maximales Element. Das muss aber schon ein m_k sein (für geeignetes $k \in \mathbb{N}$), und es folgt $m_k = m_{k+1} = m_{k+2} \ldots$ Die Folge wird also stationär.

Analog ist eine geordnete Menge genau dann artinsch, wenn jede nichtleere Teilmenge ein minimales Element enthält.

d) Insbesondere haben wir in a) eine neue Definition für noethersche Moduln und Ringe. Das ist aber nicht problematisch, denn die neue und die alte Definition stimmen überein, wie uns der folgende Hilfssatz lehrt.

Hilfssatz 3.1.9 noethersch ist noethersch

Es sei R ein Ring und M ein Links-R-Modul. Dann ist M genau dann linksnoethersch, wenn M die aufsteigende Kettenbedingung für Links-R-Untermoduln erfüllt.

Beweis. Wenn M linksnoethersch ist und

$$U_1 \subseteq U_2 \subseteq U_3 \subseteq \ldots$$

eine aufsteigende Folge von Links-R-Untermoduln, dann ist die Vereinigung

$$U := \bigcup_{i \in \mathbb{N}} U_i$$

auch ein Links-R-Untermodul von M, also endlich erzeugt. Wenn $S \subseteq U$ ein endliches Erzeugendensystem ist, dann gibt es ein $N \in \mathbb{N}$, sodass bereits $S \subseteq U_N$ gilt. Dann ist aber $U_N = U$ und damit für alle $K \geq N$ offensichtlich $U_N = U_K$.

Wenn umgekehrt M nicht noethersch ist, dann wählen wir einen Untermodul $U \subseteq M$, der nicht endlich erzeugt ist.

Mit seiner Hilfe konstruieren wir eine aufsteigende, nicht stationär werdende Folge von (endlich erzeugten) Links-R-Untermoduln.

Wir wählen ein $u_1 \in U$ und setzen $U_1 := R \cdot u_1$. Wenn U_i bereits definiert ist, so ist es ungleich U, da U_i endlich erzeugt ist. Wir wählen ein $u_{i+1} \in U \setminus U_i$ und definieren U_{i+1} als den kleinsten Untermodul, der U_i und u_{i+1} enthält. Dieser wird von $\{u_1, \ldots, u_{i+1}\}$ erzeugt und ist ungleich U_i. Die Folge

$$U_1 \subset U_2 \subset U_3 \ldots$$

lehrt, dass die aufsteigende Kettenbedingung in M verletzt ist. ◯

Bemerkung 3.1.10 doch nicht alles noethersch!

Es gibt tatsächlich Ringe, die nicht noethersch sind. Wenn zum Beispiel K ein Körper ist und $X_1, X_2, \ldots$ unendlich viele Unbestimmte über K sind, so gibt es den Polynomring

$$K[X_1, X_2, \ldots].$$

Dieser ist nicht noethersch, denn wenn wir für $n \in \mathbb{N}$ das Ideal I_n definieren als das von $X_1, \ldots, X_n$ erzeugte, so ist X_{n+1} nicht in I_n und damit

$$I_1 \subset I_2 \subset I_3 \subset \ldots$$

eine aufsteigende Folge von Iealen, die die aufsteigende Kettenbedingung verletzt.

3.2 Bilineares

In diesem Abschnitt sei R immer ein kommutativer Ring. Wir werden verschiedene Gründe kennenlernen, bilineare Abbildungen zu untersuchen.

Definition/Bemerkung 3.2.1 Bilineare Abbildung

a) Es seien U, V, W drei R-Moduln. Eine *bilineare Abbildung*

$$\beta : U \times V \longrightarrow W$$

ist (wie in der LA) dadurch definiert, dass für alle $r, s \in R, u_1, u_2 \in U, v_1, v_2 \in V$ gilt:

$$\beta(ru_1 + u_2, sv_1 + v_2) = rs\beta(u_1, v_1) + r\beta(u_1, v_2) + s\beta(u_2, v_1) + \beta(u_2, v_2).$$

b) An Beispielen kennen wir die aus der Linearen Algebra. In der Definition des Begriffs Algebra haben wir schon die Bilinearität der Multiplikation in einer R-Algebra hingeschrieben. Für einen R-Modul M und für $N := \mathrm{Hom}_{R-Mod}(M, R)$ ist die Abbildung

$$\langle \cdot, \cdot \rangle : N \times M \longrightarrow R, \quad \langle \Phi, m \rangle := \Phi(m),$$

eine Bilinearform (das heißt: bilinear mit Werten im Grundring).

c) Wenn K ein Körper und A eine endlichdimensionale K-Algebra sind, dann ist die Abbildung

$$A \times A \longrightarrow K, \quad (a,b) \mapsto \mathrm{Spur}_A(a \cdot b)$$

eine symmetrische Bilinearform auf A.

Dabei ist mit „Spur“ die Spur der Multiplikation mit dem Argument auf A gemeint.

Definition/Bemerkung 3.2.2 Tensorprodukt kategoriell

Wir bezeichnen mit $\mathrm{Bil}(M \times N, V)$ die Menge aller bilinearen Abbildungen von $M \times N$ nach V.

Für festes M, N ist dann durch $\mathcal{B}(V) := \mathrm{Bil}(M \times N, V)$ jedem R-Modul V eine Menge zugeordnet. Für einen R-Modulhomomorphismus $\Phi : V \longrightarrow W$ definieren wir die Abbildung $\mathcal{B}(\Phi) : \mathcal{B}(V) \to \mathcal{B}(W)$ durch

$$\forall \beta \in \mathcal{B}(V) : \mathcal{B}(\Phi)(\beta) := \Phi \circ \beta.$$

Gesucht ist nun nach einem universellen Element für diesen „Funktor“, das heißt nach einem R-Modul T und einer bilinearen Abbildung

$$\otimes : M \times N \longrightarrow T, \quad (m,n) \mapsto m \otimes n \in T,$$

sodass für jede bilineare Abbildung $\beta : M \times N \longrightarrow V$ ein eindeutig bestimmter R-Modulhomomorphismus $\Phi : T \longrightarrow V$ existiert, für den

$$\beta = \Phi \circ \otimes$$

gilt. Existenz und Eindeutigkeit von solch einem Φ nennt man die *universelle Abbildungseigenschaft* von $\otimes$.

Wenn es so einen Modul T gibt, dann heißt er ein *Tensorprodukt von M und N* (über dem Ring R). Dieses Tensorprodukt ist dann bis auf einen Isomorphismus eindeutig bestimmt, und man schreibt dafür $T =: M \otimes N$. Genauer müsste man eigentlich sogar $M \otimes_R N$ schreiben, was ich bisweilen tun werde.

Konstruktion 3.2.3 Es gibt ein Tensorprodukt

Wir werden nun ein Tensorprodukt für zwei R-Moduln M und N konstruieren. Dazu sei erst einmal F der freie R-Modul mit Basis $M \times N$, wir schreiben Elemente von F als formale endliche Linearkombinationen

$$F = \{ \sum_{(m,n)} a_{(m,n)} \cdot \delta_{(m,n)} \mid a_{(m,n)} \in R, \text{ endliche Summe} \}.$$

Zwei solche formalen Linearkombinationen stimmen genau dann überein, wenn die Koeffizienten $a_{(m,n)}$ für alle $(m,n) \in M \times N$ übereinstimmen. Addition und skalare Multiplikation werden komponentenweise vorgenommen.

Die Abbildung

$$M \times N \ni (m,n) \mapsto \delta_{(m,n)} \in F$$

ist natürlich nicht bilinear. Um sie bilinear zu machen, müssen wir in F geeignete Relationen fordern. Dazu betrachten wir den Untermodul B von F, der von den Ausdrücken

$$\delta_{(rm_1+m_2,sn_1+n_2)} - rs\delta_{(m_1,n_1)} - r\delta_{(m_1,n_2)} - s\delta_{(m_2,n_2)} - \delta_{(m_2,n_2)}$$

mit $r,s \in R, m_1,m_2 \in M, n_1,n_2 \in N$ erzeugt wird. Wir setzen

$$T := F/B,\ \pi : F \longrightarrow F/B \text{ die kanonische Projektion.}$$

Dann ist

$$\otimes : M \times N \longrightarrow T,\ (m,n) \mapsto \pi(\delta_{(m,n)}),$$

eine bilineare Abbildung.

Wir müssen noch zeigen, dass T die universelle Abbildungseigenschaft hat. Dazu seien V ein R-Modul und $\beta : M \times N \longrightarrow V$ irgendeine bilineare Abbildung. Dazu gibt es einen Modulhomomorphismus

$$\widetilde{\Phi} : F \longrightarrow V,\ \sum_{(m,n)} a_{(m,n)} \cdot \delta_{(m,n)} \mapsto \sum_{(m,n)} a_{(m,n)} \cdot \beta(m,n).$$

Da β bilinear ist, liegt B im Kern von $\widetilde{\Phi}$, also faktorisiert $\widetilde{\Phi}$ über $T = F/B$. Wir erhalten damit einen eindeutig bestimmten Modulhomomorphismus

$$\Phi : T \longrightarrow V,\ \text{sodass } \widetilde{\Phi} = \Phi \circ \pi.$$

Aber Φ ist nun gerade so gemacht, dass

$$\beta = \Phi \circ \otimes$$

gilt. Da die Werte der Abbildung Φ auf den Erzeugern $m \otimes n$ von T durch die gewünschte Beziehung zu β vorgeschrieben sind, gibt es auch nicht mehr als diese eine Abbildung Φ mit der gewünschten Eigenschaft. ◯

Beispiel 3.2.4 für Tensorprodukte

a) Für jeden R-Modul M gilt $R \otimes_R M \cong M$.

b) Wenn M von $\{m_i \mid i \in I\}$ und N von $\{n_j \mid j \in J\}$ erzeugt werden, dann wird $M \otimes_R N$ von der Menge $\{m_i \otimes n_j \mid i \in I, j \in J\}$ erzeugt. Denn

$M = \{\sum_{i\in I} a_i m_i \mid a_i \in R, \text{ endliche Summe}\}$, und $N = \{\sum_{j\in J} b_j n_j \mid b_j \in R, \text{ endliche Summe}\}$, und es gilt

$$m = \sum_{i\in I} a_i m_i, \quad n = \sum_{j\in J} b_j n_j \Rightarrow m \otimes n = \sum_{(i,j)\in I\times J} a_i b_j (m_i \otimes n_j).$$

Aber diese „Elementartensoren“ erzeugen $M \otimes N$ nach Konstruktion.

c) Wenn M eine direkte Summer zweier Untermoduln U und V ist, dann gilt für alle R-Moduln N:

$$M \otimes_R N \cong (U \otimes_R N) \oplus (V \otimes_R N).$$

Dies wird vermittelt durch die bilineare Abbildung

$$M \times N \ni (u+v, n) \mapsto (u \otimes n, v \otimes n) \in (U \otimes_R N) \oplus (V \otimes_R N),$$

deren Universalität man leicht nachrechnet: Ist $\beta : M \times N \to P$ eine R-bilineare Abbildung, so sind auch die Einschränkungen nach $U \times N$ und $V \times N$ bilinear und liefern Lineare Abbildungen auf den beiden Summanden der rechten Seite.

Speziell gilt $R^d \otimes_R N \cong N^d$.

d) Wenn $\Phi : M \longrightarrow P$ und $\Psi : N \longrightarrow Q$ zwei R-Modulhomomorphismen sind, dann ist die Abbildung

$$\beta : M \times N \longrightarrow P \otimes Q, (m,n) \mapsto \Phi(m) \otimes \Psi(n),$$

bilinear. Sie induziert also einen Homomorphismus

$$\Phi \otimes \Psi : M \otimes N \longrightarrow P \otimes Q, m \otimes n \mapsto \Phi(m) \otimes \Psi(n).$$

e) Wenn U ein Untermodul von M ist und ι die Einbettung von U nach M, dann ist für jeden R-Modul N

$$(M/U) \otimes N \simeq (M \otimes N)/(\iota \otimes \mathrm{Id}_N)(U \otimes N).$$

Wieso? Übung!

Bemerkung 3.2.5 Ringwechsel – Ein Hochzeitsmärchen

Aus der linearen Algebra sieht man vielleicht ein, dass es manchmal sinnvoll ist, Aussagen über rationale Matrizen zu begründen, indem man sie als reelle Matrizen auffasst, oder gar als komplexe. Dabei macht man implizit den rationalen Standardvektorraum zu einer Teilmenge des reellen Standardvektorraums (oder des komplexen). Wie man das ohne Basiswahl machen kann, lernt man durch die allgemeine Konstruktion des Ringwechsels (Skalarerweiterung).

Dazu seien R ein kommutativer Ring, M ein R-Modul und A eine R-Algebra. Dann ist $A \otimes M$ erst einmal ein R-Modul.

Für jedes $a \in A$ ist die Abbildung

$$\mu_a : A \times M \longrightarrow A \otimes M, \quad (t, m) \mapsto at \otimes m,$$

bilinear. Also gibt es eine eindeutig bestimmte R-lineare Abbildung

$$\widetilde{\mu}_a : A \otimes M \longrightarrow A \otimes M, \quad \sum a_i \otimes m_i \mapsto \sum (aa_i) \otimes m_i.$$

Wir erhalten also insgesamt eine Abbildung

$$\widetilde{\mu} : A \times (A \otimes M) \longrightarrow A \otimes M,$$

und man rechnet leicht nach, dass diese Abbildung aus $A \otimes M$ einen A-Modul macht.

Wenn $\Phi : M \longrightarrow N$ eine R-lineare Abbildung ist, dann ist die Abbildung

$$\widetilde{\Phi} : A \times M \longrightarrow A \otimes N, \quad \widetilde{\Phi}(a, m) := a \otimes \Phi(m),$$

bilinear, definiert also einen Modulhomomorphismus

$$\mathrm{Id}_A \otimes \Phi : A \otimes M \longrightarrow A \otimes N.$$

Durch $M \rightsquigarrow M_A := A \otimes M$ und $\Phi \rightsquigarrow \mathrm{Id}_A \otimes \Phi$ wird ein „kovarianter Funktor“ von der Kategorie der R-Moduln in die Kategorie der A-Moduln definiert.

Man nennt diesen Vorgang die *Skalarerweiterung* (oder Ringerweiterung) von R nach A.

Speziell gilt für $M = R^d$, dass $M \otimes A \cong A^d$ gilt, und eine Basis von R^d liefert eine Basis von A^d.

Bemerkung 3.2.6 Algebren unter sich

Wenn A und B zwei R-Algebren sind, dann ergibt sich analog zu dem eben Gesehenen, dass für feste $a \in A, b \in B$ die Abbildung

$$\nu_{a,b} : A \times B \longrightarrow A \otimes B, \ (x, y) \mapsto ax \otimes by,$$

bilinear ist, also eine Abbildung $\widetilde{\nu}_{a,b}$ von $A \otimes B$ in sich selbst induziert. Für festes $t \in A \otimes B$ ist aber auch

$$\nu^t : A \times B \longrightarrow A \otimes B, \ (a, b) \mapsto \widetilde{\nu}_{a,b}(t),$$

bilinear und definiert damit eine Abbildung $\widetilde{\nu}^t$ von $A \otimes B$ nach $A \otimes B$.

Schließlich erhalten wir eine Abbildung

$$\nu : (A \otimes B) \times (A \otimes B) \longrightarrow A \otimes B, (s, t) \mapsto s \cdot t := \widetilde{\nu}^t(s),$$

und man sieht, dass $A \otimes B$ damit eine R-Algebra ist.

