Anhang A: Konstruktive Mathematik

Die Existenz eines Objektes wird erst durch seine Konstruktion begründet.

Ausblick

In der konstruktiven Mathematik wird die Existenz eines Objektes erst dadurch bewiesen, dass eine Konstruktion desselben angegeben wird. Im Gegensatz dazu ist es in klassischer Logik erlaubt, die Existenz eines Objektes dadurch nachzuweisen, dass man seine Nichtexistenz annimmt und dies zu einem Widerspruch führt.

Ein konstruktiver Existenzbeweis enthält einen Algorithmus, um das Objekt, dessen Existenz behauptet wird, zu berechnen. Ist dagegen nur ein klassischer Beweis etwa einer Aussage der Form „Das Polynom $f(X)$ hat eine reelle Nullstelle x." gegeben, so wissen wir noch lange nicht, wie wir eine solche Nullstelle x finden können.

Jeder konstruktive Beweis ist insbesondere ein klassischer Beweis, jedoch nicht umgekehrt. Gelingt es uns also, einen Satz konstruktiv zu beweisen, so ist er nicht nur klassisch richtig, sondern wir können auch sicher sein, dass er auch einen algorithmischen Inhalt hat.

Klassische Beweise werden im Rahmen der klassischen Logik geführt. Diese dürfen wir für konstruktive Beweise nicht uneingeschränkt verwenden, weil das klassische Gesetz vom ausgeschlossenen Dritten gerade nicht konstruktiv ist. Das ist aber auch die einzige Einschränkung. Ohne das Gesetz vom ausgeschlossenen Dritten wird die klassische Logik zur intuitionistischen, mit deren Hilfe wir in der konstruktiven Mathematik Beweise führen können.

Der klassische Fundamentalsatz der Algebra lautet, dass jedes nichtkonstante Polynom über den komplexen Zahlen eine komplexe Nullstelle hat. In diesem Buch haben wir diese Aussage konstruktiv für solche Polynome gezeigt, deren Koeffizienten algebraische Zahlen sind. Und in der Tat ist die klassische Aussage konstruktiv falsch. Wir skizzieren in diesem Anhang, dass es keinen konstruktiven Beweis für die Existenz von Nullstellen beliebiger nichtkonstanter Polynome mit komplexen Koeffizienten geben kann.

M. Nieper-Wißkirchen, *Elementare Galois-Theorie,*
https://doi.org/10.1007/978-3-662-60934-7

A.1 Das Gesetz vom ausgeschlossenen Dritten

Ist der klassischen Logik besagt das Gesetz vom ausgeschlossenen Dritten, dass für jede Aussage φ die Aussage $\varphi \vee \neg\varphi$, also die Aussage „φ oder nicht φ“, beweisbar ist.

Konstruktiv ist der Inhalt dieses Gesetzes allerdings leer. Betrachten wir etwa ein verdecktes Kartenspiel. Sei φ die Aussage, dass die oberste verdeckte Karte ein Ass ist. Wir können uns dann fragen, ob die oberste Karte ein Ass ist oder nicht, ob also $\varphi \vee \neg\varphi$. Nach dem Gesetz des ausgeschlossenen Dritten ist diese Aussage wahr. Aus praktischer Sicht ist damit aber nicht viel gewonnen, denn wir können daraus weder folgern, dass die oberste Karte ein Ass ist noch dass die oberste Karte kein Ass ist.

Das Gesetz vom ausgeschlossenen Dritten ist auch die Grundlage des Beweisprinzips durch Widerspruch: Um eine Aussage φ zu beweisen, nehmen wir ihr Gegenteil $\neg\varphi$ an. Dann versuchen wir, dies zu einem Widerspruch zu führen. Gelingt uns das, kann $\neg\varphi$ nicht wahr sein. Aufgrund von $\neg\varphi \vee \varphi$ muss damit aber φ wahr sein.

Der Unterschied zwischen klassischer und konstruktiver Mathematik lässt sich an folgendem Beispiel besonders gut illustrieren. Wir betrachten folgende Aussage:

Es gibt zwei positive irrationale Zahlen a und b, sodass a^b rational ist.

Klassisch gibt es einen kurzen Beweis mithilfe des Gesetzes vom ausgeschlossenen Dritten. Und zwar betrachten wir die Zahl $\sqrt{2}^{\sqrt{2}}$. Ist diese Zahl rational, so haben wir obige Aussage bewiesen, denn dann können wir $a = b = \sqrt{2}$ setzen, denn $\sqrt{2}$ ist bekanntlich irrational.

Ansonsten ist (nach dem Gesetz des ausgeschlossenen Dritten!) die Zahl $\sqrt{2}^{\sqrt{2}}$ irrational; wir können dann $a = \sqrt{2}^{\sqrt{2}}$ und $b = \sqrt{2}$ setzen, denn dann ist

$$a^b = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = \sqrt{2}^{\sqrt{2}\cdot\sqrt{2}} = \sqrt{2}^2 = 2$$

eine rationale Zahl.

Vom Standpunkt der konstruktiven Mathematik liegt hier allerdings kein Beweis vor; schließlich erlaubt uns dieser Beweis nicht, ein Paar a, b positiver irrationaler Zahlen anzugeben, sodass a^b irrational ist.

(Nach einem Beweis von Rodion Kuzmin[1] ist die *gelfond*[2]*–schneidersche*[3] *Konstante* $2^{\sqrt{2}}$ transzendent, insbesondere also irrational, weswegen $a = 2^{\sqrt{2}}$ und $b = \sqrt{2}$ eine korrekte Wahl ist.)

A.2 Intuitionistische Logik

Die Junktoren der Logik, d. h. die logischen Verknüpfungen, erlauben uns, Aussagen zu weiteren Aussagen zu kombinieren. Seien etwa φ und ψ Aussagen. Diese können wir zu einer *Konjunktion* $\varphi \wedge \psi$, zu einer *Disjunktion* $\varphi \vee \psi$ und zu einer *Implikation* $\varphi \implies \psi$ verknüpfen.

Ist x eine (Term-)Variable, die in der Aussage $\varphi(x)$ frei vorkommt, so können wir weiter die *Allquantifizierung* $\forall x : \varphi(x)$ und die *Existenzquantifizierung* $\exists x : \varphi(x)$ bilden.

Schließlich gibt es noch das *Falsum* $\bot$.

Weitere Aussagen können wir durch mehrfache Anwendung dieser Junktoren gewinnen. So ist die *Negation* $\neg\varphi$ als $\varphi \implies \bot$ definiert, das *Verum* $\top$ als $\bot \implies \bot$ und die *Äquivalenz* $\varphi \Leftrightarrow \psi$ als $(\varphi \implies \psi) \wedge (\psi \implies \varphi)$.

Die Regeln der Logik besagen, was ein Beweis von durch Junktoren gebildete Aussagen ist. Beginnen wir mit der *intuitionistischen Logik*:

Ein Beweis einer Konjunktion $\varphi \wedge \psi$ ist die Angabe eines Beweises von φ und eines Beweises von ψ.

Ein Beweis einer Disjunktion $\varphi \vee \psi$ ist Angabe eines Beweises von φ oder die Angabe eines Beweises von ψ und insbesondere die Angabe, welcher Fall eintritt.

Ein Beweis einer Implikation $\varphi \implies \psi$ ist die Angabe eines Beweises von ψ, wenn immer ein Beweis von φ gegeben ist.