Hilfssatz 3.2.7 Assoziativität des Tensorprodukts

Es seien L, M, N drei R-Moduln. Dann gibt es einen eindeutig bestimmten Isomorphismus von R-Moduln

$$\Phi : (L \otimes M) \otimes N \longrightarrow L \otimes (M \otimes N),$$

der für alle $l \in L, m \in M, n \in N$ die Vorgabe

$$\Phi((l \otimes m) \otimes n) = l \otimes (m \otimes n)$$

erfüllt.

Beweis. Für festes $n \in N$ ist die Abbildung

$$\psi_n : L \times M \longrightarrow L \otimes (M \otimes N), \quad \psi_n(l, m) := l \otimes (m \otimes n),$$

bilinear. Also gibt es einen eindeutig bestimmten Modulhomomorphismus

$$\Psi_n : L \otimes M \longrightarrow L \otimes (M \otimes N) \text{ mit } \Psi_n(l \otimes m) = l \otimes (m \otimes n).$$

Die Abbildung

$$\psi : (L \otimes M) \times N \longrightarrow L \otimes (M \otimes N), \quad \psi(x, n) := \Psi_n(x),$$

ist bilinear, und deshalb gibt es einen eindeutig bestimmten R-Modulhomomorphismus

$$\Phi : (L \otimes M) \otimes N \longrightarrow L \otimes (M \otimes N) \text{ mit } \Phi((l \otimes m) \otimes n) = l \otimes (m \otimes n).$$

Es ist klar, dass man analog einen Homomorphismus

$$\widetilde{\Phi} : L \otimes (M \otimes N) \longrightarrow (L \otimes M) \otimes N \text{ mit } \widetilde{\Phi}(l \otimes (m \otimes n)) = (l \otimes m) \otimes n$$

erhält, und dass Φ und $\widetilde{\Phi}$ zueinander invers sind.

Die Eindeutigkeit von Φ folgt daraus, dass $(L \otimes M) \otimes N$ von den Elementen $(l \otimes m) \otimes n$ erzeugt wird. ◯

Konstruktion 3.2.8 die Tensoralgebra

a) Für einen R-Modul M definieren wir rekursiv $M^{\otimes n}$ durch

$$M^{\otimes 0} := R, M^{\otimes n+1} := M \otimes M^{\otimes n}.$$

Wir bilden die direkte Summe dieser R-Moduln:

$$T(M) := \bigoplus_{n=0}^{\infty} M^{\otimes n}.$$

Ein typisches Element dieser Menge ist eine endliche Summe von Ausdrücken der Gestalt $r \cdot (m_1 \otimes m_2 \otimes \cdots \otimes m_n)$ mit $r \in R$ und $m_1, \ldots, m_n \in M$. Ähnlich wie in 3.2.7 zeigt man, dass die Abbildung

$$M^{\otimes k} \times M^{\otimes l} \ni (x, y) \mapsto x \otimes y \in M^{\otimes (k+l)}$$

für alle $k, l \in \mathbb{N}_0$ wohldefiniert ist. Durch bilineare Fortsetzung erhalten wir eine Abbildung

$$T(M) \times T(M) \longrightarrow T(M).$$

Diese Abbildung verwenden wir als Multiplikation auf $T(M)$, das dadurch zu einer R-Algebra wird, der *Tensoralgebra* von M über R. Die Assoziativität erhalten wir wieder aus 3.2.7.

Wenn A irgendeine R-Algebra ist und $\varphi : M \longrightarrow A$ eine R-lineare Abbildung, dann setzt sich diese auf eindeutig bestimmte Art zu einem R-Algebren Homomorphismus $\Phi : T(M) \longrightarrow A$ fort. Dies liefert eine Bijektion

$$\eta_{M,A} : \mathrm{Hom}_{R-Mod}(M, A) \longrightarrow \mathrm{Hom}_{R-Alg}(T(M), A),$$

denn $T(M)$ wird als Algebra ja von M erzeugt.

b) Beispiel: Es sei M ein freier R-Modul vom Rang 1, das heißt: M hat eine Basis aus einem Element: $\{b\}$.

Dann ist $M^{\otimes n} = R \cdot b^{\otimes n}$ auch jeweils frei, und die Definition des Produkts in $T(M) = \bigoplus R \cdot b^{\otimes n}$ ist gegeben durch

$$\sum_i r_i b^{\otimes i} \cdot \sum_j s_j b^{\otimes j} = \sum_k \Big(\sum_{0 \le i \le k} r_i s_{k-i} \Big) b^{\otimes k}.$$

Wir erhalten ein neues Modell des Polynomrings in einer Variablen.

Wenn wir einen freien Modul von höherem Rang verwenden, dann bekommen wir einen nichtkommutativen Ring, und nicht direkt den Polynomring in mehreren Variablen. Wenn $\{b_1, \ldots, b_n\} =: B$ eine Basis von M ist, dann ist $T(M)$ isomorph zum Monoidring (siehe EAZ, 2.3.1) über dem freien Monoid über $\{b_1, \ldots, b_n\}$ (siehe EAZ, 1.4.6/1.4.7): Beide Algebren erfüllen dieselbe universelle Abbildungseigenschaft.

Ähnlich wie der Polynomring für kommutative Ringe lässt sich diese Tensoralgebra benutzen, um beliebige (nicht nur endlich erzeugte) R-Algebren durch Quotientenbildung zu erhalten. Allerdings ist diese Tensoralgebra manchmals nicht sehr „benutzerfreundlich“.

Beispiel 3.2.9 Clifford-Algebren und noch eine

a) Es seien K ein Körper mit Charakteristik $\neq 2$, V ein endlichdimensionaler Vektorraum und q eine quadratische Form auf V. Das heißt: Es gibt eine symmetrische Bilinearform β auf V mit $q(v) = \beta(v, v)$ für alle $v \in V$.

Weiter sei A eine K-Algebra und $\Phi : V \longrightarrow A$ eine K-lineare Abbildung, sodass für alle $v \in V$ gilt:

$$\Phi(v)^2 = \beta(v) \cdot 1_A.$$

Schließlich sei $C(q)$ die K-Algebra, die sich ergibt, indem aus der Tensoralgebra $T(V)$ das zweiseitige Ideal I herausgeteilt wird, das von den Ausdrücken $v \otimes v - q(v)$ erzeugt wird. Die offensichtliche Abbildung $V \ni v \mapsto v + I \in C(q)$ erfüllt dann auch die Bedingung

$$(v + I)^2 = q(v) \cdot 1_{C(q)}.$$

Φ induziert einen Algebrenhomomorphismus $T(V) \longrightarrow A$, und wegen der Bedingung an Φ ist I im Kern von diesem Algebrenhomomorphismus enthalten. Also erhalten wir einen Algebrenhomomorphismus $\Psi : C(q) \longrightarrow A$, sodass für alle $v \in V$ gilt:

$$\Phi(v) = \Psi(v + I).$$

Die Algebra $C(q)$ zusammen mit der Abbildung $v \mapsto v + I$ erfüllt also eine universelle Eigenschaft. Sie heißt die *Cliffordalgebra*[4] zur quadratischen Form q.

Wenn etwa $V = K$ ist, $d \in K$ und $q(v) = dv^2$, dann ist $C(q) = K[X]/(X^2 - d)$, das sieht man direkt an der Konstruktion.

Wenn $V = K^2$ gilt und die quadratische Form q durch $q(v, w) := av^2 + bw^2$ gegeben ist, dann gilt für die Standardbasis $I := e_1, J := e_2$ in $C(q)$:

$$I^2 = a, J^2 = b, (I + J)^2 = a + b.$$

Dies impliziert $IJ = -JI$, und für dieses Element gilt

$$(IJ)^2 = IJIJ = -(IIJJ) = -ab.$$

Da $C(q)$ als Algebra von I und J erzeugt wird, und da sich jedes Wort in I und J modulo der Relationen in $C(q)$ auf eine Wort der Länge ≤ 2 reduzieren lässt, hat $C(q)$ als K-Basis die Elemente $1, I, J, IJ$. $C(q)$ ist die zu a und b gehörige Quaternionenalgebra.

Jetzt können wir Quaternionenalgebren etwas flexibler definieren: eine Quaternionenalgebra ist die Cliffordalgebra zu einer nicht ausgearteten quadratischen Form auf einem zweidimensionalen Vektorraum. Die Theorie der quadratischen Formen sagt (mittels eines leicht modifizierten E. Schmidt-Verfahrens), dass jede nicht ausgeartete quadratische Form zu einer „Diagonalform“ äquivalent ist. Eine feinere Klassifikation ist im Allgemeinen schwierig; für viele interessante Körper kennt man das aber gut.

[4]William Kingdon Clifford, 1845-1879

b) Nun sei $M = \mathbb{Z}^2$ und $T(M)$ die Tensoralgebra davon. Sie wird frei erzeugt von einer Basis $\{x, y\}$ von M. Wir betrachten in $T(M)$ das zweiseitige Ideal I, das von $\{xy, yy\}$ erzeugt wird. Dann ist der (nicht-kommutative!) Ring

$$T(M)/I \cong \mathbb{Z}[x] \oplus y\mathbb{Z}[x].$$

Mit Multiplikation von rechts wird das ein endlich erzeugter $\mathbb{Z}[x]$-Modul.

Wenn J ein Rechtsideal hierin ist, dann ist es insbesondere auch ein Rechts-$\mathbb{Z}[x]$-Untermodul, und damit als solcher endlich erzeugt, weil $\mathbb{Z}[x]$ noethersch ist. Also ist $T(M)/I$ rechtsnoethersch.

Hingegen ist die Kette

$$\mathbb{Z}y \subseteq \mathbb{Z}y \oplus \mathbb{Z}yx \subseteq \mathbb{Z}y \oplus \mathbb{Z}yx \oplus \mathbb{Z}yx^2 \subseteq \dots$$

eine aufsteigende Folge von $T(M)/I$-Linksidealen, die nicht stationär wird. Also ist $T(M)/I$ nicht linksnoethersch.

Beispiel 3.2.10 Die äußere Algebra

Ein spezieller Spezialfall dieser Cliffordalgebren ergibt sich für die Nullabbildung als quadratische Form. Es sei $V = K^n$ und $q : V \to K,\ q(v) = 0$ für alle v. Dann ist die zugehörige Cliffordalgebra der Faktorring der Tensoralgebra $T(V)$ nach dem zweiseitigen Ideal, dass von den Ausdrücken der Gestalt $v \otimes v,\ v \in V$, erzeugt wird.

Diese Algebra heißt die *äußere Algebra von* V, in Zeichen: $\Lambda(V)$.

Die Multiplikation in ihr wird üblicher Weise mit $\wedge$ bezeichnet. Es wird also $\Lambda(V)$ von einer Basis B von V erzeugt, und wir erhalten die Relationen

$$\forall b, c \in B : b \wedge b = 0, b \wedge c = -c \wedge b.$$

Die zweite Art von Relationen kommt daher, dass $(b + c) \wedge (b + c) = 0$ gilt und die Distributivgesetze greifen.

Ist $B = \{b_1, \dots, b_n\}$, so erhalten wir eine Basis von $\Lambda(V)$ wie folgt:

$$\{b_{i_1} \wedge b_{i_2} \wedge \dots \wedge b_{i_k} \mid 0 \le k \le n,\ i_1 < i_2 \dots < i_k\}.$$

Die Dimension von $\Lambda(V)$ ist 2^n.

Die Linearkombinationen der $b_{i_1} \wedge b_{i_2} \wedge \dots \wedge b_{i_k}$ für festes k bilden einen Untervektorraum $\Lambda^k(V)$ der Dimension $\binom{n}{k}$ und es gilt

$$\Lambda^k(V) \wedge \Lambda^l(V) \subseteq \Lambda^{k+l}(V).$$

So etwas nennt man eine Graduierung einer Algebra.

In Analysis und Differentialgeometrie sieht man äußere Algebren in Aktion, sobald es um Differentialformen geht.

3.3 Ordnung und Ganzheit

Ausgehend von Ordnungen in endlichdimensionalen $\mathbb{Q}$-Algebren wollen wir die algebraische Theorie der Ganzheit entwickeln. Dies liefert einen ersten Einblick in eine wichtige Begriffsbildung der algebraischen Zahlentheorie und der algebraischen Geometrie.

Definition 3.3.1 Ordnung

Es sei A eine endlichdimensionale $\mathbb{Q}$-Algebra. Eine *Ordnung* in A ist ein Teilring $\mathcal{O} \subseteq \mathcal{A}$, der als $\mathbb{Z}$-Modul endlich erzeugt ist und der eine $\mathbb{Q}$-Basis von A enthält.

Bemerkung 3.3.2 Matrizen und so weiter

a) Im Matrizenring $\mathbb{Q}^{d\times d}$ gibt es mindestens eine Ordnung, nämlich $\mathbb{Z}^{d\times d}$.

Da jede d-dimensionale Algebra A sich auffassen lässt als Teilalgebra von $\mathbb{Q}^{d\times d}$, findet sich auch in A eine Ordnung, nämlich

$$\mathcal{O} := A \cap \mathbb{Z}^{d\times d}.$$

Es gibt also in jeder endlichdimensionalen $\mathbb{Q}$-Algebra mindestens eine Ordnung.

b) Eine Ordnung $\mathcal{O}$ in einer $\mathbb{Q}$-Algebra ist immer eine Untergruppe des Vektorraums A, also torsionsfrei (d.h. keine Elemente $\neq 0$ von endlicher Ordnung). Da $\mathcal{O}$ auch endlich erzeugt ist, greift der Struktursatz für endlich erzeugte abelsche Gruppen (EAZ, 3.4.12): $\mathcal{O}$ ist eine freie abelsche Gruppe.

Da $\mathcal{O}$ eine Basis von A enthält, ist der Rang mindestens so groß wie die Dimension d von A. Umgekehrt sind mehr als d Element aus A immer $\mathbb{Q}$-linear abhängig, und diese Abhängigkeit lässt sich ganz machen durch Multiplikation mit einem gemeinsamen Nenner der Koeffizienten. Also ist der Rang von $\mathcal{O}$ genau gleich d und es gibt eine Basis $\{b_1, \ldots, b_d\}$ von A, sodass gilt:

$$\mathcal{O} = \mathbb{Z}b_1 \oplus \cdots \oplus \mathbb{Z}b_d.$$

Da dies ein Ring sein soll, muss das Produkt zweier Basisvektoren eine ganzzahlige Linearkombination von Basisvektoren sein:

$$\forall i, j : \exists c_{ijk} \in \mathbb{Z} : b_i \cdot b_j = \sum_{k=1}^{d} c_{ijk} b_k.$$

c) Nun sei $x \in \mathcal{O}$ für eine Ordnung $\mathcal{O}$ der d-dimensionalen $\mathbb{Q}$-Algebra A. Beschreibt man die Multiplikation mit x bezüglich einer Basis der Ordnung, so erhält man eine ganzzahlige Abbildungsmatrix. Dann sagen Hamilton[5] und

[5]William Hamilton, 1788-1856

Cayley[6] unisono, dass x als Nullstelle des charakteristischen Polynoms dieser Matrix ein normiertes ganzzahliges Polynom als annullierendes Polynom hat.

Diese Eigenschaft werden wir in Kürze Ganzheit nennen.

d) Die einzige Ordnung in $\mathbb{Q}$ ist $\mathbb{Z}$. Denn eine Ordnung muss ja die 1 enthalten, also sicherlich $\mathbb{Z}$ umfassen; und wenn ein echter Bruch p/q in der Ordnung liegt, dann auch alle Potenzen davon, aber deren Nenner wären dann unbeschränkt, und damit wäre die Ordnung nicht endlich erzeugt als $\mathbb{Z}$-Modul.