Ein Beweis einer Allquantifizierung $\forall x : \varphi(x)$ ist die Angabe eines Beweises von $\varphi(t)$ für jeden Term t.

Ein Beweis einer Existenzquantifizierung $\exists x : \varphi(x)$ ist die Angabe eines Termes t und eines Beweises für die Aussage $\varphi(t)$.

Das Falsum besitzt keinen Beweis.

Die *klassische Logik* hat auch alle diese Beweisregeln; es kommt lediglich eine weitere Beweismöglichkeit hinzu:

Für jede Aussage φ gibt es einen Beweis von $\varphi \vee \neg\varphi$.

A.3 Der Fundamentalsatz der Algebra in der konstruktiven Mathematik

Klassisch besagt der Fundamentalsatz der Algebra Folgendes: Ist $f(X)$ ein nichtkonstantes Polynom mit komplexen Koeffizienten, so gibt es eine komplexe Zahl w mit $f(w) = 0$. Im ersten Kapitel dieses Buches haben wir den Fundamentalsatz konstruktiv für Polynome $f(X)$ mit algebraischen Koeffizienten bewiesen; die Nullstelle w ist dann automatisch eine algebraische Zahl.

In diesem Abschnitt wollen wir ein Argument dafür skizzieren, warum der allgemeinere Fundamentalsatz für beliebige nichtkonstante Polynome über den komplexen Zahlen konstruktiv nicht beweisbar ist, warum es also insbesondere keinen Algorithmus geben kann, der für jedes nichtkonstante komplexe Polynom $f(X)$ eine komplexe Zahl w mit $f(w) = 0$ berechnet.

Wir benötigen für dieses Argument einige wenige Begriffe aus der Analysis: Sei Y ein topologischer Raum (für unser Argument können wir $Y = \mathbf{C}$ annehmen). Wir wollen eine Interpretation der Sprache der Logik *über* Y entwickeln. Um eine Verwechslungsgefahr mit der üblichen Interpretation zu verhindern, verwenden wir das Adjektiv *lokal,* wenn wir über die Interpretation über Y sprechen.

Fangen wir mit dem Begriff eines Termes bzw. eines lokalen Termes an. Sei U eine offene Teilmenge von Y. Dann ist ein *(lokaler) Term t* über U einfach eine (termwertige) Funktion mit Definitionsbereich U. Ist $V \subseteq U$ eine offene Teilmenge, so bezeichnen wir mit $t|V$ die Einschränkung von t auf V.

Als Nächstes betrachten wir *lokale Aussagen*. Auch diese sind jeweils über offenen Mengen U von Y definiert und machen jeweils Aussagen über lokale Terme über U. Ist $V \subseteq U$ eine offene Teilmenge von U, so können wir jede lokale Aussage φ über U zu einer lokalen Aussage $\varphi|V$ über V einschränken.

Wir machen weiter folgende Lokalitätsannahme: Ist $(U_i)_{i\in I}$ eine offene Überdeckung von U, so ist eine lokale Aussage φ über U genau dann wahr, wenn für alle $i \in I$ die lokale Aussage $\varphi|U_i$ über U_i wahr ist.

Die logischen Junktoren und Quantoren müssen wir dann folgendermaßen interpretieren: Seien φ und ψ lokale Aussagen über der offenen Menge U. Dann ist $\varphi \wedge \psi$ die Aussage, dass sowohl φ als auch ψ über U wahr ist. Weiter ist $\varphi \vee \psi$ die Aussage, dass eine offene Überdeckung $(U_i)_{i\in I}$ von U existiert, sodass für alle $i \in I$ die Aussage $\varphi|U_i$ oder die Aussage $\psi|U_i$ über $i \in I$ wahr ist. Die Aussage $\varphi \implies \psi$ ist wahr, wenn für jede offene Teilmenge $V \subseteq U$ von U, für die $\varphi|V$ wahr ist, auch $\psi|V$ über V wahr ist.

Weiter ist $\forall x\colon \varphi(x)$ die Aussage, dass für alle offenen Teilmengen $V \subseteq U$ und alle Terme t über V die Aussage $(\varphi|V)(t)$ gilt. Die Aussage $\exists x\colon \varphi(x)$ ist wahr, wenn eine offene Teilmenge $(U_i)_{i\in I}$ von U und für jedes $i \in I$ ein Term t_i über U_i existieren, sodass $(\varphi|U_i)(t_i)$ wahr ist.

Schließlich ist $\bot$ nur über der leeren offenen Menge $\emptyset$ wahr.

Es zeigt sich nun, dass die intuitionistische Logik eine Interpretation in den so definierten lokalen Aussagen über Y hat. Existiert also eine Ableitung einer lokalen Aussage φ über U nach den Regeln der intuitionistischen Logik, so ist φ über U wahr.

Ersetzen wir intuitionistische Logik durch klassische Logik, so gilt dies nicht mehr: Sei etwa $Y = \mathbf{R}$, und sei φ die lokale Aussage, dass die (identische) Funktion x keine Nullstelle besitzt. Nach klassischer Logik würde $\varphi \vee \neg\varphi$ gelten, das heißt, es gibt offene Mengen U und V von $\mathbf{R}$, sodass $\varphi|U$ und $\neg\varphi|V$ gelten. Die Aussage $\neg\varphi|V$ ist äquivalent zu $\varphi|V \implies \bot$ und bedeutet damit, dass für jede offene Teilmenge $W \subseteq V$, für die $\varphi|W$ gilt, auch das Falsum gilt, das heißt, φ darf nur auf $\emptyset$ gelten, das heißt, $\neg\varphi|V$ ist wahr, wenn die Nullstellen von x in V dicht liegen. Dies ist aber nur für $V = \emptyset$ möglich. Damit muss $U = Y = \mathbf{R}$ gelten. Damit gilt aber φ auf $\mathbf{R}$, das heißt, x hat auf $\mathbf{R}$ keine Nullstelle, ein Widerspruch.

Definieren wir eine *lokale natürliche Zahl* über einer offenen Menge U als eine lokal konstante Funktion $f\colon U \to \mathbf{N}_0$, definieren wir als ihren *Nachfolger* die Funktion $f + 1\colon U \to \mathbf{N}_0$ und als *lokale Null* die konstante Nullfunktion $0\colon U \to \mathbf{N}_0$, so übertragen sich die Eigenschaften der üblichen natürlichen Zahlen mutatis mutandis auf die lokalen natürlichen Zahlen über offenen Mengen von Y.

Mutatis mutandis übertragen sich außerdem die Konstruktionen der ganzen und dann der rationalen Zahlen aus den natürlichen Zahlen. Wir können also von *lokalen ganzen Zahlen*

und *lokalen rationalen Zahlen* sprechen. Es folgt, dass eine lokale ganze bzw. rationale Zahl dabei eine lokal konstante Funktion über einer offenen Menge nach $\mathbf{Z}$ bzw. $\mathbf{Q}$ ist.

Eine *lokale reelle Zahl* x über U ist dann ein Objekt, welches sich durch lokale rationale Zahlen beliebig genau approximieren lässt, das heißt, für jedes $\epsilon > 0$ existiert eine rationale Zahl r, sodass x von r um weniger als ϵ abweicht. (Hierbei ist die Existenz von r wieder lokal zu interpretieren, das heißt, es existieren eine offene Überdeckung $(U_i)_{i\in I}$ und rationale Zahlen r_i über U_i, sodass für alle $i \in I$ jeweils $x|U_i$ um weniger als ϵ von r_i abweicht.

Eine lokale komplexe Zahl ist wiederum ein Ausdruck der Form $a + b \cdot \mathrm{i}$, wobei a und b lokale reelle Zahlen sind.

Nach Definition der Stetigkeit zeigt sich, dass jede stetige reellwertige Funktion $U \to \mathbf{R}$ eine lokale reelle Zahl über U definiert und dass umgekehrt jede lokale reelle Zahl über U eine stetige Funktion $U \to \mathbf{R}$ definiert. Analog können wir lokale komplexe Zahlen mit stetigen Funktionen $U \to \mathbf{C}$ gleichsetzen.

Nehmen wir jetzt an, wir hätten einen konstruktiven Beweis für den Fundamentalsatz der Algebra für beliebige nichtkonstante Polynome mit komplexen Koeffizienten. Da sich jeder konstruktive Beweis auch lokal über Y interpretieren lässt, hätten wir damit einen Beweis der folgenden Aussage:

> Sei $f(X)$ ein nichtkonstantes Polynom, dessen Koeffizienten stetige komplex-wertige Funktionen über einem topologischen Raum Y sind. Dann existiert eine stetige komplexwertige Funktion w, so dass $f(w)$ die Nullfunktion ist.

Dass diese Aussage nicht stimmen kann, sehen wir an folgendem Beispiel: Wir wählen als topologischen Raum die komplexe Zahlenebene $Y = \mathbf{C}$. Mit $z\colon \mathbf{C} \to \mathbf{C}$ bezeichnen wir die identische Funktion. Dann ist $X^2 - z$ ein nichtkonstantes Polynom, das heißt, nach obiger Aussage gäbe es eine stetige Funktion $w\colon \mathbf{C} \to \mathbf{C}$ mit $w^2 = z$, also eine global auf $\mathbf{C}$ definierte stetige Quadratwurzel. Aus der Funktionentheorie ist aber bekannt, dass das nicht sein kann.

(Ein kurzes Argument dafür ist das folgende: Nach dem Satz über implizit definierte Funktionen wäre w außerhalb des Ursprunges holomorph, nach dem riemannschen[4] Hebbarkeitssatz dann auch auf ganz $\mathbf{C}$, da w am Ursprung stetig ist. Differenzieren von $w^2 = z$ nach z liefert $2\,w\,w' = 1$. Am Ursprung $z = 0$ erhalten wir dann wegen $w(0) = 0$ (da 0 die einzige Quadratwurzel von 0 ist) den Widerspruch $0 = 1$).

Damit ist der Fundamentalsatzes der Algebra für nichtkonstante Polynome, deren Koeffizienten stetige komplexwertige Funktionen sind, falsch. Damit kann es auch keinen konstruktiven Beweis für den Fundamentalsatz für nichtkonstante Polynome mit komplexwertigen Koeffizienten geben.

Das allgemeine Motto, welches wir hier ausgenutzt haben, lautet: Ist eine Aussage konstruktiv wahr, so bleibt sie wahr, wenn die Objekte stetig in Familien variieren. Diese Eigenschaft ist im Wesentlichen auch der Grund, warum konstruktive Schlussweisen auch in der klassischen Mathematik von großem Interesse sind.

Anhang B: Lineare Algebra

Es gibt wenig Mathematik, die ohne lineare Algebra auskommt.

Ausblick
Die galoissche Theorie kommt nicht ganz ohne lineare Algebra aus, ein weiterer wichtiger Teilbereich der Algebra. Im Haupttext dieses Buches ist dies dadurch deutlich geworden, dass wir in Beweisen zum Beispiel die Matrizennotation verwendet haben und etwa über Determinanten gesprochen haben.

Um dieses Buch aber auch für Leser, die über das Lösen linearer Gleichungssysteme hinaus keine Vorkenntnisse in der linearen Algebra haben, vollständig zugänglich zu machen, stellen wir in diesem Anhang die benötigten Begriffe zusammen.

Außerdem gehen wir auf die Sätze aus der linearen Algebra ein, die wir im Hauptteil verwendet haben. Das sind die cramersche Regel für die Lösungen eines linearen Gleichungssystems und die Formel über die vandermondesche Determinante.

B.1 Matrizen

Definition B.1 Seien n und m zwei natürliche Zahlen. Eine $(n \times m)$-*Matrix* A ist ein rechteckiges Schema mit n Zeilen und m Spalten, in dem insgesamt $n \cdot m$ Zahlen a_{ij}, $1 \leq i \leq n$, $1 \leq j \leq m$ angeordnet sind:

$$A = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \dots & a_{nn} \end{pmatrix}.$$

M. Nieper-Wißkirchen, *Elementare Galois-Theorie,*
https://doi.org/10.1007/978-3-662-60934-7

Je nachdem aus welchem Rechenbereich die Zahlen a_{ij} stammen, sprechen wir von *ganzzahligen, rationalen, reellen* oder *komplexen* Matrizen. Wir können aber auch Matrizen mit noch allgemeineren Einträgen bilden, etwa Matrizen, deren Einträge Polynome sind.

Beispiel B.1 Die $(n \times n)$-*Einheitsmatrix* ist die Matrix, die auf der Diagnonalen 1 und überall sonst 0 stehen hat:

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

Beispiel B.2 Sei $A = (a_{ij})$ eine $(n \times n)$-Matrix. Dann heißt die $(n \times n)$-Matrix

$$X \cdot I - A = \begin{pmatrix} X - a_{11} & -a_{12} & \dots & \dots & -a_{1n} \\ -a_{21} & X - a_{22} & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & X - a_{n-1,n-1} & -a_{n-1,n} \\ -a_{n1} & \dots & \dots & -a_{n,n-1} & X - a_{nn} \end{pmatrix}$$

die *charakteristische Matrix* von A. Die charakteristische Matrix ist eine Matrix von Polynomen in der Unbestimmten X.

B.2 Determinanten

Definition B.2 Sei $A = (a_{ij})$ eine $(n \times n)$-Matrix. Dann heißt die Zahl

$$0 = \sum_{\sigma \in S_n} \operatorname{sgn} \sigma \cdot \prod_{i=1}^{n} a_{i\sigma(i)} = a_{11}a_{22}a_{33} \cdots a_{nn} - a_{12}a_{21}a_{33} \cdots a_{nn} + \cdots$$

die *Determinante* von A. Dabei läuft die Summe über alle $n!$ Permutationen σ von $\{1, \dots, n\}$.

Die Determinante von A ist also eine Summe von $n!$ Termen. Jeder Term ist bis auf sein Vorzeichen ein n-faches Produkt von je einem Matrixeintrag aus jeder Zeile und Spalte.

Die Vorzeichen sind genau so gewählt, dass die Determinante ihr Vorzeichen wechselt, wenn zwei Zeilen oder wenn zwei Spalten vertauscht werden. Mehr noch, die Determinante verschwindet, wenn zwei Zeilen oder zwei Spalten identisch sind.

Weiter ist die Determinante linear sowohl in ihren Zeilen als auch in ihren Spalten. Insbesondere verschwindet die Determinante einer Matrix, die eine Zeile oder eine Spalte

aus Nullen besitzt. Außerdem ändert sich die Determinante nicht, wenn ein Vielfaches einer Zeile bzw. Spalte auf eine andere Zeile bzw. Spalte addiert wird.

Ist also eine Zeile bzw. Spalte einer Matrix eine Linearkombination (also eine Summe von Vielfachen) der anderen Zeilen bzw. Spalten, so verschwindet die Determinante dieser Matrix.