Alternativ: Wenn $q \in \mathbb{Q}$ eine Nullstelle eines normierten ganzzahligen Polynoms f ist, dann ist q selbst ganz.

e) Nun seien $\zeta \in \mathbb{C}$ eine primitive n-te Einheitswurzel und $K = \mathbb{Q}(\zeta)$ der zugehörige Kreisteilungskörper. Da ζ eine Nullstelle von $X^n - 1$ ist, ist $\mathbb{Z}[\zeta]$ als abelsche Gruppe von $1, \zeta, \ldots, \zeta^{n-1}$ erzeugt, worin eine Basis von K liegt. Daher ist $\mathbb{Z}[\zeta]$ eine Ordnung in K. Jede Ordnung von K ist darin enthalten, aber das zu zeigen ist etwas aufwendiger.

f) $\mathbb{R} \otimes_{\mathbb{Q}} A$ ist eine endlichdimensionale $\mathbb{R}$-Algebra. Insbesondere ist das ein endlichdimensionaler reeller Vektorraum, und darauf kann man Normen betrachten. All diese Normen induzieren dieselbe Topologie auf $\mathbb{R} \otimes_{\mathbb{Q}} A$, und bezüglich dieser Topologie ist $\{1 \otimes z \mid z \in \mathcal{O}\}$ eine diskrete Untergruppe von $\mathbb{R} \otimes_{\mathbb{Q}} A$. Auf diese Art lassen sich geometrische Argumente ins Rechnen mit Algebren einbeziehen. Das ist der Ursprung der „Geometrie der Zahlen“, die etwa in der algebraischen Zahlentheorie Anwendung findet im Rahmen der Minkowski-Theorie.

Definition 3.3.3 Diskriminante, Maximalordnung

a) Auf jeder endlichdimensionalen $\mathbb{Q}$-Algebra A gibt es die Spurform

$$A \times A \ni (a, b) \mapsto \mathrm{Spur}(ab).$$

Diese Bilinearform ist symmetrisch. Wenn $\mathcal{O} \subseteq A$ eine Ordnung ist, so wählen wir eine Basis $\{b_1, \ldots, b_n\}$ von $\mathcal{O}$, und betrachten die zugehörige Fundamentalmatrix der Spurform:

$$F := (\mathrm{Spur}(b_i b_j))_{1 \le i,j}.$$

Dies ist eine ganzzahlige Matrix, denn die Multiplikation mit $b_i b_j$ beschreibt sich durch eine ganzzahlige Matrix bezüglich der gewählten Basis. Die Determinante von F heißt die *Diskriminante* von $\mathcal{O}$. Sie ist wohldefiniert, da eine andere Basis von $\mathcal{O}$ aus der gewählten durch eine ganzzahlige Basiswechselmatrix mit Determinante ± 1 hervorgeht.

Die Spurform heißt *nicht ausgeartet*, wenn die Diskriminante nicht 0 ist. Hierbei könnte man auch die Fundamentalmatrix der Spurform bezüglich einer beliebigen

[6] Arthur Cayley, 1821-1895

anderen Basis nehmen. Äquivalent dazu ist auch, dass es zu jedem $a \in A \setminus \{0\}$ ein $b \in A$ gibt mit Spur $(ab) \neq 0$.

b) Eine Ordnung $\mathcal{O}$ von A heißt eine *Maximalordnung* von A, wenn sie in keiner größeren Ordnung enthalten ist.

Beispiel 3.3.4 Matrizenring

Es sei A der Ring der rationalen $d \times d$-Matrizen. Darin betrachten wir die Ordnung $\mathcal{O}$, die aus den ganzzahligen Matrizen besteht. Sie hat als Basis die Menge B der Elementarmatrizen $E_{ij}, 1 \leq i, j \leq d$. Was ist hiervon die Diskriminante?

Für zwei Elementarmatrizen $E_{i,j}$ und $E_{k,l}$ gilt:

$$E_{i,j} \cdot E_{k,l} = \begin{cases} E_{i,l} & \text{falls } j = k, \\ 0 & \text{sonst.} \end{cases}$$

Die Spur von $E_{i,l}$ (auf A) wiederum ist d, wenn $i = l$ ist, und sonst 0. Denn: Wenn $i \neq l$ gilt, dann ist $E_{i,l}^2 = 0$, also die Multiplikation mit $E_{i,l}$ nilpotent, und ansonsten ist die Multiplikation mit $E_{i,i}$ eine Projektion auf den Raum aller Matrizen, die außerhalb der i-ten Zeile 0 sind.

Damit ist die Fundamentalmatrix der Spurform bezüglich B gegeben durch $d \cdot P$, wobei P die Matrix ist, die die Transposition als lineare Abbildung von A nach A beschreibt.

P ist diagonalisierbar, und die Eigenwerte sind 1 und -1. Die zugehörigen Eigenräume sind die Räume der symmetrischen bzw. antisymmetrischen Matrizen und haben Dimension $d(d+1)/2$ bzw. $d(d-1)/2$.

Das zeigt, dass die Diskriminante von $\mathcal{O}$ die Zahl

$$(-1)^{d(d-1)/2} \cdot d^{d^2}$$

ist.

Hilfssatz 3.3.5 manchmals gibt es eine Maximalordnung

Es seien A eine endlichdimensionale $\mathbb{Q}$-Ordnung, deren Spurform nicht ausgeartet ist, und $\mathcal{O}$ eine Ordnung in A. Dann ist $\mathcal{O}$ in einer Maximalordnung von A enthalten.

Beweis. Wenn $\mathcal{O}$ noch nicht maximal ist, dann ist es enthalten in einer größeren Ordnung $\widetilde{\mathcal{O}}$, und hat darin endlichen Index m. Dann gilt für die Diskriminanten D und $\widetilde{D}$ dieser Ordnungen:

$$\widetilde{D} = D/m^2,$$

denn aus einer Basis von $\widetilde{\mathcal{O}}$ macht man eine Basis von $\mathcal{O}$ durch eine ganzzahlige Basiswechselmatrix mit Determinante $\pm m$. (Hier darf man entweder geometrisch

argumentieren: Determinanten sind Volumina und Indizes irgendwie auch; oder algebraisch: über den Elementarteilersatz.)

Da aber alle Zahlen ganz und nicht Null sind (hier brauche ich, dass die Spurform nicht ausgeartet ist), kann man $\mathcal{O}$ nur endlich oft vergrößern und gelangt auf diese Art schließlich zu einer Maximalordnung. ◯

Beispiel 3.3.6 Maximalforderung

a) Wenn die Diskriminante einer Ordnung quadratfrei ist, dann ist die Ordnung maximal, wie man am Beweis von 3.3.5 sieht.

b) Der Matrizenring $\mathbb{Q}^{d\times d}$ besitzt eine Maximalordnung. Zum Beispiel ist $\mathbb{Z}^{d\times d}$ eine Maximalordnung. Wenn nämlich $\widetilde{\mathcal{O}}$ eine Maximalordnung ist, die die ganzzahligen Matrizen umfasst, und wenn die Matrix $M = (a_{ij}) \in \widetilde{\mathcal{O}}$ nicht ganzzahlig wäre, dann kann man durch Multiplikation mit Permutationsmatrizen (die ganzzahlig sind) erzwingen, dass zum Beispiel a_{11} nicht ganzzahlig ist. Dann ist aber auch $E_{11} \cdot M \cdot E_{11} = a_{11}E_{11} \in \widetilde{\mathcal{O}}$. Diese Matrix hat aber kein ganzzahliges charakteristisches Polynom, und ist damit nicht in einer Ordnung enthalten.

Für jede invertierbare Matrix M ist $M\mathbb{Z}^{d\times d}M^{-1}$ ebenfalls eine Maximalordnung in $\mathbb{Q}^{d\times d}$, Maximalordnungen sind also meistens nicht eindeutig bestimmt.

c) Wenn K eine endliche Körpererweiterung von $\mathbb{Q}$ ist, dann ist die Spurform nicht ausgeartet: es gibt zu $x \in K \setminus \{0\}$ ein $y \in K$, sodass xy von 0 verschiedene Spur hat, zum Beispiel $y = x^{-1}$. Daher gibt es in K eine Maximalordnung. Wir werden später sehen, dass diese eindeutig bestimmt ist. Sie heißt der Ganzheitsring von K und spielt eine übergeordnete Rolle in der algebraischen Zahlentheorie.

d) Die Algebra $A := \{\left(\begin{smallmatrix} a & b \\ 0 & a \end{smallmatrix}\right) \mid a, b \in \mathbb{Q}\}$ enthält für jedes $q \in \mathbb{Q}$ die Ordnung

$$\mathcal{O}_q := \{\begin{pmatrix} a & bq \\ 0 & a \end{pmatrix} \mid a, b \in \mathbb{Z}\}.$$

Jede Ordnung von A ist in einer solchen enthalten. Daher besitzt A keine Maximalordnung. Tatsächlich ist die Spurform ausgeartet. Bezüglich der Basis $B := \{\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right)\}$ ist ihre Fundamentalmatrix

$$F = \begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix}.$$

Definition 3.3.7 Ganzheit

Es seien R ein kommutativer Ring und S eine R-Algebra.

a) Ein Element $s \in S$ heißt *ganz über* R, falls ein normiertes Polynom $f \in R[X]$ existiert mit $f(s) = 0$.

b) Wenn S kommutativ ist, so heißt die Menge aller über R ganzen Elemente in S der *ganze Abschluss* von R in S.

c) Wenn R nullteilerfrei ist und S der Quotientenkörper von R, so heißt R *ganz abgeschlossen*, wenn der ganze Abschluss von R in S gleich R ist. Beispielsweise Hauptidealringe sind ganz abgeschlossen.

Algebraische Geometer reden hier eher von *normalen* Ringen, meinen aber auch ganz abgeschlossene Ringe.

d) Eine Ringerweiterung $R \subseteq S$ heißt *ganz*, wenn jedes Element von S ganz über R ist.

Hilfssatz 3.3.8 Cayley-Hamilton

Es sei R ein beliebiger kommutativer Ring und $M \in R^{d\times d}$ eine quadratische Matrix mit Einträgen in R. Weiter sei

$$F := \det(XI_d - M)$$

das charakteristische Polynom.

Dann gilt $F(M) = 0$.

Beweis. Wir wissen, dass die Aussage für nullteilerfreies R gilt, denn dann liegt R in seinem Quotientenkörper, und man kann das entsprechende Faktum aus der Linearen Algebra benutzen.

Nun sei R ein beliebiger kommutativer Ring. Weiter sei

$$S := \mathbb{Z}[t_{i,j} \mid 1 \leq i, j \leq d]$$

der Polynomring über $\mathbb{Z}$ in d^2 Unbekannten.

Die Vorschrift $t_{i,j} \mapsto m_{i,j}$ (der (i,j)-te Eintrag in M) definiert per universeller Abbildungseigenschaft des Polynomrings einen Ringhomomorphismus $\varphi : S \to R$ vermöge

$$\varphi(g(t_{1,1}, \ldots, t_{d,d}) := g(m_{1,1}, \ldots, m_{d,d}).$$

Dieser liefert auch einen Ringhomomorphismus

$$\varphi^{d\times d} : S^{d\times d} \to R^{d\times d}, \quad (g_{i,j}) \mapsto (\varphi(g_{i,j})).$$

Die Matrix T mit den Einträgen $t_{i,j}$ wird hierbei auf unsere alte Matrix M abgebildet.

Als nächstes liefert uns φ auch noch einen Ringhomomorphismus $\varphi_* : S[X] \to R[X], \varphi_*(\sum g_i X^i) := \sum \varphi(g_i) X^i$.

Dieser bildet das charakteristische Polynom C von T auf das von M ab, denn beide werden über die Leibnizformel berechnet.

Es folgt insgesamt

$$F(M) = \varphi_*(C)(\varphi^{d\times d}(T)) = \varphi^{d\times d}(C(T)) = 0,$$

wobei wir am Ende ausnutzen, dass S nullteilerfrei ist. ◯

Hilfssatz 3.3.9 Kriterium der Ganzheit

Es seien R ein kommutativer Ring und S eine R-Algebra. Dann sind für $s \in S$ äquivalent:

a) s ist ganz über R.

b) Die Unteralgebra $R[s]$ von S ist als R-Modul endlich erzeugt.

c) $R[s]$ ist in einer Unteralgebra A von S enthalten, die als R-Modul endlich erzeugt ist.

Beweis:

a)$\Rightarrow$ b)

Es sei $f(X) = X^d + \sum_{i=0}^{d-1} r_i X^i$ ein Polynom, wie es nach Voraussetzung existiert: normiert mit $f(s) = 0$. Dann gilt:

$$R[s] = \{\sum_{i=0}^{d-1} a_i s^i \mid a_i \in R\}.$$

Die Inklusion $\supseteq$ ist hierbei klar, die andere Inklusion folgt, da $s^d, s^{d+1}, \ldots$ sich induktiv durch kleinere Potenzen von s ausdrücken lassen, die linker Hand enthalten sind.

b)$\Rightarrow$ c) sollte klar sein.

c)$\Rightarrow$ a)

Es sei $a_1, \ldots, a_d$ ein endliches Erzeugendensystem des R-Moduls A. Die (R-lineare!) Multiplikation μ mit s (d.h. $\mu(x) = sx$) ist dann auf A gegeben durch

$$s \cdot a_j = \sum_{i=0}^{d} m_{ij} a_j, \quad m_{ij} \in R.$$

Auf dem freien R-Modul R^d betrachten wir den Endomorphismus Φ, der durch Multiplikation mit der Matrix $M := (m_{ij})$ gegeben ist. Außerdem machen wir A zu einem $R[X]$-Modul, indem wir X als Multiplikation mit s wirken lassen. Dann ist die Abbildung

$$\pi : R^d \longrightarrow A, \quad (r_i) \mapsto \sum_i r_i a_i$$

ein surjektiver Homomorphismus, und es gilt $\pi \circ \Phi = \mu \circ \pi$, da dies auf den jeweils betrachteten Erzeugern stimmt. Man sieht schnell ein, dass für jedes Polynom $F \in R[X]$ auch $\pi \circ F(\Phi) = F(\mu) \circ \pi$ gilt.

Da das charakteristische Polynom F von M ausgewertet bei Φ die Nullabbildung ergibt, gilt $F(\mu) \circ \pi = 0$. Da π surjektiv ist, folgt $F(\mu) = 0$, aber $F(\mu)$ ist die Multiplikation mit $F(s)$, und daher ist

$$F(s) = F(\mu)(1) = 0.$$

Daher ist s ganz über R. ◯

Folgerung 3.3.10 Der ganze Abschluss

Es seien R ein kommutativer Ring und S eine kommutative R-Algebra.

Dann ist der ganze Abschluss von R in S eine Teilalgebra von S.

Beweis. Es seien $s, t \in S$ ganz über R. Dann ist t auch ganz über $R[s]$. Da $R[s,t]$ kommutativ ist, ist es nach dem letzten Hilfssatz $R[s]$-Modul endlich erzeugt, und damit auch als R-Modul, denn $R[s]$ ist endlich erzeugter R-Modul. Damit liegen st und $s+t$ in einem endlich erzeugten R-Modul, der eine Algebra ist, sind also ganz über R. Das zeigt die Behauptung. ◯

Folgerung 3.3.11 Der Ganzheitsring

Es sei K eine endliche Körpererweiterung von $\mathbb{Q}$. Dann ist der ganze Abschluss von $\mathbb{Z}$ in K die eindeutig bestimmte Maximalordnung $\mathcal{O}$ in K.