Proposition B.1 *Sei n eine natürliche Zahl. Seien weiter x_1, x_2, ..., x_n beliebige Zahlen. Dann ist die* vandermondesche Determinante *durch*

$$\det \begin{pmatrix} 1 & \dots & 1 \\ x_1 & \dots & x_n \\ x_1^2 & \dots & x_n^2 \\ \vdots & & \vdots \\ x_1^{n-1} & \dots & x_n^{n-1} \end{pmatrix} = \prod_{1 \le i < j \le n} (x_j - x_i)$$

gegeben.

Beweis Es reicht, folgende Polynomgleichheit in den Unbestimmten $X_1, \dots, X_n$ zu zeigen:

$$\det \begin{pmatrix} 1 & \dots & 1 \\ X_1 & \dots & X_n \\ X_1^2 & \dots & X_n^2 \\ \vdots & & \vdots \\ X_1^{n-1} & \dots & X_n^{n-1} \end{pmatrix} = \prod_{1 \le i < j \le n} (X_j - X_i)$$

Dies machen wir per Induktion über n. Im Falle von $n = 0$ ist die linke Seite die Determinante der (0×0)-Matrix, also 1. Weiter ist in diesem Falle die rechte Seite das leere Produkt, also ebenfalls 1.

Für den Induktionsschluss auf n nehmen wir an, dass wir die Behauptung für $n - 1$ schon gezeigt haben.

Nach der Definition der Determinanten können wir die linke Seite der behaupteten Gleichheit für n als ein Polynom vom Grad $n - 1$ in X_n auffassen. Die rechte Seite ist ebenfalls ein Polynom vom Grad $n - 1$ in X_n. Die Koeffizienten dieser Polynome in X_n lassen sich wiederum als rationale Funktionen in den Unbestimmten $X_1, \dots, X_{n-1}$ auffassen.

Wir müssen zeigen, dass die beiden Seiten als Polynome in X_n übereinstimmen. Dazu reicht es zu zeigen, dass sie die gleichen $n - 1$ Nullstellen haben und den gleichen führenden Term besitzen.

Die linke Seite verschwindet, wenn wir $X_1, \dots, X_{n-1}$ für X_n einsetzen, denn die Determinante einer Matrix mit zwei gleichen Spalten verschwindet. Die rechte Seite verschwindet offensichtlich ebenfalls, wenn $X_1, \dots, X_{n-1}$ für X_n eingesetzt wird.

Damit haben wir die jeweils $n-1$ Nullstellen beider Seiten gefunden, und sie stimmen überein. Es bleibt die Berechnung des führenden Koeffizienten in X_n auf beiden Seiten. Auf der linken Seite ist dieser aber nach Definition der Determinanten gerade

$$\det \begin{pmatrix} 1 & \dots & 1 \\ X_1 & \dots & X_{n-1} \\ X_1^2 & \dots & X_{n-1}^2 \\ \vdots & & \vdots \\ X_1^{n-2} & \dots & X_{n-1}^{n-2} \end{pmatrix}$$

und auf der rechten Seite

$$\prod_{1 \le i < j \le n-1} (X_j - X_i).$$

Nach Induktionsvoraussetzung stimmen diese überein.

B.3 Die cramersche Regel

Die folgende Aussage ist unter dem Namen *cramersche Regel* bekannt.

Proposition B.2 *Sei das lineare Gleichungssystem*

$$\begin{aligned} b_1 &= a_{11}\, x_1 + a_{12}\, x_2 + a_{13}\, x_3 + \cdots + a_{1n}\, x_n, \\ b_2 &= a_{21}\, x_1 + a_{22}\, x_2 + a_{23}\, x_3 + \cdots + a_{2n}\, x_n, \\ &\vdots \\ b_n &= a_{n1}\, x_1 + a_{n2}\, x_2 + a_{n3}\, x_3 + \cdots + a_{nn}\, x_n \end{aligned} \tag{B.1}$$

in x_1, ..., x_n gegeben.

Wir definieren die Matrix

$$A := \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix}$$

und für alle $1 \le j \le n$ die Matrix

$$A_j := \begin{pmatrix} a_{11} & \dots & a_{1,j-1} & b_1 & a_{1,j+1} & \dots & a_{1n} \\ a_{21} & \dots & a_{2,j-1} & b_2 & a_{2,j+1} & \dots & a_{2n} \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{n1} & \dots & a_{n,j-1} & b_n & a_{n,j+1} & \dots & a_{nn} \end{pmatrix}.$$

Ist dann $\det A \neq 0$*, so besitzt Gl.* (B.1) *genau eine Lösung, und zwar gilt*

$$x_j = \frac{\det A_j}{\det A}$$

für alle $1 \leq j \leq n$.

Beweis Wir fixieren ein $1 \leq j \leq n$. Nach Definition der Determinanten von A existieren Zahlen $c_1, \ldots, c_n$, sodass

$$\det A = c_1\, a_{1j} + c_2\, a_{2j} + \cdots + c_n\, a_{nj},$$

und diese Zahlen hängen nur von den Einträgen von A ab, die nicht in der j-ten Spalte stehen.

Wir kombinieren als Nächstes die Gleichungen von Gl. (B.1), indem wir das c_1-Fache der ersten, das c_2-Fache der zweiten usw. bis zum c_n-Fachen der n-ten Gleichung addieren. Wir erhalten

$$c_1\, b_1 + c_2\, b_2 + \cdots + c_n\, b_n = d_1\, x_1 + d_2\, x_2 + \cdots + d_n\, x_n, \tag{B.2}$$

wobei für die Vorfaktoren d_i:

$$d_i = c_1\, a_{1i} + c_2\, a_{2i} + \cdots + c_n\, a_{ni}$$

gilt.

Es folgt $d_j = \det A$. Weiter ist d_i für $i \neq j$ die Determinante der Matrix, die aus A entsteht, indem die j-Spalte durch die i-te Spalte ersetzt wird. Die Determinante einer solchen Matrix verschwindet aber, d. h. $d_i = 0$ für $i \neq j$.

Mit der gleichen Überlegung ist die linke Seite von Gl. (B.2) die Determinante der Matrix, die aus A entsteht, indem die Einträge der j-ten Spalte durch $b_1, b_2, \ldots, b_n$ ersetzt werden, also A_j.

Damit folgt aus Gl. (B.2), dass

$$\det A_j = \det A \cdot x_j.$$

Da nach Voraussetzung $\det A \neq 0$, sind die x_j damit wie behauptet im Falle der Existenz eindeutig bestimmt.

Es bleibt, die Existenz einer Lösung des linearen Gleichungssystems zu zeigen. Dazu überlegen wir uns zunächst, dass sich durch das Addieren von Vielfachen von Zeilen auf anderen Zeilen die Determinante der Koeffizientenmatrix nicht ändert, also insbesondere nicht verschwindet. Beim Vertauschen von Zeilen ändert sich höchstens das Vorzeichen.

Da die Determinante der Koeffizientenmatrix nicht verschwindet, können nicht alle Koeffizienten in der ersten Spalte verschwinden, ohne Einschränkung der Koeffizient a_{11}. Durch Addition von geeigneten Vielfachen der ersten Zeile auf die übrigen erhalten wir ein äqui-

valentes lineares Gleichungssystem mit $a_{21} = \cdots = a_{n1} = 0$, sodass die Determinante weiterhin nicht verschwindet.