Beweis. Es seien R der ganze Abschluss von $\mathbb{Z}$ in K, und $\mathcal{O}$ eine Maximalordnung. Dann ist $\mathcal{O}$ in R enthalten (wegen 3.3.2 c)). Jedes $r \in R$ ist ganz über $\mathbb{Z}$ und damit auch ganz über $\mathcal{O}$. Daher ist $\mathcal{O}[r]$ ein endlich erzeugter $\mathcal{O}$-Modul und (da $\mathcal{O}$ endlich erzeugter $\mathbb{Z}$-Modul ist) auch endlich erzeugter $\mathbb{Z}$-Modul. Daher ist $\mathcal{O}[r]$ eine Ordnung, folglich $r \in \mathcal{O}$, da dies eine Maximalordnung ist.

Es folgt $R = \mathcal{O}$. Daher kann es auch nur eine Maximalordnung geben. ◯

Definition/Bemerkung 3.3.12 Quadratische Zahlkörper, Gauß-Lemma

Es sei $\mathbb{Q} \subseteq K$ eine endliche Körpererweiterung.

a) Ein Element $s \in K$ ist genau dann ganz über $\mathbb{Z}$, wenn sein (wie immer: normiertes!) Minimalpolynom in $\mathbb{Q}[X]$ bereits ganzzahlige Koeffizienten hat.

Wenn dem so ist, ist s ganz, das ist klar.

Ist umgekehrt s ganz, so sei $f \in \mathbb{Z}[X]$ ein normiertes Polynom mit $f(s) = 0$. Dies ist ein Vielfaches des Minimalpolynoms m von s, also gibt es ein Polynom $g \in \mathbb{Q}[X]$, sodass $f = m \cdot g$.

Da f ganzzahlig mit Leitkoeffizient 1 ist, ist sein Inhalt 1. Das Gauß-Lemma sagt, dass das Produkt der Inhalte von m und g dann auch 1 ist. Es folgt

$$f = \frac{m}{\mathrm{Inh}(m)} \cdot \frac{g}{\mathrm{Inh}(g)},$$

aber die beiden Faktoren rechter Hand sind ganzzahlige Polynome. Da ihr Produkt normiert ist, sind sie beide (bis aufs Vorzeichen) normiert, das heißt aber, dass der Inhalt von m schon 1 ist, also liegt m in $\mathbb{Z}[X]$.

b) Es sei $d \in \mathbb{Z}$ eine quadratfreie Zahl und $L = \mathbb{Q}(\sqrt{d})$. Dann ist natürlich $\mathbb{Z}[\sqrt{d}]$ eine Ordnung in L, und ihre Diskriminante ist

$$\det \begin{pmatrix} 2 & 0 \\ 0 & 2d \end{pmatrix} = 4d.$$

Da d als quadratfrei vorausgesetzt ist, kann es in der Maximalordnung höchstens Index 2 haben (denn das Quadrat des Index teilt die Diskriminante!). Diese liegt also in $\frac{1}{2}(\mathbb{Z}[\sqrt{d}])$.

Da $1/2$ und $\sqrt{d}/2$ nicht ganzalgebraisch (d.h. ganz über $\mathbb{Z}$) sind, ist $\mathbb{Z}[\sqrt{d}]$ genau dann die Maximalordnung, wenn $\frac{\sqrt{d}+1}{2}$ nicht ganz ist. Dies ist genau dann der Fall, wenn d gerade oder $\equiv 3 \pmod 4$ ist.

Im Fall $d \equiv 1 \pmod 4$ ist die Maximalordnung eben $\mathbb{Z}[\frac{\sqrt{d}+1}{2}]$.

c) Der ganze Abschluss von $\mathbb{Z}$ in K heißt der *Ganzheitsring* von K und wird meistens mit $\mathcal{O}_K$ notiert.

d) Die Kommutativität von S ist in 3.3.10 nicht nur hilfreich sondern tatsächlich essentiell. Zum Beispiel sind die beiden folgenden Elemente der $\mathbb{Z}$-Algebra $\mathbb{Q}^{2\times 2}$ zwar ganz, ihre Produkte aber nicht:

$$\begin{pmatrix} 0 & 0 \\ \frac{1}{2} & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}.$$

Das Minimalpolynom des Produkts ist ja $X(X - \frac{1}{2})$, und es gibt kein normiertes ganzzahliges Vielfaches davon.

Kapitel 4

Dedekindringe

4.1 Auf dem Weg zur Definition

Hilfssatz 4.1.1 Index

Es sei K eine endliche Körpererweiterung von $\mathbb{Q}$ und $\mathcal{O}$ eine Ordnung in K.

Dann hat jedes Ideal $I \neq \{0\}$ von $\mathcal{O}$ in $\mathcal{O}$ endlichen Index, und jedes von Null verschiedene Primideal ist maximal.

Beweis. Die Ordnung $\mathcal{O}$ ist ein endlich erzeugter freier $\mathbb{Z}$-Modul, sein Rang ist gleich dem Körpergrad von K über $\mathbb{Q}$.

Es sei $x \in I$ ein von Null verschiedenes Element. Die Determinante der Multiplikation mit x auf K ist nicht 0, denn x ist invertierbar. Also hat $x\mathcal{O}$ denselben Rang wie $\mathcal{O}$, und damit endlichen Index in $\mathcal{O}$. Damit hat auch I, das zwischen $x\mathcal{O}$ und $\mathcal{O}$ liegt, endlichen Index in $\mathcal{O}$.

Ist I ein von Null verschiedenes Primideal, so ist $\mathcal{O}/I$ ein endlicher Integritätsbereich, also ein Körper, und damit I maximal. ◯

Definition/Bemerkung 4.1.2 Norm

Wenn $K \subseteq L$ eine Körpererweiterung ist, dann ist für $x \in L$ die Multiplikation mit x auf L ein K-Vektorraum-Homomorphismus. Die Determinante dieses Homomorphismus nennt man auch die *Norm von x* in der gegebenen Erweiterung: $N_{L|K}(x)$.

Im Zahlkörperfall gilt, dass die Norm (von L über $\mathbb{Q}$) von $x \in \mathcal{O}$ betragsmäßig gleich dem Index von $\mathcal{O}x$ in $\mathcal{O}$ ist. Das sieht man am Elementarteilersatz.

Man bezeichnet daher allgemeiner den Index eines Ideals $0 \neq I \subseteq \mathcal{O}$ auch als die *Norm* $N(I)$ dieses Ideals, oder noch genauer als die *Absolutnorm*.

Eine interessante Größe des Ringes $\mathcal{O}$ ist seine *Dedekindsche* [1] *Zetafunktion.* Diese ist zunächst definiert für $s \in \mathbb{C},\ \Re(s) > 1,$ und zwar durch die Formel

$$\zeta(\mathcal{O}, s) := \sum_{0 \neq I \leq \mathcal{O}} N(I)^{-s},$$

wobei die Summe über alle von 0 verschiedenen Ideale in $\mathcal{O}$ geht.

Es ist klar, dass es in $\mathcal{O}$ jeweils nur endlich viele Ideale von festem Index geben kann. Für $K = \mathbb{Q}$ ist $\zeta_{\mathbb{Z}}(s)$ einfach die Riemannsche[2] Zetafunktion. Dass diese für $\Re(s) > 1$ lokal gleichmäßig konvergiert und dort holomorph ist, ist einfach zu sehen, auch, dass sie einen Pol bei $s = 1$ haben muss. Sie lässt sich holomorph nach $\mathbb{C} \setminus \{1\}$ fortsetzen, was schon deutlich schwieriger ist.

Man kann dies und andere Einsichten noch benutzen, um zu zeigen, dass die Dedekindsche Zetafunktion stets dieses Konvergenzverhalten hat.

In speziellen Werten der Dedekindschen Zetafunktion sind arithmetische Eigenschaften von K codiert. Ihr Nullstellenverhalten gibt Aufschluss über die Verteilung der Primideale in $\mathcal{O}$, was am prägnantesten im Primzahlsatz dokumentiert wird: Aus der Tatsache, dass $\zeta_{\mathbb{Z}}$ keine Nullstelle mit Realteil 1 hat, folgt für die Funktion $\pi(x) = |\{p \in \mathbb{P} \mid p \leq x\}|$ die Aussage

$$\lim_{x \to \infty} \pi(x) \ln(x)/x = 1.$$

Beispiel 4.1.3 Quadratisches

Es sei $d \in \mathbb{Z}$ kein Quadrat und $K = \mathbb{Q}(\sqrt{d})$. Dann liegt in K die Ordnung $\mathcal{O} := \mathbb{Z}[\sqrt{d}]$. Ist $I \in \mathcal{O}$ ein von Null verschiedenes Ideal, so gibt es darin ein Element $a + b\sqrt{d}$, wobei $a, b \in \mathbb{Z}$ nicht beide Null sind. Dann liegt aber in I auch das Element $N := (a + b\sqrt{d})(a - b\sqrt{d}) = a^2 - b^2 d \neq 0$, und damit liegt auch $N\mathcal{O}$ in I. Aber $N\mathcal{O}$ hat Index N^2 in $\mathcal{O}$, und damit ist der Index von I in $\mathcal{O}$ ein Teiler von N^2.

Bemerkung 4.1.4 Warnhinweis

Entgegen den ersten Reflexen sollte man sich einen Zahlkörper nicht von vorneherein als einen Teilkörper von $\mathbb{C}$ vorstellen. Es ist vielmehr so, dass man ihn erst einmal als abstrakte Erweiterung von $\mathbb{Q}$ denken sollte, die sich auf mehrere Arten in $\mathbb{C}$ oder andere Körper einbetten lässt. Es erweist sich oft als hilfreich, diese verschiedenen Einbettungen zu berücksichtigen.

Im Abschnitt über Bewertungen werden wir dies noch flexibler gestalten.

[1] Richard Dedekind, 1831 - 1916
[2] Bernhard Riemann, 1826-1866

Definition 4.1.5 Dedekindring

Ein *Dedekindring* ist ein noetherscher Integritätsbereich, der in seinem Quotientenkörper ganz abgeschlossen ist und in dem jedes von Null verschiedene Primideal maximal ist.

Bemerkung 4.1.6 Die Maximalordnung in einem Zahlkörper ist immer ein Dedekindring. Sie ist ja eine endlich erzeugte Algebra über dem Hauptidealring $\mathbb{Z}$ und damit nach Hilberts Basissatz 3.1.6 noethersch. Die anderen Eigenschaften sind nach Definition und nach dem Hilfssatz 4.1.1 klar.

Wenn p eine Primzahl ist und K eine endliche Körpererweiterung von $\mathbb{F}_p(T)$, dann ist der ganze Abschluss von $\mathbb{F}_p[T]$ in K ein Dedekindring.

Dedekind hat Ganzheitsringe in Zahlkörpern systematisch untersucht und dabei eben die Eigenschaften ausgenutzt, die jetzt definierend für seine Ringe sind. Noethersch konnte er anfangs ja kaum schreiben...

4.2 Die Klassengruppe

Ziel dieses Abschnitts ist es, den Fundamentalsatz der Arithmetik auf den Ganzheitsring eines Zahlkörpers zu übertragen. Da dies so nicht geht, betrachtet man anstelle der Zahlen die Ideale im Ganzheitsring, und weil das wieder allgemeiner geht, betrachtet man das Ganze für Dedekindringe.

Es war übrigens eine Idee von Kummer[3], den Fundamentalsatz durch Einführung *idealer Zahlen* zu retten, was dann nach und nach zum Konzept der Ideale geführt hat. Sein Interesse lag in erster Linie darin, den großen Satz von Fermat zu beweisen, was mit seinen Methoden aber nur für eine kleine Klasse von Primzahlexponenten funktioniert, die vielleicht sogar endlich ist.

Definition 4.2.1 Produkt von (gebrochenen) Idealen

a) Es sei R ein kommutativer Ring. Das *Produkt zweier Ideale* $I, J \leq R$ ist dann definiert als das kleinste Ideal von R, das alle Produkte $ij,\ i \in I, j \in J,$ enthält:

$$IJ := \{i_1 j_1 + \cdots + i_n j_n \mid n \in \mathbb{N},\ i_a \in I, j_a \in J\}.$$

Durch diese Verknüpfung wird die Menge aller Ideale in R zu einer kommutativen Halbgruppe. Das neutrale Element ist das Ideal R selbst.

b) Wenn R nullteilerfrei ist, dann ist die Menge aller von Null verschiedenen Ideale eine Unterhalbgruppe der eben beschriebenen Halbgruppe.

[3] Ernst Eduard Kummer, 1810 - 1893

c) Wenn R nullteilerfrei und noethersch mit Quotientenkörper K ist, dann nennt man einen von Null verschiedenen Untermodul $I \subseteq K$ ein *gebrochenes Ideal*, wenn es ein $r \in R$ gibt, sodass $rI \subseteq R$ ein Ideal ist. Das sind genau die endlich erzeugten R-Untermoduln von K.

Auch die gebrochenen Ideale bilden eine kommutative Halbgruppe bezüglich der Multiplikation, die wieder durch die Formel aus a) gegeben ist.

d) In der Halbgruppe der gebrochenen Ideale gibt es mindestens eine richtige Untergruppe, nämlich die der gebrochenen Hauptideale. Das sind die Untermoduln von K, die von einem von 0 verschiedenen Element aus K erzeugt werden. Diese Gruppe ist isomorph zu $K^\times/R^\times$. Man nennt sie die Gruppe der Hauptideale, oft und auch hier wird sie mit $\mathrm{Prin}(R)$ bezeichnet. Das ist eine Abkürzung für *principal ideal*.

Beispiel 4.2.2 Hauptidealringe

Wenn R in der eben genannten Situation ein Hauptidealring ist, dann entsprechen die Ideale bijektiv den Assoziiertenklassen der Elemente von R und dies funktioniert auch mit dem Produkt.

Da in einem Hauptidealring jedes Element $\neq 0$ zu einem Produkt irreduzibler Elemente assoziiert ist, erzeugen die von Null verschiedenen Primideale die Halbgruppe aller von Null verschiedenen Ideale bezüglich der Multiplikation.

In diesem Fall ist die Halbgruppe der gebrochenen Ideale sogar eine Gruppe, nämlich $K^\times/R^\times$. Diese Gruppe ist frei abelsch mit der Menge aller Primideale als Erzeuger. Hierfür steht der Fundamentalsatz der Arithmetik (EAZ, Satz 3.2.10) gerade.

Kann man ein ähnliches Verhalten für eine größere Klasse von Ringen finden?

Definition 4.2.3 Inverses

Es sei R ein noetherscher nullteilerfreier Ring mit Quotientenkörper K und $I \subseteq K$ ein gebrochenes Ideal. Dann heißt

$$I^{-1} := \{x \in K \mid xI \subseteq R\}$$

das zu I *inverse Ideal.*

Ob es diesen Namen verdient ist eine berechtigte Frage, im Allgemeinen wird das nicht so sein.

Hilfssatz 4.2.4 Erste Miete

Es sei R ein noetherscher nullteilerfreier Ring mit Quotientenkörper K und $I \subseteq K$ ein gebrochenes Ideal.

Dann gilt für $r \in K$ die Gleichung $(rI)^{-1} = r^{-1}I^{-1}$, und I^{-1} ist ein gebrochenes Ideal.

Ist J ein weiteres gebrochenes Ideal und gilt $I \subseteq J$, so gilt $J^{-1} \subseteq I^{-1}$.

Beweis. Die erste Behauptung ist klar, wirklich, und auch die letzte.

Es ist auch klar, dass I^{-1} ein R-Modul ist. Wir müssen nur noch einsehen, dass er endlich erzeugt ist.

Dafür wählen wir ein Element $0 \neq a \in I$. Dann ist für $x \in I^{-1}$ auch $xa \in R$, also

$$I^{-1} \subseteq a^{-1}R,$$

und da R noethersch ist, ist I^{-1} endlich erzeugt.

Das ist also eigentlich auch klar. ◯

Hilfssatz 4.2.5 Ganzheit

Es seien R ein ganzabgeschlossener noetherscher Ring mit Quotientenkörper K und $I \subseteq K$ ein gebrochenes Ideal.

Weiter sei $x \in K$ ein Element mit $xI \subseteq I$.

Dann liegt x in R.

Beweis. Da I endlich erzeugt ist, lässt sich die Wirkung der Multiplikation mit x durch eine quadratische Matrix mit Koeffizienten in R beschreiben (sogar durch sehr viele Matrizen). Nach dem Satz von Cayley-Hamilton ist also x die Nullstelle eines normierten Polynoms mit Koeffizienten in R, mithin ganz über R. Da R als ganz abgeschlossen vorausgesetzt ist, gehört x bereits zu R. ◯

Hilfssatz 4.2.6 Kürzung

Es seien R ein kommutativer Ring, $P \subset R$ ein Primideal und $A, B \subseteq R$ Ideale. Wenn dann $AB \subseteq P$ gilt, aber $B \not\subseteq P$, dann folgt $A \subseteq P$.

Wenn weiter in der obigen Situation A maximal ist, dann gilt $A = P$.

Beweis. Übung!

Hilfssatz 4.2.7 Induktiv und produktiv

Es seien R ein noetherscher Ring, der kein Körper ist, und $I \subseteq R$ ein von Null verschiedenes Ideal. Dann gibt es ein $k \in \mathbb{N}_0$ und von Null verschiedene Primideale $P_1, \ldots, P_k$, sodass

$$P_1 \cdot \ldots \cdot P_k \subseteq I.$$

Beweis. Wir nehmen das Gegenteil an und bezeichnen mit $\mathcal{A}$ die dann nichtleere Menge aller von Null verschiedenen Ideale in R, in denen sich kein Produkt von Primidealen findet.

Da R noethersch ist, gibt es in $\mathcal{A}$ ein maximales Element J. Dieses ist nach Definition von $\mathcal{A}$ kein Primideal. Es ist auch nicht R, da in R ein Primideal $\neq \{0\}$ liegt.

Folglich gibt es $x, y \in R \setminus J$ mit $xy \in J$. Die Ideale $\langle J, x\rangle$ und $\langle J, y\rangle$ sind echt größer als J und daher nicht in $\mathcal{A}$, also enthalten sie Produkte $P_1 \cdot \ldots \cdot P_k$ beziehungsweise $Q_1 \cdot \ldots \cdot Q_l$ von Primidealen. Es folgt

$$P_1 \cdot \ldots \cdot Q_l \subseteq \langle J, x\rangle \cdot \langle J, y\rangle \subseteq \langle J^2, xJ, yJ, xy\rangle \subseteq J$$

im Widerspruch zu $J \in \mathcal{A}$. ◯

Hilfssatz 4.2.8 Existenz des Inversen

Es sei R ein Dedekindring und I ein gebrochenes Ideal.

Dann gilt $I^{-1} \cdot I = R$.

Beweis. Wegen 4.2.4 ist klar, dass es genügt, die Behauptung für echte Ideale in R zu zeigen.

Es sei also $I \subseteq R$ ein Ideal, $I \neq \{0\}$.

Wenn $I = R$ gilt, so folgt $I^{-1} = R$ und auch $I^{-1}I = R$.

Wenn I ein maximales Ideal ist, so gilt die Behauptung im Falle, dass I ein Hauptideal ist. Ansonsten sei $x \in I, x \neq 0$ beliebig. Mit unserem letzten Hilfssatz finden wir in Rx ein Produkt $P_1 \cdot \ldots \cdot P_k$ von 0 verschiedener Primideale, das wir so einrichten, dass k minimal ist. Es folgt mit 4.2.6, dass ohne Einschränkung $I = P_1$ angenommen werden darf (im Moment setzen wir I als maximal voraus!). Aufgrund der Minimalität von k ist $P_2 \cdot \ldots \cdot P_k$ nicht in Rx enthalten, und es gibt ein $y \in P_2 \cdot \ldots \cdot P_k$, sodass $yx^{-1} \notin R$. Für alle $z \in I$ gilt dann aber immer noch

$$yx^{-1}z \in x^{-1}P_2 \cdot \ldots \cdot P_k \cdot P_1 \subseteq x^{-1}Rx = R,$$

was in I^{-1} das Element $yx^{-1} \notin R$ zutage fördert.

Daher ist in diesem Fall $I \subset I^{-1}I \subseteq R$, und wegen der Maximalität finden wir $I^{-1}I = R$.

Nun kommt der eigentlich Beweis. Wir nehmen an, die Behauptung des Satzes sei nicht wahr. Dann ist die Menge aller ganzen Ideale $I \neq 0$ mit $I^{-1}I \neq R$ nicht leer. Da R noethersch ist, enthält diese Menge ein maximales Element M.

M ist nicht prim, da sonst nach dem oben gesehenen $M^{-1}M = R$ im Widerspruch zur Annahme. Es sei $M \subseteq P \subset R$ ein Primideal, das M enthält. Da R ein Dedekindring ist, ist P maximal.

Dann ist $P^{-1} \subseteq M^{-1}$ und daher $P^{-1}M \subseteq R$. Da P^{-1} ein nicht ganzes Element enthält, ist wegen 4.2.5 das ganze Ideal $N := P^{-1}M$ echt größer als M und somit gilt $N^{-1}N = R$.

Es folgt $M = PN$ und $P^{-1}N^{-1} \subseteq M^{-1}$, also

$$R = P^{-1}N^{-1}PN \subseteq M^{-1}M \subseteq R$$

im Widerspruch zu unserer Annahme. ◯

Beispiel 4.2.9 Quadratischer Fall

Es sei $d \in \mathbb{Z}$ quadratfrei und nicht 1 (mod 4) und $K = \mathbb{Q}(\sqrt{d})$ die zugehörige quadratische Erweiterung. Weiter sei $\mathcal{O} = \mathbb{Z}[\sqrt{d}]$ der Ganzheitsring. Der nichttriviale Automorphismus σ von K liefert auch einen Automorphismus von $\mathcal{O}$.

Weiter sei nun $0 \neq I \subseteq \mathcal{O}$ ein Ideal. Wir wollen zeigen, dass

$$\frac{1}{N(I)}\sigma(I) = I^{-1}.$$

Dazu schreiben wir uns I mittels einer $\mathbb{Z}$-Basis auf. Wir wählen ein Element $b + c\sqrt{d}$ mit minimalem positivem c. Weiter sei a der positive Erzeuger von $\mathbb{Z} \cap I$. Es ist dann klar, dass $I = \mathbb{Z}a \oplus \mathbb{Z}(b + c\sqrt{d})$. Die Norm von I ist ac.

Dabei haben wir zunächst nur die Untergruppeneigenschaft und den Rang ausgenutzt. Da I aber sogar ein Ideal ist, liegen auch $a\sqrt{d}$ und $b\sqrt{d}+cd$ in I, und die Koeffizienten vor $\sqrt{d}$ müssen durch c teilbar sein. Also teilt c sowohl a als auch b.

Da $I^{-1} = c^{-1} \cdot (I/c)^{-1}$ gilt, müssen wir die Behauptung nur für $c = 1$ testen. Das nehmen wir im weiteren an.

Da zu I auch $(b - \sqrt{d})(b + \sqrt{d}) = b^2 - d$ gehört, muss a ein Teiler hiervon sein.

Wir haben nun zu zeigen, dass $I\sigma(I) = a\mathcal{O}$ gilt. Dazu schreiben wir uns die Produkte der Erzeuger von I und $\sigma(I)$ hin:

$$a^2, a(b + \sqrt{d}), a(b - \sqrt{d}), b^2 - d.$$

Jedes dieser Elemente wird von a geteilt, also liegt sicher $I\sigma(I) \subseteq a\mathcal{O}$.

Wir müssen noch zeigen, dass $a \in I\sigma(I)$. Dazu überlegen wir uns, dass der ggT der Elemente $a^2, 2ab, b^2 - d \in I\sigma(I) \cap \mathbb{Z}$ gleich a ist. Wenn nämlich für einen Primteiler p von a die Zahl ap sowohl $2ab$ als auch b^2-d teilt, dann ist entweder $p = 2$ und damit 4 ein Teiler von b^2-d, was $d \equiv 0, 1 \pmod 4$ erzwingt und somit verboten ist. Oder p ist ein Teiler von b, und da p^2 ein Teiler von pa und damit von $b^2 - d$ ist, teilt es auch d, das aber quadratfrei sein soll. Ein Widerspruch.

Das verifiziert unsere Formel für I^{-1}, die übrigens auch für den Fall $d \equiv 1 \pmod 4$ gilt.

Folgerung 4.2.10 Eine Gruppe

Die Menge der gebrochenen Ideale eines Dedekindrings R bildet bezüglich der Multiplikation eine Gruppe. Sie ist frei abelsch über der Menge der von Null verschiedenen Primideale von R.

Beweis. Die Gruppeneigenschaft ist jetzt klar, es fehlte ja nur noch die Inversenbildung.

Jedes von Null verschiedene Ideal in R ist ein Produkt von Primidealen. Denn sonst gäbe es ein maximales Element in der Menge aller solcher Ideale M, die sich nicht als Produkt von Primidealen schreiben lassen. Dieses läge in einem Primideal P, und nach den gesehen Argumenten wäre $P^{-1}M$ ein größeres Ideal, also Produkt von Primidealen, und damit wäre auch $M = PP^{-1}M$ ein Produkt von Primidealen.

Die Darstellung von M als Produkt von Primidealen ist eindeutig. Denn aus

$$P_1P_2 \dots P_k = Q_1Q_2 \dots Q_l$$

für Primideale $P_1, \dots, Q_l$ folgt aus 4.2.6, dass eines der Primideale $Q_1, \dots, Q_l$ bereits P_1 ist.

Wenn wir dann die Gleichung auf beiden Seiten mit P_1^{-1} multiplizieren und rekursiv fortfahren, sehen wir die Eindeutigkeit der Darstellung. (Formal: Noethersche Induktion!)

Das zeigt, dass die Halbgruppe der von Null verschiedenen Ideale frei von den maximalen Idealen erzeugt wird, und dies vererbt sich auf die Gruppe der gebrochenen Ideale. ◯

Definition/Bemerkung 4.2.11 Terminologischer Übertrag

Es seien R ein Dedekindring und $I, J \subseteq R$ Ideale. Dann heißt I ein *Teiler* von J, wenn ein Ideal G existiert, sodass $GI = J$.

Ein Blick auf Hauptideale legt diese Definition nahe.

Nach dem, was wir gerade gesehen haben, teilt I genau dann J, wenn $I^{-1}J \subseteq R$, denn dies ist das einzige gebrochene Ideal, für das die gewünschte Gleichheit gilt. Nach Definition ist das äquivalent zu $I^{-1} \subseteq J^{-1}$, also zu $J \subseteq I$.

Zwei Ideale heißen *teilerfremd* wenn sie keinen echten gemeinsamen Teiler besitzen, also nicht beide in einem gemeinsamen maximalen Ideal liegen. Das ist äquivalent zu $I + J = R$.

In diesem Fall gilt $IJ = I \cap J$ und auch der Chinesische Restsatz ist gültig:

$$R/(IJ) \cong R/I \times R/J.$$

Definition/Bemerkung 4.2.12 Bewertung

Es sei K der Quotientenkörper des Dedekindrings R und $I \subset K$ ein gebrochenes R-Ideal. Dann lässt sich I schreiben als

$$I = \prod_{\substack{P \subset R \\ \text{maximal}}} P^{\mathrm{v}_P(I)}$$

mit ganzen Zahlen $\mathrm{v}_P(I)$. Insbesondere kann man dies für ein Hauptideal $I = Ra$ machen und erhält für jedes Primideal P eine Abbildung

$$\mathrm{v}_P : K \setminus \{0\} \to \mathbb{Z}, \quad a \mapsto \mathrm{v}_P(a) := \mathrm{v}_P(aR).$$

Formal setzt man dies durch $\mathrm{v}_P(0) := \infty$ nach ganz K fort.

Alternativ könnten wir für $a \in R$ auch $\mathrm{v}_P(a)$ als das Supremum aller $k \in \mathbb{Z}$ definieren, für die $a \in P^k$ gilt. Wieder formal ist hier $\sup(\mathbb{Z}) = \infty$. Dies setzt sich dann von $R \setminus \{0\}$ nach $K^\times$ multiplikativ fort.

Diese Funktion heißt die *P-adische Bewertung* auf K. Der Buchstabe v kommt vom lateinischen „valor“. Diese Abbildung hat die folgenden Eigenschaften:

$$\begin{aligned} \mathrm{v}_P(a+b) &\geq \min(\mathrm{v}_P(a), \mathrm{v}_P(b)) \\ \mathrm{v}_P(ab) &= \mathrm{v}_P(a) + \mathrm{v}_P(b) \end{aligned}$$

In der ersten Zeile gilt Gleichheit, wenn a und b verschiedene Bewertungen haben. Das folgt bequem aus der alternativen Beschreibung von $\mathrm{v}_P(a)$.

Diese Eigenschaften werden wir später wieder aufgreifen, um aus der Bewertung eine Metrik auf K zu gewinnen. Das gibt uns dann für jedes Primideal eine Topologie auf K, und man kann gerade im Zahlkörperfall manche arithmetischen Phänomene dann topologisch zum Ausdruck bringen oder auch beweisen.

Definition 4.2.13 Die Idealklassengruppe

Es sei R ein Dedekindring.

Die Gruppe der gebrochenen Ideale von R heißt die *Divisorengruppe* $\mathrm{Div}(R)$.

Darin ist die Gruppe $\mathrm{Prin}(R)$ der gebrochenen Hauptideale eine Untergruppe.

Die Faktorgruppe $\mathrm{Cl}(R) := \mathrm{Div}(R)/\mathrm{Prin}(R)$ heißt die *Idealklassengruppe* von R. Ihre Größe misst, wie weit R davon entfernt ist, ein Hauptidealring zu sein.

R ist nämlich genau dann ein Hauptidealring, wenn $\mathrm{Cl}(R)$ trivial ist.

Da die Gruppe der gebrochenen Ideale von den Primidealen erzeugt wird, ist dies auch äquivalent dazu, dass alle Primideale Hauptideale sind.

Ein wichtiges Hilfsmittel bei der Frage, wieviele Idealklassen es gibt, ist die Norm der Ideale, wie wir sie in 4.1.2 eingeführt haben. Es gilt der folgende Satz:

Hilfssatz 4.2.14 Multiplikativität der Absolutnorm

Es seien K ein Zahlkörper und $I, J \subseteq \mathcal{O}_K$ zwei von Null verschiedene Ideale. Dann gilt $N(IJ) = N(I) \cdot N(J)$.

Beweis. Aus der Zerlegung von I und J als Produkte von Primidealen sieht man wegen des Chinesischen Restsatzes, dass es genügt, die Behauptung für Potenzen eines festen Primideals $P \neq \{0\}$ zu zeigen.

Das heißt: Wir zeigen für alle $n \in \mathbb{N}_0$ die Gleichung $N(P^{n+1}) = N(P) \cdot N(P^n)$.