Damit können aber nicht auch noch alle $a_{22}, \ldots, a_{n2}$ verschwinden, sodass wir wieder ohne Einschränkung annehmen können, dass $a_{22} \neq 0$. Wieder durch Addition von geeigneten Vielfachen, diesmal der zweiten Zeile auf die weiteren, erhalten wir ein äquivalentes Gleichungssystem, für das auch noch $a_{32} = \cdots = a_{n2} = 0$ gilt.

Führen wir dieses Verfahren fort, erhalten wir schließlich ein äquivalentes Gleichungssystem, für das die Diagonaleinträge $a_{11}, \ldots, a_{nn}$ nicht verschwinden und für das die Einträge unterhalb der Diagonalen a_{ij}, $i > j$ verschwinden. Ein solches lineares Gleichungssystem *in Dreiecksgestalt* hat aber eine offensichtliche Lösung.

Anhang C: Analysis

Die komplexen Zahlen sind ein Objekt der Analysis und nicht der Algebra. Der Fundamentalsatz der Algebra verdient seinen Namen daher eigentlich nicht.

Ausblick

In der galoisschen Theorie geht es um Ausdrücke der Form $\sqrt[3]{1-\sqrt{2}}$ und allgemeiner um Lösungen von Polynomgleichungen. Bevor Eigenschaften dieser Terme oder allgemeiner dieser Lösungen untersucht werden können, muss der erste Schritt aber darin bestehen, überhaupt sicherzustellen, dass es Zahlen gibt, die die Rolle von $\sqrt[3]{1-\sqrt{2}}$ spielen können, und dass es immer Lösungen von (nichttrivialen) Polynomgleichungen gibt.

In diesem Buch haben wir das Problem dahingehend gelöst, dass wir den Rechenbereich der rationalen Zahlen auf den der komplexen Zahlen erweitert und dann durch den Fundamentalsatz der Algebra gezeigt haben, dass jede nichttriviale Polynomgleichung (mit rationalen oder allgemeiner algebraischen Koeffizienten) eine Lösung in den komplexen Zahlen besitzt.

Die komplexen Zahlen sind ein Objekt der Analysis. Sie entstehen zwar durch algebraische Weise aus den reellen Zahlen, wie im Haupttext dieses Buches beschrieben, allerdings sind die reellen Zahlen über Grenzwertprozesse definiert. Damit ist klar, dass der Beweis des Fundamentalsatzes der Algebra einige Tatsachen aus der Analysis benötigt, die wir in diesem Kapitel von der Warte eines konstruktiven Mathematikers aus zusammengestellt haben.

Vom Standpunkt der reinen Algebra ist es vielleicht ein wenig unbefriedigend, dass wir die Analysis bemüht haben, um unsere galoissche Theorie aufzubauen. In der Tat ist es so, dass für die reine galoissche Theorie die Einführung der komplexen Zahlen nicht nötig gewesen wäre. Wie wir in Band 2 zeigen werden, gibt es eine rein algebraische Konstruktion des Körpers $\overline{\mathbf{Q}}$ der algebraischen Zahlen, in dem jede nichttriviale Polynomgleichung eine Lösung besitzt, der also algebraisch abgeschlossen ist.

M. Nieper-Wißkirchen, *Elementare Galois-Theorie,*
https://doi.org/10.1007/978-3-662-60934-7

Es gibt zwei Gründe, warum wir in diesem Buch diesen Weg nicht beschritten haben. Zum einen ist die algebraische Konstruktion vergleichsweise abstrakt, während die Konstruktion der komplexen Zahlen aus den schon bekannten reellen Zahlen relativ simpel ist. Zum anderen führen einige Anwendungen der galoisschen Theorie, wie etwa die numerische Berechnung von Nullstellen oder die diversen Konstruktionsprobleme mit Zirkel und Lineal, direkt auf die komplexen Zahlen.

C.1 Reelle Zahlen

Die Länge der Diagonalen eines Einheitsquadrates, also $\sqrt{2}$, lässt sich beliebig genau durch rationale Zahlen approximieren, ist aber selbst keine rationale Zahl (das haben wir im ersten Kapitel gesehen). Die reellen Zahlen $\mathbf{R}$ schließen solche Lücken in den rationalen Zahlen. Und zwar soll eine reelle Zahl ein Objekt sein, welches beliebig genau durch rationale Zahlen approximiert werden kann. Was damit genau gemeint ist, wird im Folgenden erläutert:

Ist x eine reelle Zahl und sind q und $\epsilon > 0$ rationale Zahlen, so soll zunächst

$$|x - q| < \epsilon$$

eine wohlgeformte Aussage sein. Ist diese Aussage wahr, so sagen wir, dass x durch q mit einem Fehler kleiner als ϵ *approximiert* wird. Wird x durch q mit einem Fehler kleiner als ϵ approximiert, dann auch durch einen Fehler kleiner als ϵ' für alle $\epsilon' \geq \epsilon$.

Für diese Relation gelten zwei weitere Eigenschaften: Zunächst lässt sich jede reelle Zahl x beliebig genau approximieren, das heißt, für jede rationale Zahl $\epsilon > 0$ existiert auch eine rationale Zahl q, durch die x mit einem Fehler kleiner als ϵ approximiert wird, also

$$\forall x \in \mathbf{R}\, \forall \epsilon \in \mathbf{Q}_+\, \exists q \in \mathbf{Q}\colon\ |x - q| < \epsilon.$$

Weiter sind je zwei Approximationen für x nahe beieinander. Genauer: Sind q_1 und q_2 zwei rationale Zahlen, durch die x mit einem Fehler kleiner als ϵ_1 bzw. ϵ_2 approximiert wird, so ist der Abstand zwischen q_1 und q_2 höchstens $\epsilon_1 + \epsilon_2$, also

$$\forall x \in \mathbf{R}\, \forall \epsilon_1, \epsilon_2 \in \mathbf{Q}_+ \forall q_1, q_2 \in \mathbf{Q}\colon \\ (|x - q_1| < \epsilon_1 \wedge |x - q_2| < \epsilon_2 \implies |q_1 - q_2| < \epsilon_1 + \epsilon_2)\,.$$

Damit haben wir die Approximationsrelation für reelle Zahlen erklärt. Es bleibt, eine Konstruktionsvorschrift für die reellen Zahlen anzugeben. Und zwar gilt:

Ist eine Vorschrift gegeben, die es uns erlaubt, zu jeder rationalen Zahl $\epsilon > 0$ eine rationale Zahl q_ϵ zu konstruieren, und zwar so, dass $\left|q_{\epsilon_1} - q_{\epsilon_2}\right| < \epsilon_1 + \epsilon_2$ für jedes Paar ϵ_1, $\epsilon_2 > 0$, so existiert eine reelle Zahl x mit $|x - q_\epsilon| < \epsilon$ für alle $\epsilon > 0$.

Wir haben hier mit Absicht von einer *Konstruktionsvorschrift* geschrieben und nicht von einer Abbildung $\epsilon \mapsto q_\epsilon$ gesprochen. Der Unterschied zwischen beiden ist, dass bei einer

Konstruktionsvorschrift Wahlen in jedem Schritt eingehen dürfen. Erst mit dem (abzählbaren) Auswahlaxiom, welches mit unserer konstruktiven Sichtweise aber nicht verträglich ist, wird durch jede Konstruktionsvorschrift auch eine Abbildung bestimmt.