Dazu wählen wir ein $t \in P^n \setminus P^{n+1}$ und betrachten die Abbildung

$$\Phi : \mathcal{O}_K \to P^n/P^{n+1}, \quad x \mapsto xt + P^{n+1}.$$

Der Kern von Φ ist ein Ideal, das P enthält, da $tP \subseteq P^{n+1}$. Da jedoch $1 \notin \text{Kern}(\Phi)$, gilt $P = \text{Kern}(\Phi)$ wegen der Maximalität von P. Das Bild von Φ ist $(\mathcal{O}_K t + P^{n+1})/P^{n+1}$. Da aber $\mathcal{O}_K t + P^{n+1}$ ein Ideal ist, das zwischen P^n und P^{n+1} liegt, muss es P^n sein (da $t \notin P^{n+1}$). Folglich vermittelt Φ eine Bijektion zwischen $\mathcal{O}_K/P$ und P^n/P^{n+1}.

Das zeigt die behauptete Multiplikativität. ◯

Bemerkung 4.2.15 Ein Vektorraum

Wir sehen am Argument, dass P^n/P^{n+1} jeweils ein eindimensionaler $\mathcal{O}_K/P$-Vektorraum ist. Das gilt – mit dem selben Argument – für jeden Dedekindring.

Bemerkung 4.2.16 Eulers Produktformel

Wir erinnern an 4.1.2 und die dort gemachte Definition der Dedekindschen Zetafunktion eines Zahlkörpers. Sie ist gegeben durch

$$\zeta_K(s) = \sum_I \frac{1}{N(I)^s},$$

wobei sich die Summe über alle Ideale $I \neq \{0\}$ im Ganzheitsring erstreckt.

Wir hatten eingesehen, dass sie wenigstens für großen Realteil von s konvergiert. Aus der Identität

$$N(I) = N(\prod_P P^{v_P(I)}) = \prod_P N(P)^{v_P(I)}$$

und der Eindeutigkeit der Zerlegung von I als Produkt von Primidealen folgt wie für die Riemannsche Zetafunktion eine Produktformel:

$$\zeta_K(s) = \prod_P \frac{1}{1 - N(P)^{-s}}, \quad \Re(s) >> 0.$$

Das sieht man durch Entwicklung der Faktoren in eine geometrische Reihe und Cauchy-Faltung der Faktoren.

Bemerkung 4.2.17 Ideale und Matrizen

Bevor wir uns genauer den Primidealen zuwenden soll hier noch ein kurzer Blick auf Äquivalenz von (gebrochenen) Idealen riskiert werden.

Es sei K ein Zahlkörper und $\mathcal{O}$ eine Ordnung in K. Zwei $\mathcal{O}$-Ideale I, J heißen äquivalent, wenn es eine Einheit $\alpha \in K^\times$ gibt, mit $I = \alpha J$. Im Falle der Hauptordnung sind die Äquivalenzklassen gerade die Elemente der Klassengruppe.

Was ist so ein Ideal im Falle einer von einem Element γ erzeugten Ordnung? Sei also jetzt $\mathcal{O} = \mathbb{Z}[\gamma]$. Der Grad von K über $\mathbb{Q}$ sei n.

Ein Ideal in $\mathcal{O}$ ist dann immer eine frei abelsche Gruppe vom Rang n, auf der ein Endomorphismus φ definiert ist, der dasselbe Minimalpolynom wie γ hat: Die Multiplikation mit γ. Bezüglich einer Basiswahl ist dann φ durch eine $n \times n$ Matrix mit ganzzahligen Einträgen beschrieben. Bei Wahl einer anderen $\mathbb{Z}$-Basis des Ideals wird diese Matrix ersetzt durch eine unimodular äquivalente Matrix, also eine Matrix, die ähnlich ist, wo jedoch die Ähnlichkeit durch eine ganzzahlige Matrix mit ganzzahliger Inverser vermittelt wird.

Wenn umgekehrt $A \in \mathbb{Z}^{n\times n}$ eine Nullstelle des Minimalpolynoms von γ ist, dann ist $\mathbb{Z}^n$ ein $\mathbb{Z}[A] \cong \mathbb{Z}[\gamma]$-Modul, und $\mathbb{Q}^n$ wird zu einem $\mathbb{Q}[A] \cong \mathbb{Q}(\gamma) = K$-Modul, also ein K-Vektorraum, der – die Dimension über $\mathbb{Q}$ kennen wir ja – über K eindimensional ist. Wir können also $\mathbb{Z}^n$ auffassen als Untergruppe eines eindimensionalen K-Vektorraums, die gleichzeitig ein $\mathcal{O}$-Modul ist. Das ist also isomorph zu einem gebrochenen $\mathcal{O}$-Ideal.

Wir erhalten damit eine Bijektion zwischen der Menge aller Äquivalenzklassen von Idealen und der Menge aller unimodularen Äquivalenzklassen von Nullstellen des Minimalpolynoms von γ in $\mathbb{Z}^{n\times n}$.

Bemerkung 4.2.18 Primideale

Es sei K ein Zahlkörper und $\mathcal{O}$ sein Ganzheitsring. Der Durchschnitt eines Primideals $P \neq \{0\}$ in $\mathcal{O}$ mit $\mathbb{Z}$ ist dann ein Primideal in $\mathbb{Z}$, und damit von einer Primzahl p erzeugt.

Umgekehrt sei $p \in \mathbb{Z}$ eine Primzahl. Dann ist $p\mathcal{O}$ ein echtes Ideal in $\mathcal{O}$, denn sonst wäre p^{-1} ganz. Also liegt $p\mathcal{O}$ in mindestens einem Primideal von $\mathcal{O}$. Da $p\mathcal{O}$ endlichen Index in $\mathcal{O}$ hat, gibt es nur endlich viele Primideale, die p enthalten.

Dies sind genau die Primideale P_i, die an der Faktorisierung

$$p\mathcal{O} = P_1^{e_1} \cdot \dots \cdot P_m^{e_m}$$

nichttrivial beteiligt sind. Denn $p \in P$ ist äquivalent zu $P^{-1} \subseteq (p)^{-1}$.

Man kennt also alle Primideale in $\mathcal{O}$, wenn für jede Primzahl p klar ist, wie (p) sich als Produkt von Primidealen schreiben lässt. Das muss man systematisch untersuchen.

Das kennen wir aus EAZ, 3.2.11, wo wir so etwas für den Ring der ganzen Gaußschen Zahlen gemacht haben.

Je nachdem, wie sich $p\mathcal{O}_K$ in Primideale faktorisiert, schreibt man p ein Adjektiv zu. Wenn $p\mathcal{O}_K$ selbst prim ist, so nennt man p *träge*, wenn kein Primideal in der Faktorisierung mehrfach auftritt *unverzweigt*, und wenn alle Primfaktoren Index p haben, heißt p *voll zerlegt*.

Dies sind Eigenschaften, die in der algebraischen Zahlentheorie eine große Rolle spielen.

Beispiel 4.2.19 Quadratisch - praktisch - gut

Es sei $1 \neq d \in \mathbb{Z}$ quadratfrei und $L = \mathbb{Q}(\sqrt{d})$ die zugehörige quadratische Erweiterung von $\mathbb{Q}$. Weiter sei $\omega \in \mathcal{O}_L$ der übliche Erzeuger, also $\omega = \frac{1+\sqrt{d}}{2}$, wenn d bei Division durch 4 Rest 1 lässt, und $\omega = \sqrt{d}$ sonst. Die Diskriminante von $\mathcal{O}_L = \mathbb{Z}[\omega]$ ist hier die Diskriminante des Minimalpolynoms M von ω.

Dann gilt für die Primzahl $p \in \mathbb{Z}$ (bzw. für das von ihr erzeugte Ideal in $\mathbb{Z}$):

- p ist genau dann träge, wenn das Minimalpolynom von ω keine Nullstelle in $\mathbb{F}_p$ hat.
- p ist genau dann voll zerlegt, wenn das Minimalpolynom von ω zwei einfache Nullstellen in $\mathbb{F}_p$ hat.
- p ist genau dann verzweigt wenn es die Diskriminante von L teilt.

Denn:

Für jede Primzahl p gilt

$$\mathcal{O}_L/(p) = \mathbb{Z}[X]/(p, M) = \mathbb{F}_p[X]/(M \pmod p).$$

Wenn p ein Teiler der Diskriminante ist, dann hat M eine doppelte Nullstelle $a + p\mathbb{Z}$ in $\mathbb{F}_p$. Es folgt, dass p in genau einem Primideal von $\mathcal{O}_L$ liegt, nämlich dem, das von p und $\omega - a$ erzeugt wird. Dieses hat Norm p, und es ist das einzige Primideal, das an der Primidealzerlegung von $p\mathcal{O}_L$ beteiligt ist. Also muss

$$p\mathcal{O}_L = P^2$$

gelten.

Wenn p kein Teiler der Diskriminante ist, dann hat M entweder 2 einfache Nullstellen $a + p\mathbb{Z}$ und $b + p\mathbb{Z}$ in $\mathbb{F}_p$, und p liegt in den zwei Primidealen $P_1 = (p, \omega - a)$ und $P_2 = (p, \omega - b)$. Diese Primideale sind beide an der Primzerlegung von $p\mathcal{O}_L$ beteiligt, und aus Indexgründen folgt $p\mathcal{O}_L = P_1 \cdot P_2$. Oder M hat keine

Nullstelle in $\mathbb{F}_p$, ist also (da quadratisch) in $\mathbb{F}_p[X]$ irreduzibel, was zeigt, dass $p\mathcal{O}_L$ ein Primideal ist.

Alles in allem sind damit alle Behauptungen gezeigt.

Hilfssatz 4.2.20 *Es sei K ein algebraischer Zahlkörper von Grad n über $\mathbb{Q}$ und*

$$p\mathcal{O}_K = P_1^{e_1} \cdot \ldots \cdot P_g^{e_g}$$

die Zerlegung des von der Primzahl p erzeugten Ideals in $\mathcal{O}_K$.

Weiter sei $\mathcal{O}_K/P_i = \mathbb{F}_{p^{f_i}}$.

Dann gilt $\sum_{i=1}^{g} e_i f_i = n$.

Beweis. Es ist p^n die Norm des betrachteten Ideals, die andererseits auch

$$\prod N(P_i)^{e_i} = \prod (p^{f_i})^{e_i} = p^{\sum f_i e_i}$$

ist. Das zeigt die Behauptung. ◯

4.3 Diskrete Bewertungen

Definition 4.3.1 Diskrete Bewertung

Es sei K ein Körper. Eine *diskrete Bewertung* auf K ist eine Abbildung

$$\mathrm{v} : K \to \mathbb{R} \cup \{\infty\}$$

mit folgenden Eigenschaften:

- $\mathrm{v}^{-1}(\infty) = \{0\}$.
- $\mathrm{v}(K^\times) \subset \mathbb{R}$ ist diskret.
- $\forall x, y \in K : \ \mathrm{v}(xy) = \mathrm{v}(x) + \mathrm{v}(y)$.
- $\forall x, y \in K : \ \mathrm{v}(x+y) \geq \min\{\mathrm{v}(x), \mathrm{v}(y)\}$.

Insbesondere ist $\mathrm{v}(K^\times)$ eine diskrete Untergruppe von $(\mathbb{R}, +)$ und damit zyklisch. Die Bewertung v heißt *trivial*, wenn $\forall x \in K^\times : \mathrm{v}(x) = 0$.

Beispiel 4.3.2 Zahlentheorie

Die Bewertungen aus 4.2.12 sind natürlich Beispiele für Bewertungen.

Hilfssatz 4.3.3 Bewertungsring

Es sei v *eine nichttriviale Bewertung auf dem Körper* K*.*

Dann ist $\mathcal{O}_\mathrm{v} := \{x \in K \mid \mathrm{v}(x) \geq 0\}$ *ein Teilring von* K*. Er ist ein Hauptidealring mit nur einem Primideal* $P \neq \{0\}$*, und* v *ist (bis auf einen Faktor) die Bewertung* v_P*.*

Beweis. Die Ringeigenschaften kann man sofort nachrechnen, man bemerke insbesondere, dass $\mathrm{v}(1) = 0$. Das zeigt insbesondere, dass die Einheiten in $\mathcal{O}_\mathrm{v}$ genau die Elemente mit Bewertung 0 sind.

Nun sei $\pi \in \mathcal{O}_\mathrm{v}$ derart, dass $\mathrm{v}(K^\times) = \mathbb{Z}\mathrm{v}(\pi)$.

Weiter sei $I \subseteq \mathcal{O}_\mathrm{v}$ ein von Null verschiedenes Ideal.

Dann ist auch $\mathrm{v}(I \setminus \{0\}) \subseteq \mathbb{R}$ diskret und enthält damit ein kleinstes Element w. Es sei $a \in I$ ein Element mit Bewertung w und $b \in I$ beliebig. Dann ist $\mathrm{v}(b/a) \geq 0$ und damit $b/a \in \mathcal{O}_\mathrm{v}$, also $I = \mathcal{O}_\mathrm{v} \cdot a$ ein Hauptideal.

Da außerdem $\mathrm{v}(a/\pi^n) = w - n\mathrm{v}(\pi) = 0$ ist für eine geeignete natürliche Zahl n, ist a assoziiert zu einer Potenz von π.

Das zeigt, dass jedes Ideal $\neq \{0\}$ in $\mathcal{O}_\mathrm{v}$ von einer Potenz von π erzeugt wird. Damit ist $\mathcal{O}_\mathrm{v} \cdot \pi$ das einzige von Null verschiedene Primideal in $\mathcal{O}_\mathrm{v}$.

Die letzte Behauptung ist dann klar. ◯

Definition 4.3.4 Bewertungsring

In der Situation des letzten Hilfssatzes heißt $\mathcal{O}_\mathrm{v}$ der *Bewertungsring* von v und das maximale Ideal darin heißt das *Bewertungsideal*.

Zwei Bewertungen heißen äquivalent, wenn sie denselben Bewertungsring besitzen.

Der Bewertungsring hat folgende Eigenschaft: Für alle $x \in K^\times$ gilt $x \in \mathcal{O}_\mathrm{v}$ oder $x^{-1} \in \mathcal{O}_\mathrm{v}$. Diese Eigenschaft gehört zu den definierenden Eigenschaften des abstrakten Konzepts eines Bewertungsrings, der dann aber nicht unbedingt zu einer diskreten Bewertung gehören muss.

Beispiel 4.3.5 Alle Bewertungen auf $\mathbb{Q}$ und einige auf $\mathbb{C}(T)$

a) Es sei v eine nichttriviale, diskrete Bewertung auf $\mathbb{Q}$. Der Bewertungsring von v umfasst dann $\mathbb{Z}$, und das Bewertungsideal von v hat mit $\mathbb{Z}$ ein Primideal als Durchschnitt. Es gibt also genau eine Primzahl p im Bewertungsideal, und alle anderen Primzahlen sind Einheiten. Also ist der Bewertungsring der Ring

$$\mathbb{Z}_{(p)} = \{\frac{a}{b} \mid a, b \in \mathbb{Z}, b \notin p\mathbb{Z}\}.$$

Damit ist jede nichttriviale Bewertung auf $\mathbb{Q}$ zu einer unserer altbekannten p-adischen Bewertungen äquivalent.

b) Es sei v eine nichttriviale Bewertung auf dem rationalen Funktionenkörper $\mathbb{C}(T)$ in einer Variablen. Weiter sei v auf $\mathbb{C}$ trivial, also $\mathbb{C}$ im Bewertungsring $\mathcal{O}$ enthalten.

Nach der Bemerkung aus der letzten Definition gilt dann für die Variable T, dass $T \in \mathcal{O}_\mathrm{v}$ oder $T^{-1} \in \mathcal{O}_\mathrm{v}$.