In Anhang A haben wir eine Interpretation der intuitionistischen Logik lokal über einem topologischen Raum Y gegeben. Hier wird der Unterschied zwischen einer Konstruktionsvorschrift und einer Abbildung noch deutlicher: Ist eine Abbildung $\epsilon \mapsto q_\epsilon$ über Y gegeben, so wird jeder rationalen Zahl $\epsilon > 0$ über Y eine rationale Zahl q_ϵ über Y zugeordnet. Im Gegensatz dazu würden wir bei einer Konstruktionsvorschrift zu jedem $\epsilon > 0$ eine offene Überdeckung $(U_i)_{i\in I}$ von Y und lokal über jedem U_i eine lokale rationale Zahl $q_{\epsilon,i}$ über U_i wählen, ohne dass diese Zahlen Einschränkungen $q_{\epsilon,i} = q_\epsilon|U_i$ einer über Y definierten rationalen Zahl q_ϵ sein müssen.

Doch zurück zu unserer Definition der reellen Zahlen. Wir kennen jetzt die elementare Eigenschaft reeller Zahlen, nämlich dass sie beliebig genau durch rationale Zahlen approximiert werden können, und durch jede solche Approximationsvorschrift wird eine reelle Zahl gegeben.

Beispiele reeller Zahlen können wir sofort angeben. Und zwar können wir jede rationale Zahl q als eine reelle Zahl auffassen, nämlich als diejenige reelle Zahl, welche für alle $\epsilon > 0$ mit einem Fehler kleiner als ϵ durch q approximiert wird. Diese reelle Zahl schreiben wir wieder als q, ohne dass es zu Verwechslungen kommen sollte.

Wir nennen zwei reelle Zahlen x_1 und x_2 *verschieden,* geschrieben $x_1 \neq x_2$, wenn rationale Approximationen q_1 und q_2 mit $|x_1 - q_1| < \epsilon_1$ und $|x_2 - q_2| < \epsilon_2$ aber $|q_1 - q_2| \geq \epsilon_1 + \epsilon_2$ existieren.

Zwei reelle Zahlen x_1 und x_2 heißen *gleich,* geschrieben $x_1 = x_2$, wenn sie nicht verschieden sind, wir haben also

$$x_1 = x_2 \iff \neg(x_1 \neq x_2).$$

Der Grund, warum wir die Gleichheit als Negation der Ungleichheit und nicht umgekehrt die Ungleichheit als Negation der Gleichheit definieren müssen, liegt wieder in unserer konstruktiven Sichtweise begründet. Am einfachsten lässt sich dies wieder mit unserer lokalen Interpretation der intuitionistischen Logik über einem topologischen Raum Y erklären.

Wir wählen dazu $Y = \mathbf{R}$. Wir erinnern uns dann daran, dass eine lokale reelle Zahl über $Y = \mathbf{R}$ als eine stetige Funktion über $\mathbf{R}$ aufgefasst werden kann. Sei x_1 die so als lokale reelle Zahl aufgefasste identische Funktion auf $\mathbf{R}$ und x_2 die Nullfunktion. Dann sind ist die (lokale) Aussage $x_1 \neq x_2$ auf der offenen Teilmenge $\mathbf{R} \setminus \{0\}$, aber nicht auf ganz $\mathbf{R}$ wahr. Nach Definition der Negation ist die lokale Aussage $\neg(x_1 \neq x_2)$, also $x_1 = x_2$, auf der größten offenen Teilmenge im Komplement von $\mathbf{R} \setminus \{0\}$ in $\mathbf{R}$ wahr, also nirgends. Es folgt, dass $\neg(x_1 = x_2)$ überall wahr ist; insbesondere ist $\neg(x_1 = x_2)$ also nicht äquivalent zu $x_1 \neq x_2$ (letztere Aussage impliziert erstere).

C.2 Die reellen Zahlen als Rechenbereich

Sind x_1 und x_2 zwei reelle Zahlen, so ist ihre *Summe* $x_1 + x_2$ diejenige reelle Zahl, welche durch $q_1 + q_2$ bis auf $\epsilon_1 + \epsilon_2$ approximiert wird, wenn x_1 durch q_1 bis auf ϵ_1 und x_2 durch q_2 bis auf ϵ_2 approximiert wird.

Weiter ist das *Produkt* $x_1 \cdot x_2$ von x_1 und x_2 diejenige reelle Zahl, welche durch $q_1 \cdot q_2$ bis auf $q_2\,\epsilon_1 + q_1\,\epsilon_2 + \epsilon_1\,\epsilon_2$ approximiert wird, wenn x_1 durch q_1 bis auf ϵ_1 und x_2 durch q_2 bis auf ϵ_2 approximiert wird.

Um eine rationale Approximation des Produktes $x_1 \cdot x_2$ zu einem vorgegebenen $\epsilon > 0$ zu finden, können wir folgendermaßen vorgehen. Zunächst finden wir rationale Approximationen $\tilde{q}_1$ und $\tilde{q}_2$ von x_1 bzw. von x_2 bis auf 1. Dann wählen wir eine rationale Zahl $0 < \tilde{\epsilon} < 1$, sodass $(4 + |\tilde{q}_1| + |\tilde{q}_2|)\,\tilde{\epsilon} + \tilde{\epsilon}^2 \leq \epsilon$. Sind dann q_1 und q_2 Approximationen von x_1 bzw. x_2 bis auf $\tilde{\epsilon}$, so ist $q_1 \cdot q_2$ eine Approximation von $x_1 \cdot x_2$ bis auf ϵ. Die kurze Rechnung hierzu überlassen wir dem Leser.

Zusammen mit den reellen Zahlen 0 und 1 (welche beliebig genau durch die rationalen Zahlen mit denselben Namen approximiert werden) erfüllen die so definierte Addition und die so definierte Multiplikation die üblichen Rechengesetze, wie sie auch in den ganzen Zahlen gelten. Insbesondere existiert zu jeder reellen Zahl x eine reelle Zahl $-x$, sodass $x + (-x) = 0$.

Jeder reellen Zahl x können wir weiterhin ihren *Betrag* $|x|$ zuordnen: Wird x durch q bis auf ϵ approximiert, so wird $|x|$ durch $|q|$ bis auf ϵ approximiert.

Eingeschränkt auf die rationalen Zahlen stimmen all die hier eingeführten Operationen mit den üblichen überein. Dies gilt auch für folgende Vergleichungsvorschrift:

Ist x eine reelle Zahl, so heißt sie *positiv,* geschrieben $x > 0$, falls ein rationales $c > 0$ existiert, sodass x durch rationale Zahlen $q \geq c$ beliebig genau approximiert werden kann, also

$$x > 0 \iff \exists c \in \mathbf{Q}_+\, \forall \epsilon \in \mathbf{Q}_+\, \exists q \in \mathbf{Q}\colon q \geq c \wedge |x - q| < \epsilon.$$

Sind x_1 und x_2 zwei reelle Zahlen, so heißt x_1 *kleiner* als x_2, geschrieben $x_1 < x_2$, wenn $x_2 - x_1$ positiv ist.

C.3 Cauchysche Prozesse und cauchysche Folgen

Unter einem *cauchyschen Prozess* wollen wir eine Vorschrift verstehen, nach der wir für jede natürliche Zahl n eine reelle Zahl x_n konstruieren können, und zwar so, dass $|x_n - x_{n'}|$ für genügend großes n, n' beliebig klein wird, d. h.

$$\forall \epsilon > 0\, \exists m\, \forall n, n' \geq m\colon\ |x_n - x_{n'}| < \epsilon.$$

Eine *cauchysche Folge* ist ein cauchyscher Prozess, bei dem $n \mapsto x_n$ eine Abbildungsvorschrift ist.

Jede reelle Zahl definiert einen cauchyschen Prozess: Ist nämlich x eine reelle Zahl, so wählen wir für jede natürliche Zahl n eine rationale Approximation q_n von x mit einem Fehler kleiner als $\frac{1}{n}$. Wegen $|q_n - q_{n'}| < \frac{1}{n} + \frac{1}{n'} \to 0$ für $n, n' \to \infty$ folgt, dass q_n ein cauchyscher Prozess ist.

Ist umgekehrt ein cauchyscher Prozess x_n gegeben, so definiert dieser eine reelle Zahl x, die folgendermaßen durch rationale Zahlen approximiert wird: Sei $\epsilon > 0$ eine rationale Zahl. Dann wählen wir eine natürliche Zahl n mit $\frac{1}{n} < \frac{\epsilon}{3}$. Ist dann q_n eine Approximation von x_n mit einem Fehler von weniger als $\frac{1}{n}$, so ist q_n eine Approximation von x mit einem Fehler von weniger als ϵ.

Wir nennen die so definierte reelle Zahl x den *Limes* oder *Grenzwert* des cauchyschen Prozesses x_n und schreiben $x = \lim\limits_{n\to\infty} x_n$.

Jede reelle Zahl ist also insbesondere ein Grenzwert der Form $\lim\limits_{n\to\infty} q_n$, wobei die q_n einen cauchyschen Prozess rationaler Zahlen bilden.

Summe und Produkt sind mit Grenzwertbildung verträglich, das heißt, es gelten

$$\lim_{n\to\infty} (x_n + y_n) = \lim_{n\to\infty} x_n + \lim_{n\to\infty} y_n$$

und

$$\lim_{n\to\infty} (x_n \cdot y_n) = \lim_{n\to\infty} x_n \cdot \lim_{n\to\infty} y_n$$

für je zwei cauchysche Prozesse x_n und y_n.

Allgemein nennen wir eine Funktion f von reellen Zahlen *stetig,* wenn

$$f\left(\lim_{n\to\infty} x_n\right) = \lim_{n\to\infty} f\,(x_n)$$

für cauchysche Prozesse x_n.

Summe und Produkt sind damit (in beiden Argumenten) stetig. Allgemeiner folgt, dass jede Polynomfunktion stetig ist. Weiter ist die Betragsfunktion stetig.

C.4 Wurzeln aus nichtnegativen reellen Zahlen

Wir können die Theorie der cauchyschen Prozesse nutzen, um zu zeigen, dass jede nichtnegative reelle Zahl (eindeutige) k-te Wurzeln für alle $k = 1, 2, 3, \ldots$ betrifft.

Dazu stellen wir zunächst fest, dass k-te Wurzeln aus rationalen Zahlen $q \geq 0$ beliebig genau durch rationale Zahlen approximiert werden können, d h. für jede natürliche Zahl n existiert eine rationale Zahl $r_n \geq 0$ mit $\left|q - r_n^k\right| < \frac{1}{n}$. Die Existenz von r_n folgt konstruktiv; es gibt Algorithmen wie das schriftliche Wurzelziehen oder das newtonsche[5] Verfahren, die es erlauben, ein solches r_n aus q zu bestimmen.

Aus $\left|q - r_n^k\right| < \frac{1}{n}$ für alle n folgt nach einer kleinen Abschätzung, dass die r_n einen cauchyschen Prozess bilden, das heißt, es gibt eine reelle Zahl $y \geq 0$ mit $y = \lim\limits_{n\to\infty} r_n$,

insbesondere $y^k = q$. Wir erhalten damit, dass jede rationale Zahl $q \geq 0$ eine (eindeutige) k-te Wurzel $\sqrt[k]{q} \geq 0$ in den reellen Zahlen besitzt.

Sei schließlich eine beliebige reelle Zahl $x \geq 0$ gegeben. Dann ist x Grenzwert eines cauchyschen Prozesses q_n, wobei die q_n allesamt nichtnegative rationale Zahlen sind. Eine kurze Abschätzung zeigt, dass dann auch die $\sqrt[k]{q_n}$ einen cauchyschen Prozess bilden, also eine reelle Zahl $y \geq 0$ als Grenzwert besitzen. Es folgt $y^k = x$. Damit gibt es für jede nichtnegative reelle Zahl x eine (eindeutige) nichtnegative k-te Wurzel $\sqrt[k]{x}$ in den reellen Zahlen.

C.5 Die Exponentialreihe

Ist x eine beliebige reelle Zahl, so bilden die Summen

$$s_n := \sum_{k=0}^{n-1} \frac{x^k}{k!}$$

eine cauchysche Folge, denn für $0 \ll m \leq n$ gilt

$$\begin{aligned} |s_n - s_m| &= \left| \sum_{k=m}^{n-1} \frac{x^k}{k!} \right| \\ &\leq \sum_{k=m}^{n-1} \frac{|x|^k}{k!} \\ &\leq \frac{|x|^m}{m!} \cdot \sum_{\ell=0}^{n-m-1} \left(\frac{|x|}{m} \right)^\ell \\ &< \frac{|x|^m}{m!} \cdot \frac{1}{1 - \frac{|x|}{m}}, \end{aligned}$$

und die rechte Seite wird für genügend großes m beliebig klein.

Wir erhalten, dass der Grenzwert

$$\mathrm{e}^x := \sum_{k=0}^{\infty} \frac{x^k}{k!} := \lim_{n \to \infty} \sum_{k=0}^{n-1} \frac{x^k}{k!}$$

existiert. Wir nennen die so erhaltene reelle Funktion $x \mapsto \mathrm{e}^x$ *(reelle) Exponentialfunktion*.

Auf ganz ähnliche Weise zeigt sich, dass *Kosinus*

$$\cos x := \sum_{n=0}^{\infty} (-1)^n \frac{x^{2n}}{(2n)!}$$

und *Sinus*

$$\sin x := \sum_{n=0}^{\infty} (-1)^n \frac{x^{2n+1}}{(2n+1)!}$$

reelle Zahlen sind.

Proposition C.1 *Sind x_1 und x_2 zwei reelle Zahlen, so gilt folgendes Additionstheorem:*

$$\mathrm{e}^{x_1+x_2} = \mathrm{e}^{x_1} \cdot \mathrm{e}^{x_2}.$$

Beweis Nach dem Binomialtheorem gilt:

$$\begin{aligned}
\mathrm{e}^{x_1+x_2} &= \sum_{n=0}^{\infty} \frac{(x_1+x_2)^n}{n!} \\
&= \sum_{n=0}^{\infty} \sum_{k=0}^{n} \binom{n}{k} \frac{x_1^k\, x_2^{n-k}}{n!} \\
&= \sum_{n=0}^{\infty} \sum_{k=0}^{n} \frac{x_1^k}{k!} \frac{x_2^{n-k}}{(n-k)!} \\
&= \sum_{n_1,n_2=0}^{\infty} \frac{x_1^{n_1}}{n_1!} \frac{x_2^{n_2}}{n_2!} \\
&= \left(\sum_{n_1=0}^{\infty} \frac{x_1^{n_1}}{n_1!} \right) \cdot \left(\sum_{n_2=0}^{\infty} \frac{x_2^{n_2}}{n_2!} \right) \\
&= \mathrm{e}^{x_1} \cdot \mathrm{e}^{x_2}.
\end{aligned}$$

Korollar C.1 *Ist x eine reelle Zahl, so gilt für jede ganze Zahl, dass*

$$\mathrm{e}^{n \cdot x} = \left(\mathrm{e}^{x}\right)^n.$$

Glossar

Äquivalenzrelation Reflexive, symmetrische und transitive Relation.