Im ersten Fall liegt der Polynomring $\mathbb{C}[T]$ im Bewertungsring, und das Bewertungsideal hat mit $\mathbb{C}[T]$ ein Primideal als Durchschnitt. Da $\mathbb{C}$ algebraisch abgeschlossen ist, wird dieses Primideal von einem linearen Polynom $(T-a)$, $a \in \mathbb{C}$, erzeugt. Die Bewertung v ist dann einfach die zu $T-a$ gehörende Bewertung, und

$$\mathrm{v}(f) = \mathrm{ord}(f, a)$$

ist die (Nullstellen-)Ordnung der rationalen Funktion f an der Stelle a.

Ist hingegen $T \notin \mathcal{O}_\mathrm{v}$, so umfasst der Bewertungsring den Polynomring $\mathbb{C}[T^{-1}]$ und das Bewertungsideal liefert ein Primideal darin. Da $\mathrm{v}(T) < 0$ gilt, folgt $\mathrm{v}(T^{-1}) > 0$, und somit liegt das irreduzible Element T^{-1} im Bewertungsideal, also hat dieses mit $\mathbb{C}[T^{-1}]$ gerade das von T^{-1} erzeugte Hauptideal als Durchschnitt. Es ist also

$$\mathrm{v}(f) = -\mathrm{grad}(\text{Zähler von } f) + \mathrm{grad}(\text{Nenner von } f).$$

Das ist die Nullstellenordnung von f bei unendlich!

Wir erhalten somit als Menge aller Äquivalenzklassen von Bewertungen die Menge

$$\mathbb{C} \cup \{\infty\} = \mathbb{P}^1(\mathbb{C}).$$

Diese Sichtweise auf Bewertungen sorgt (mit noch einigem Aufwand) dafür, dass man für jeden Körper K, der über einem Körper k Transzendenzgrad 1 hat (also eine algebraische Erweiterung eines rationalen Funktionenkörpers $k(T)$ ist), die Menge der Äquivalenzklassen nichttrivialer Bewertungen, die auf k trivial sind, als geometrisches Objekt auffassen kann.

4.4 Beträge

Definition 4.4.1 Betragen gut

Es sei K ein Körper und $|\cdot| : K \to \mathbb{R}_{\geq 0}$ eine Abbildung mit den Eigenschaften

- $\forall a \in K : \ |a| = 0 \iff a = 0$,

- $\forall a, b \in K: \ |ab| = |a| \cdot |b|$,
- $\forall a, b \in K: \ |a + b| \leq |a| + |b|$.

Dann heißt $|\cdot|$ ein *Betrag* auf K.

Hierbei ist stets $|1| = 1$, da $|1| = |1 \cdot 1| = |1| \cdot |1|$.

Aus $|1| = |-1| \cdot |-1|$ folgt dann, dass auch $|-1| = 1$ gelten muss.

Die letzte Ungleichung in der Definition heißt wieder die Dreiecksungleichung. K wird zu einem metrischen Raum, wenn wir

$$d(a, b) := |a - b|$$

setzen. Wegen $|-1| = 1$ ist dies symmetrisch.

Der Betrag $|\cdot|$ heißt *trivial*, wenn er auf $K \setminus \{0\}$ konstant gleich 1 ist. Dies ist genau dann der Fall, wenn die zugehörige Metrik die diskrete Metrik auf K ist.

Beispiel 4.4.2 Der Betrag zu einer diskreten Bewertung

Es sei K ein Körper und v eine diskrete Bewertung auf K. Weiter sei $b > 1$ eine reelle Zahl. Dann wird durch

$$|x|_{\mathrm{v}} := b^{-\mathrm{v}(x)}$$

ein Betrag auf K gegeben.

Bemerkung 4.4.3 Stetigkeit

Es sei K ein Körper mit einem gegebenen Betrag. Dann kann man wie in der Analysis den Begriff der stetigen Funktion auf (Teilmengen von) K definieren. Für $D \subseteq K$ ist die Abbildung $f: D \to K$ stetig in $x_0 \in D$, wenn für alle $\delta > 0$ ein $\varepsilon > 0$ existiert, sodass

$$\forall x \in D: |x - x_0| < \varepsilon \Rightarrow |f(x) - f(x_0)| < \delta.$$

Wegen der Dreiecksungleichung ist die Summe zweier in x_0 stetiger Funktionen wieder in x_0 stetig. Die Multiplikativität des Betrags und ein Teleskopsummenargument zeigen, dass auch das Produkt zweier in x_0 stetiger Funktionen wieder in x_0 stetig ist.

Die Abbildung f heißt stetig, wenn sie in jedem Punkt aus D stetig ist. Da insbesondere konstante Funktionen und die Identität stetig sind, ist damit auch jede polynomiale Abbildung stetig.

In Wirklichkeit merkt die Definition der Stetigkeit gar nicht den Betrag, sondern nur die Topologie, die durch ihn geliefert wird. Eine Teilmenge von D heißt *in*

D offen, wenn sie mit jedem Punkt auch eine ganze r-Umgebung dieses Punkts in D enthält (für geeignetes $r > 0$).

Stetigkeit verlangt dann einfach, dass das Urbild einer offenen Menge in K stets in D offen ist.

Beispiel 4.4.4 Rationale Zahlen

Auf $K = \mathbb{Q}$ betrachten wir die folgenden Beträge:

$|\cdot|_\infty$ sei der übliche Absolutbetrag. Diesen verzieren wir ab jetzt mit dem Index ∞, um ihn von anderen Beträgen unterscheiden zu können.

Für eine Primzahl p wird durch $|a|_p = p^{-\mathrm{v}_p(a)}$ der *p-adische Absolutbetrag* definiert. Dabei ist v_p die p-adische Bewertung aus EAZ 3.2.5-3.2.7 .

Wie unterschiedlich sind diese Beträge?

Definition 4.4.5 Eine Äquivalenzrelation

Es seien K eine Körper und $|\cdot|_1$ und $|\cdot|_2$ zwei Beträge auf K. Dann nennen wir diese Beträge *äquivalent*, wenn jede offene Kugel bezüglich des einen auch eine offene Kugel bezüglich des anderen enthält und umgekehrt.

Abstrakter gesagt heißt das, dass die beiden Beträge dieselbe Topologie auf K liefern (siehe 4.4.3), also dieselben offenen Mengen.

Insbesondere muss dann für $x \in K$ die Folge (x^n) bezüglich $|\cdot|_1$ gegen 0 konvergieren genau dann, wenn sie dies bezüglich $|\cdot|_2$ tut. Das heißt aber wegen der Multiplikativität der Beträge, dass

$$|x|_1 < 1 \iff |x|_2 < 1.$$

Hilfssatz 4.4.6 Eine Konkretisierung

Es seien $|\cdot|_1$ und $|\cdot|_2$ zwei nichttriviale Beträge auf dem Körper K.

Dann sind äquivalent:

i) $|\cdot|_1$ und $|\cdot|_2$ sind äquivalent.

ii) Es gibt eine positive reelle Zahl s mit $|\cdot|_1 = |\cdot|_2^s$.

Beweis. Nur *i)* $\Rightarrow$ *ii)* ist bemerkenswert.

Zunächst sehen wir aufgrund der letzten Bemerkung in der Definition, dass für alle $x, y \in K$ gilt:

$$|x|_1 < |y|_1 \iff |x|_2 < |y|_2.$$

Da die Beträge nicht trivial sind, können wir ein $a \in K$ wählen mit $|a|_i > 1$, $i = 1, 2$.

Wir definieren $s > 0$ durch die Gleichung

$$|a|_1 = |a|_2^s.$$

Nun sei $0 \neq x \in K$ beliebig. Wir müssen zeigen, dass für das eben definierte s auch $|x|_1 = |x|_2^s$ richtig ist.

Dazu schreiben wir $|x|_1 = |a|_1^e,\ |x|_2 = |a|_2^f$ für positive Zahlen e, f und weisen jetzt nach, dass $e = f$.

Dazu betrachten wir rationale Zahlen

$$\frac{k}{n} < e < \frac{m}{n},\ k, m, n \in \mathbb{N}.$$

Dann gilt wegen $k < ne < m$ und wegen der Multiplikativität der Beträge

$$|a^k|_1 < |a|_1^{ne} = |x^n|_1 < |a^m|_1,$$

und dieselbe Ungleichungskette muss für $|\cdot|_2$ gelten, wobei hier jedoch $|x^n|_2 = |a|_2^{nf}$ gilt. Das zeigt durch Vergleich, dass auch

$$\frac{k}{n} < f < \frac{m}{n}$$

stimmt, und das geht nur dann für alle Wahlen von $k, n, m,$ wenn $e = f$. ◯

Folgerung 4.4.7 Verschiedenheit

Die in 4.4.4 angegebenen Beträge auf $\mathbb{Q}$ sind paarweise nicht äquivalent.

Denn: Es gibt für je zwei verschiedene dieser Beträge immer eine rationale Zahl, deren einer Betrag < 1 ist und der andere ≥ 1.

Dafür kann man entweder eine der beteiligten Primzahlen nehmen, wenn beide Beträge p-adisch sind, oder die eine Primzahl, wenn ein Betrag p-adisch und der andere der reelle ist.

Hilfssatz 4.4.8 Heureka

Es sei K ein Körper, der $\mathbb{Q}$ enthält und $|\cdot|$ ein nichttrivialer Betrag auf K.

Dann sind äquivalent:

i) $|2| \leq 1$

ii) $\forall n \in \mathbb{N} :\ |n| \leq 1.$

Beweis.

Die eine Richtung ist klar, setzen wir also $|2| \leq 1$ voraus. Es sei $1 < n \in \mathbb{N}$. Dann hat n eine Binärentwicklung:

$$n = \sum_{i=0}^{\lfloor \log_2(n) \rfloor} a_i 2^i, \quad a_i \in \{0,\ 1\}.$$

Aus $|2^i| = |2|^i \leq 1$ und der Dreiecksungleichung folgt

$$|n| \leq \log_2(n).$$

Andererseits ist für $e \in \mathbb{N}$

$$|n|^e = |n^e| \leq e \log_2(n),$$

und da dies die Potenzfunktion durch eine lineare Funktion majorisiert, muss $|n| \leq 1$ gelten. Also ist tatsächlich $|n| \leq 1$ für alle natürlichen Zahlen. ◯

Definition 4.4.9 Archimedes[4]

Es sei $|\cdot|$ ein Betrag auf einem Körper K, der $\mathbb{Q}$ enthält. Dieser heißt *archimedisch*, falls eine natürliche Zahl n existiert mit $|n| > 1$.

Wir haben eben gesehen, dass dies zu $|2| > 1$ gleichbedeutend ist. Ein zum Argument dort analoges Argument zeigt, dass dann tatsächlich für alle $n \in \mathbb{N}_{>1}$ die Ungleichung $|n| > 1$ gilt.

Der Betrag heißt *nicht archimedisch*, falls für alle $n \in \mathbb{N}$ die Ungleichung $|n| \leq 1$ gilt.

Zum Beispiel auf dem Körper $K = \mathbb{Q}$ ist $|\cdot|_\infty$ archimedisch und $|\cdot|_p$ nicht-archimedisch (für jede Primzahl p).

Satz 4.4.10 Satz von Ostrowski[5]

Es sei $|\cdot|$ ein nichttrivialer Betrag auf $\mathbb{Q}$. Dann ist $|\cdot|$ äquivalent zu einem der Beträge $|\cdot|_\infty$ oder $|\cdot|_p$, $p \in \mathbb{P}$.

Beweis. Wir unterscheiden den archimedischen und den nicht archimedischen Fall.

Fall 1: Es sei $|\cdot|$ nicht archimedisch, das heißt $|n| \leq 1$ für alle $n \in \mathbb{N}$. Da $|\cdot|$ als nicht trivial vorausgesetzt ist, gibt es eine Primzahl p mit $|p| < 1$. Sonst wäre ja stets $|p| = 1$ und der Betrag aufgrund seiner Multiplikativität trivial.

[4] Archimedes, ca. 287 v.Chr. - 212 v.Chr.
[5] Alexander Ostrowski, 1893 - 1986

Wenn es nun eine zweite Primzahl q gäbe mit $|q| < 1$, so könnten wir eine natürliche Zahl N finden mit

$$|p^N|,\ |q^N| < \frac{1}{2}.$$

Da andererseits p, q teilerfremd sind, können wir die 1 linear aus ihnen kombinieren:

$$\exists a, b \in \mathbb{Z} : 1 = ap^N + bq^N.$$

Das erzwingt

$$|1| = |ap^N + bq^N| < \frac{1}{2}(|a| + |b|) \leq 1,$$

da ja auch $|a|, |b| \leq 1$.

Das ist ein Widerspruch zu $|1| = 1$.

Also gibt es genau eine Primzahl p mit $|p| < 1$. Nun sei $x \in \mathbb{Q}^\times$ beliebig. Dann ist

$$x = \pm \prod_{\ell \in \mathbb{P}} \ell^{\mathrm{v}_\ell(x)},$$

und aus der Multiplikativität des Betrags folgt

$$|x| = \prod_{\ell \in \mathbb{P}} |\ell|^{\mathrm{v}_\ell(x)} = |p|^{\mathrm{v}_p(x)},$$

denn alle anderen Faktoren sind ja 1. Wenn wir hier die reelle Zahl $s > 0$ durch

$$|p| = p^{-s}$$

definieren (was geht, da $|p| < 1$), so folgt

$$|x| = p^{-s\mathrm{v}_p(x)} = |x|_p^s.$$

Da s von x nicht abhängt, sind $|\cdot|$ und $|\cdot|_p$ äquivalent.

Fall 2: Es sei $|\cdot|$ archimedisch. Nach Hilfssatz 4.4.8 und der Dreiecksungleichung wissen wir $1 < |2| \leq 2$.

Sei $1 < a \in \mathbb{N}$ eine weitere Zahl. Auch hier wissen wir $1 < |a| \leq a$.

Wir entwickeln 2^n bezüglich der Grundzahl a:

$$2^n = \sum_{i=0}^{N} c_i a^i,\ 0 \leq c_i < a.$$

Für N haben wir die Abschätzung $a^N \leq 2^n$, also

$$N \leq n \log 2 / \log a.$$

Die Dreiecksungleichung sagt uns dann

$$|2|^n \leq a \cdot (N+1)|a|^N \leq a(n \log 2/\log a + 1)(|a|^{\log 2/\log a})^n.$$

Lässt man hier n gegen unendlich gehen, so folgt aus asymptotischen Gründen

$$\log |2|/\log 2 \leq \log |a|/\log a.$$

Nun können aber die Rollen von a und 2 bei dieser Abschätzung vertauscht werden, was die Gleichheit dieser beiden Quotienten zeigt.

Es folgt

$$|a| = a^{\log |2|/\log 2} = |a|_\infty^{\log |2|/\log 2}$$

für beliebiges $a \in \mathbb{N}$, und aus der Multiplikativität des Betrags folgt dieselbe Beziehung für alle $a \in \mathbb{Q}$. ◯

Bemerkung 4.4.11 Die ultrametrische Ungleichung

Es sei p eine Primzahl und $|\cdot|_p$ der p-adische Betrag auf $\mathbb{Q}$. Die Menge

$$\mathbb{Z}_{(p)} := \{x \in \mathbb{Q} \mid |x|_p \leq 1\} = \{\frac{m}{n} \mid m, n \in \mathbb{Z},\ p \not| n\}$$

ist ein Teilring von $\mathbb{Q}$. Die Einheiten darin sind genau die Zahlen mit Betrag 1, also

$$\mathbb{Z}_{(p)}^\times = \{\frac{m}{n} \mid p \not| mn\}.$$

Jede Zahl $0 \neq x \in \mathbb{Q}$ lässt sich auf eindeutige Art zerlegen als

$$x = p^{\mathrm{v}_p(x)}u, \quad u \in \mathbb{Z}_{(p)}^\times.$$

Daran sieht man für alle x, y:

$$\begin{aligned} |x+y|_p &\leq \max\{|x|_p, |y|_p\}, \\ |x+y|_p &= \max\{|x|_p, |y|_p\}, \text{ falls } |x|_p \neq |y|_p. \end{aligned}$$

Wenn x oder y 0 sind, ist das klar. Ansonsten schreiben wir $x = p^v u, y = p^f e$ mit $u, e \in \mathbb{Z}_{(p)}^\times$ und sehen mit $m := \min(v, f)$

$$|x+y|_p = |p^m(p^{v-m}u + p^{f-m}e)|_p \leq p^{-m}.$$

Im Fall $v \neq f$ ist der zweite Faktor zwangsläufig eine Einheit in $\mathbb{Z}_{(p)}$.