Algebraisch eindeutige Wurzel Nullstelle eines irreduziblen Polynoms der Form $X^n - a$.

Algebraische Unabhängigkeit Ein System von Zahlen heißt algebraisch unabhängig, wenn es keine nichttriviale polynomielle Beziehung zwischen ihnen gibt.

Algebraische Relation Polynomielle Beziehung zwischen algebraischen Zahlen, häufig den Nullstellen eines separablen Polynoms.

Algebraische Zahl Komplexe Zahl, die Nullstelle eines nichttrivialen Polynoms mit rationalen Koeffizienten ist.

Alternierende Gruppe Untergruppe der geraden Permutationen in der symmetrischen Gruppe.

Auflösbare Gruppe Gruppe, die eine Normalreihe besitzt, deren Faktoren von Primordnung sind.

Diskriminante Polynom in den Koeffizienten einer Gleichung, welches genau dann verschwindet, wenn die Gleichung eine mehrfache Lösung (in einem algebraischen Abschluss) besitzt.

Einfache Gruppe Gruppe, die genau zwei Normalteiler besitzt (die triviale Untergruppe und sich selbst).

Einheitswurzel Komplexe Nullstelle von $X^n - 1$.

Elementarsymmetrische Funktion Bestimmte symmetrische Polynome in n Unbestimmten.

Fehlstand einer Permutation Anzahl der Paare von Stellen, deren relative Anordnung durch die Permutation vertauscht wird.

Galoissch konjugiert Zwei Zahlen sind galoissch konjugiert, wenn sie das gleiche Minimalpolynom besitzen.

Galoissche Gruppe Gruppe aller Symmetrien der Nullstellen eines separablen Polynoms.

M. Nieper-Wißkirchen, *Elementare Galois-Theorie,*
https://doi.org/10.1007/978-3-662-60934-7

Ganze algebraische Zahl Komplexe Zahl, die Nullstelle eines normierten Polynoms mit ganzzahligen Koeffizienten ist.

Gerade Permutation Permutation, deren Signum positiv ist.

Grad einer algebraischen Zahl Grad des Minimalpolynoms der algebraischen Zahl.

Index einer Untergruppe Anzahl der Kongruenzklassen modulo der Untergruppe.

Komplexe Zahlen Die komplexen Zahlen bilden die kleinste Erweiterung der reellen Zahlen, in denen eine Quadratwurzel i aus -1 existiert.

Komplexprodukt Teilmenge der Form $H \cdot N = \{h \cdot n \mid h \in H, n \in N\}$ für Teilmengen H und N einer Gruppe.

Kongruenz modulo einer Untergruppe Zwei Elemente τ und τ' einer Gruppe G heißen kongruent modulo H, falls ein $\rho \in H$ mit $\tau = \tau' \circ \rho$ existiert.

Konstruierbare Zahl Punkt in der komplexen Zahlenebene, welcher nur mit Zirkel und Lineal aus den Punkten 0 und 1 konstruiert werden kann.

Kreisteilungsgleichung Gleichung der Form $X^n - 1 = 0$.

Kreisteilungspolynom Minimalpolynom einer primitiven Einheitswurzel.

Minimalpolynom einer algebraischen Zahl Normiertes Polynom kleinsten Grades, welches eine algebraische Zahl als Nullstelle hat.

Normalreihe Absteigende Folge von Untergruppe einer Gruppe, sodass die einzelnen Faktoren jeweils durch Inklusionen von Normalteilern gebildet werden.

Normalteiler Untergruppe einer Gruppe, welche invariant unter Konjugation mit beliebigen Gruppenelementen ist.

Ordnung einer Gruppe Anzahl der Elemente einer Gruppe.

Ordnung eines Elements Kleinster positiver Exponent, sodass die Potenz des Elementes mit diesem Exponenten 1 ergibt.

***p*-Gruppe** Gruppe von Primpotenzordnung.

Permutationsgruppe Untergruppe einer symmetrischen Gruppe.

Polynomgleichung Gleichung der Form $a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0 = 0$, wobei die Koeffizienten $a_0, \ldots, a_n$ Elemente eines Rechenbereiches sind.

Quadratur des Kreises Problem, zu einem vorgegebenen Kreis nur mit Zirkel und Lineal ein Quadrat mit gleichem Flächeninhalt zu konstruieren.

Radikalerweiterung Erweiterung der Form $K(a)$ über K, wobei a eine algebraisch eindeutige Wurzel über K ist.

Separables Polynom Polynom, welches keine mehrfachen Nullstellen (in einem algebraischen Abschluss) besitzt.

Signum einer Permutation Das Signum einer Permutation ist $+1$, falls die Permutation eine gerade Anzahl von Fehlständen besitzt, sonst -1.

Symmetrische Gruppe Volle Permutationsgruppe.

Transitive Operation Operation einer Gruppe auf einer Menge, sodass für jedes Paar x, y von Elementen der Menge ein Gruppenelement g mit $g \cdot x = y$ existiert.

Transzendente Zahl Komplexe Zahl, welche nichtalgebraisch ist.

Untergruppe Teilmenge einer Gruppe, welche unter Komposition und Inversenbildung abgeschlossen ist und die Identität enthält.

Vandermondesche Determinante Polynom in n Unbestimmten, welches als Determinante einer bestimmten $(n \times n)$-Matrix definiert ist.

Würfelverdoppelung Problem, zu einem vorgegebenen Würfel nur mit Zirkel und Lineal einen Würfel mit doppeltem Volumen zu konstruieren.

Winkeldreiteilung Problem, einen vorgegebenen Winkel nur mit Zirkel und Lineal in drei gleiche Teile zu teilen.

Zahlkörper Erweiterung von $\mathbf{Q}$ der Form $\mathbf{Q}(t_1, \ldots, t_n)$ mit algebraischen Zahlen $t_1, \ldots, t_n$.

Zentralisator eines Elementes Der Zentralisator eines Gruppenelementes σ ist die Teilmenge der Gruppenelemente, die mit σ vertauschen.

Zentrum Teilmenge der Gruppenelemente, die mit allen anderen Gruppenelementen vertauschen.

Zykel Permutation der Form $(i_1, i_2, i_3, \ldots, i_k)$, also eine Permutation, die i_1 auf i_2, i_2 auf i_3 usw. und i_k auf i_1 abbildet und die übrigen Elemente jeweils auf sich selbst.

Zyklische Gruppe Gruppe, die von einem Element erzeugt wird.

Anmerkungen

1. Rodion Ossijewitsch Kusmin, 1891–1949, sowjetischer Mathematiker.
2. Alexander Osipovich Gelfond, 1906–1968, sowjetischer Mathematiker.
3. Theodor Schneider, 1911–1988, deutscher Mathematiker.
4. Georg Friedrich Bernhard Riemann, 1826–1866, deutscher Mathematiker.
5. Sir Isaac Newton, 1642–1727, englischer Mathematiker, Physiker, Astronom und Theologe.

Stichwortverzeichnis

M. Nieper-Wißkirchen, *Elementare Galois-Theorie,*
https://doi.org/10.1007/978-3-662-60934-7