Bemerkung 4.4.12 Komplettierung

Es sei $|\cdot|$ ein Betrag auf $\mathbb{Q}$. Dann können wir $\mathbb{Q}$ bezüglich dieses Betrags vervollständigen.

Das Ergebnis heißt im Fall des p-adischen Betrags $\mathbb{Q}_p$. In Analogie schreiben manche Leute statt $\mathbb{R}$ in diesem Kontext auch $\mathbb{Q}_\infty$.

Ein Unterschied, der bei den Komplettierungen wesentlich ist, ist, dass bei einer p-adischen Cauchy-Folge in $\mathbb{Q}$ der p-adische Betrag der Folgenglieder automatisch fast konstant ist, wenn es sich nicht um eine Nullfolge handelt. Dies kann man benutzen, um die Metrik von $\mathbb{Q}$ nach $\mathbb{Q}_p$ fortzusetzen. Die Norm einer p-adischen Cauchy-Folge (x_n) in $\mathbb{Q}$ ist 0, wenn es eine Nullfolge ist, oder $\lim_{n\to\infty} |x_n|_p$, was ja schließlich konstant wird. Wenn es nämlich keine Nullfolge ist, dann existiert ein $\varepsilon > 0$ und ein $N \in \mathbb{N}$, sodass für alle $n \geq N$ auch $|x_n|_p \geq \varepsilon$. Wenn weiter – was man durch Wahl von N einrichten kann – für alle $m, n \geq N$ $|x_m - x_n| \leq \varepsilon/2$ gilt, dann folgt aus 4.4.11 die Behauptung

$$|x_n|_p = |x_m + (x_n - x_m)|_p = |x_m|_p.$$

Diese Norm liefert einen Abstand auf dem Vektorraum Cauchy-Folgen/Nullfolgen, und bezüglich dieses Abstands rechnet man die Vollständigkeit desselben nach.

Bemerkung 4.4.13 Die ganzen p-adischen Zahlen

Ein ungewohntes Phänomen bei den p-adischen Zahlen ist, dass $\mathbb{Z}$ hier nicht diskret liegt. Der Abschluss $\mathbb{Z}_p$ von $\mathbb{Z}$ in $\mathbb{Q}_p$ heißt auch Ring der ganzen p-adischen Zahlen.

Dieser Ring $\mathbb{Z}_p$ lässt sich auf folgende Art besser vor Augen führen. Wir fangen an mit einer speziellen Klasse von Cauchy-Folgen in $\mathbb{Z}$, nämlich Folgen, die wir als „Potenzreihen“ in p schreiben: Für Zahlen $a_i \in \mathbb{Z}, i = 0, 1, 2, \ldots$ ist die Folge der Zahlen

$$x_n := \sum_{i=0}^{n} a_i p^i \in \mathbb{Z}$$

eine p-adische Cauchy-Folge. Denn: Für $m \geq n$ gilt

$$|x_m - x_n|_p = |\sum_{i=n+1}^{m} a_i p^i|_p = p^{-n}|\sum_{i=n+1}^{m} a_i p^{i-n}|_p \leq p^{-n}.$$

Also hat jede solche Folge einen Grenzwert $\sum_{i=0}^{\infty} \in \mathbb{Z}_p$. Da diese Folgen einen Ring bilden und der Grenzwert einen Ringhomomorphismus nach $\mathbb{Z}_p$ vermittelt, sind die genannten Grenzwerte ein Teilring von $\mathbb{Z}_p$. Dieser Ring enthält $\mathbb{Z}$ und ist vollständig, also ist dieser Ring genau $\mathbb{Z}_p$

Die Wahl der a_i kann man nachträglich noch einschränken. Es sei nämlich sukzessive $b_i \in \{0, 1, \ldots, p-1\}$ so gewählt, dass

$$p^n \mid \sum_{i=0}^{n} (a_i - b_i) p^i.$$

Dann gilt offensichtlich

$$\lim_n x_n = \sum_{i=0}^{\infty} b_i p^i.$$

Wir können also $\mathbb{Z}_p$ ähnlich wie die reellen Zahlen entwickeln, nur dass dort die Grundzahl für die Potenzreihe eben landläufiger Weise $\frac{1}{10}$ ist.

Die Einheitengruppe in $\mathbb{Z}_p$ ist die Menge

$$\mathbb{Z}_p^\times = \{x \in \mathbb{Z}_p \mid |x|_p = 1\} = \mathbb{Z}_p \smallsetminus p\mathbb{Z}_p.$$

Da jedes Element aus $\mathbb{Z}_p \smallsetminus \{0\}$ zu einer Potenz von p assoziiert ist, ist jedes Ideal in $\mathbb{Z}_p$ ein Hauptideal. Genauer: Wenn $I \subseteq \mathbb{Z}_p$ ein von $\{0\}$ verschiedenes Ideal ist, dann sei

$$v := \min\{\mathrm{v}_p(x) \mid 0 \neq x \in I\}.$$

Dann ist p^v ein Erzeuger von I.

Der obigen Schreibweise der Elemente von $\mathbb{Z}_p$ als Potenzreihen in p entnimmt man, dass der Restklassenring $\mathbb{Z}_p/p^v\mathbb{Z}_p$ durch die ganzen Zahlen $0, 1, \ldots, p^v - 1$ repräsentiert wird, dass also auch gilt:

$$\mathbb{Z}_p/p^v\mathbb{Z}_p \cong \mathbb{Z}/p^v\mathbb{Z}.$$

Der Ring der ganzen p-adischen Zahlen ist intim verknüpft mit den Restklassenringen $\mathbb{Z}/p^v\mathbb{Z}$. Das ist der Gegenstand des folgenden Lemmas, das die Arithmetik in $\mathbb{Z}_p$ diktiert:

Hilfssatz 4.4.14 Lemma von Hensel[6]

Es seien $f \in \mathbb{Z}_p[X]$ ein Polynom, und $a \in \mathbb{Z}_p$ ein Element, sodass $f(a) \in p\mathbb{Z}_p$ und $f'(a) \notin p\mathbb{Z}_p$.

Dann gibt es ein $\tilde{a} \in \mathbb{Z}_p$ mit $p \mid a - \tilde{a}$ und $f(\tilde{a}) = 0$.

Beweis. Wir setzen $a_1 := a$ und konstruieren davon ausgehend eine Cauchy-Folge in $\mathbb{Z}_p$, die gegen eine Nullstelle von f konvergiert.

Im ersten Schritt suchen wir ein $a_2 \in a_1 + p\mathbb{Z}_p$ mit $p^2 \mid f(a_2)$. Dazu machen wir den Ansatz

$$a_2 = a_1 + pt,\ t \in \mathbb{Z}_p$$

und evaluieren das Polynom f an der Stelle a_2. Die Binomischen Formeln, angewandt auf die Summanden von f, sagen dann

$$f(a_1 + pt) = f(a_1) + f'(a_1)pt + p^2 \cdot \mathrm{Rest},$$

[6] Kurt Hensel, 1861 - 1941

wobei der Rest auch in $\mathbb{Z}_p$ liegt. Damit das durch p^2 teilbar ist, muss also nur die Summe $f(a_1) + f'(a_1)pt$ durch p^2 teilbar sein. Nun ist aber $f(a_1) = ps$ für ein $s \in \mathbb{Z}_p$. Wir müssen also dafür sorgen, dass

$$t = -s/f'(a_1)$$

gilt, was lösbar ist, da $f'(a_1)$ in $\mathbb{Z}_p$ eine Einheit ist.

Damit finden wir

$$a_2 = a_1 - \frac{ps}{f'(a_1)} = a_1 - \frac{f(a_1)}{f'(a_1)}.$$

Wenn sukzessive a_k konstruiert ist mit $p^k \mid f(a_k)$ und $p \mid (a_1 - a_k)$, dann ist immer noch $f'(a_k) \in \mathbb{Z}_p^\times$, denn modulo p ist es zu $f'(a_{k-1})$ kongruent. Wir können also weitermachen wie im ersten Schritt.

$$a_{k+1} := a_k - \frac{f(a_k)}{f'(a_k)}$$

liefert einen Wert mit

$$f(a_{k+1}) = f(a_k - \frac{f(a_k)}{f'(a_k)}) = f(a_k) - f'(a_k)f(a_k)/f'(a_k) + (\frac{f(a_k)}{f'(a_k)})^2 \cdot \text{Rest},$$

wobei der Rest in $\mathbb{Z}_p$ liegt und daher p^{k+1} sicher ein Teiler von $f(a_{k+1})$ ist.

Die so konstruierte Folge ist offensichtlich eine Cauchy-Folge, und die Stetigkeit der durch f gegebenen Abbildung (siehe 4.4.3) zwingt den Grenzwert

$$\tilde{a} := \lim_{k \to \infty} a_k$$

dazu, eine Nullstelle von f zu sein. ◯

Bemerkung 4.4.15 Newtonverfahren[7]

a) Am Beweis sieht man insbesondere, dass unter den Bedingungen des Lemmas von Hensel das Newton-Verfahren funktioniert, und zwar viel besser als man sich das in der reellen Analysis jemals träumen lassen darf.

Wenn f rationale Koeffizienten hat und $a \in \mathbb{Q}$ gewählt wird, kann es passieren, dass das Newton-Verfahren sowohl reell als auch p-adisch konvergiert. Die Cauchy-Folgen sind dieselben, denn diese sehen nur das rationale Polynom und den rationalen Startwert und brauchen den drumherumliegenden vollständigen Körper gar nicht für ihre Definition.

Bei anderer Wahl des Startwerts kann es jedoch passieren, dass zum Beispiel die neue Folge gegen dieselbe p-adische Nullstelle läuft, aber gegen eine andere

[7]Isaac Newton, 1643-1727

reelle. Es gibt also keine natürliche Entsprechung zwischen reellen und p-adischen Nullstellen, zumal die eine oder andere vielleicht gar nicht existiert.

b) Die Voraussetzungen lassen sich noch etwas abschwächen. Was man eigentlich braucht ist, dass

$$\mathrm{v}_p(f(a)) > 2\mathrm{v}_p(f'(a))$$

gilt. Im Fall unserer Version des Hensel-Lemmas ist $\mathrm{v}_p(f'(a)) = 0$.

Beispiel 4.4.16 Quadrate

a) Es sei p eine ungerade Primzahl und $b \in \mathbb{Z}_p^\times$ derart, dass die Restklasse von b in $\mathbb{F}_p^\times$ ein Quadrat ist. Das heißt:

$$\exists a \in \mathbb{Z}_p : a^2 - b \in p\mathbb{Z}_p.$$

Wir benutzen das Polynom $f(X) = X^2 - b$. Modulo p ist a eine Nullstelle von f, und $f'(a) = 2a$ ist immer noch eine Einheit in $\mathbb{Z}_p$, da $p \neq 2$.

Also gibt es ein $\tilde{a} \in a + p\mathbb{Z}_p$ mit $\tilde{a}^2 = b$.

Konkreter sei $p = 5$ und $b = -1$. Eine Nullstelle von $X^2 + 1$ modulo 5 ist zum Beispiel $a_1 = 2$ mit $f'(a_1) = 4$.

Dann ist im Beweis des Lemmas von Hensel

$$\begin{aligned}
a_2 &= a_1 - \tfrac{f(a_1)}{f'(a_1)} = 2 - \tfrac{5}{4} = \tfrac{3}{4},\\
a_3 &= a_2 - \tfrac{f(a_2)}{f'(a_2)} = \tfrac{3}{4} - \tfrac{\frac{9}{16}+1}{2\frac{3}{4}} = \tfrac{3}{4} - \tfrac{25}{24} = \tfrac{-7}{24}.\\
a_4 &= \cdots = \tfrac{527}{336},\\
a_5 &= \tfrac{164833}{354144},\\
a_6 &= \tfrac{-98248054847}{116749235904}
\end{aligned}$$

und so weiter.

Hier kann man etwa testen, dass

$$a_6^2 + 1 = \frac{152587890625}{125417972736} = 5^{16} \cdot \frac{1}{125417972736},$$

also ist $|a_6^2 + 1|_5 = 5^{-16}$, und a_6 liegt in $\mathbb{Z}_5$ tatsächlich äußerst nah an einer Quadratwurzel aus -1.

b) Jetzt machen wir das für $p = 2$ und suchen zum Beispiel eine Quadratwurzel aus 17. Das zu verwendende Polynom ist $X^2 - 17$, wir nehmen $a_1 = 1$ und finden

$f(a_1) = -16, f'(a_1) = 2.$

$$\begin{aligned} a_2 &= a_1 - f(a_1)/f'(a_1) = 1 - (-8) = 9, \\ a_3 &= a_2 - f(a_2)/f'(a_2) = 9 - 64/18 = 49/9, \\ a_4 &= 1889/441, \\ a_5 &= 3437249/833049, \\ a_6 &= 11806090753409/2863396842201, \end{aligned}$$

und so weiter. Tatsächlich ist zum Beispiel

$$a_6^2 + 17 = \frac{737869762948382064 64}{819904147592665849452440 1} = 2^{66}\frac{1}{819904147592665849452440 1},$$

und wir sind in $\mathbb{Z}_2$ schon sehr nah an einer Quadratwurzel aus 17 dran.

Hier haben wir das Phänomen aus 4.4.15a) vorliegen. Tatsächlich ist auch reell a_6 schon sehr nah an einer Quadratwurzel aus 17:

$$a_6^2 = 17.00000899946371920246652520\ldots$$

Wenn wir aber den Startwert durch $a_1 = -7$ ersetzen, dann bekommen wir dieselbe 2-adische Nullstelle als Limes im Newtonverfahren, während reell die Folgenglieder alle negativ sind, also gegen die andere Wurzel von 17 konvergieren.

Bemerkung 4.4.17 Bedeutung

Die p-adischen Zahlen sind in der modernen Zahlentheorie von großer Bedeutung, was in dieser Vorlesung noch nicht so recht vermittelt werden kann.

Erst in der algebraischen Zahlentheorie oder in der arithmetischen Geometrie wird klarer, was durch sie gewonnen wird. Für den Ring $\mathbb{Z}$ sollte man $\mathbb{Z}_p$ tatsächlich als eine Art universelles Instrument zur Behandlung von Kongruenzen modulo p-Potenzen verstehen. Die endlichen Ringe $\mathbb{Z}/p^e\mathbb{Z}$ werden auf einen Schlag durch einen nullteilerfreien Ring ersetzt, der $\mathbb{Z}$ enthält, das ist für manche Untersuchungen nicht zu unterschätzen. Und man hat eine interessante Topologie, sodass sich sogar analytische Argumente als Hilfsmittel anbieten.

Der Mathematik wird ein Stück Einheit zurückgegeben, das durch die oft künstliche und starre Unterteilung in disjunkte Disziplinen verloren zu gehen droht.

INDEX

INDEX