Lineare Algebra individuell
Online-Fassung, Ver. 0.42
Internes Material, **12.4.2004**

Kapitel 2

Algebraische Gleichungen

Das Wort „Algebra“ wird auf eine Aufgabensammlung aus dem 9. Jahrhundert zurückgeführt; es entstand aus ihrem Titel „Hisâb al-jabr w'almuqâbalah“ („Wissenschaft der Reduktion und des gegenseitigen Aufhebens“). Verfasst wurde dieses Buch von Muhammad ibn Musa al Hwârizmí, aus dessen Namen im Laufe der Zeit auch das Wort „Algorithmus“ entstanden sein soll.
Algebra in ihrem ursprünglichen Sinn ist so als die Lehre der Auflösung von Gleichungen zu verstehen. Damit beschäftigten sich bereits Mathematiker früher Kulturen, etwa im Zusammenhang mit Problemen geometrischer Art, wie sie in der Landvermessung auftraten. Es gibt Keilschrifttafeln aus dem 2. Jahrtausend v.u.Z., auf denen lineare Gleichungssysteme mit mehreren Unbekannten und sogar Systeme höheren Grades gelöst werden.

Wir haben bereits im 1. Kapitel gesehen, dass die Frage nach der Auflösung von Gleichungen immer wieder Anlass zur Erweiterung des Zahlbegriffs gab. Die ganzen Zahlen erhalten wir als Lösung des Problems, wie zu gegebenen natürlichen Zahlen a und b eine Zahl x gefunden werden kann, für die $a + x = b$ ist. Das ist allgemein möglich, wenn anstelle der natürlichen die ganzen Zahlen betrachtet werden.
Eine ähnliche Situation ergibt sich für die Multiplikation.
Die Gleichung $a{\cdot}x = b$ mit $a, b \in \mathbb{Z}$ und $a \neq 0$ besitzt erst nach Übergang zum Körper $\mathbb{Q}$ der rationalen Zahlen stets eine Lösung $x \in \mathbb{Q}$.
Wie schon früher erwähnt, entsteht durch die Konstruktion des Körpers $\mathbb{C}$ der komplexen Zahlen ein Zahlbereich, in dem jedes nichtkonstante Polynom mindestens eine Nullstelle besitzt. Wir wollen allerdings nicht übersehen, dass es vom Wissen über die Existenz einer Nullstelle bis zu ihrem Auffinden ein weiter Weg sein kann. Es gibt sogar Gleichungen, für die es prinzipiell unmöglich ist, eine Lösung im Sinne einer Formel anzugeben, in der außer den Grundrechenarten nur Wurzelausdrücke vorkommen, so wie wir dies z.B. von quadratischen Gleichungen kennen.
Ein Gegenbeispiel (wir geben hier keinen Beweis an) ist die recht einfach anmutende Gleichung $x^5 - 10x - 2 = 0$, die nach dem Zwischenwertsatz der Analysis sogar eine reelle Lösung besitzt. Dieses Phänomen werden wir erst recht zu beachten haben, wenn wir Systeme von Gleichungen höheren Grades mit mehreren Variablen lösen.
Der Verzicht auf Exaktheit beim Rechnen mit Näherungen wirft dagegen neue Probleme auf.

Die Naturwissenschaften und die Technik stellen gerade in der Gegenwart allerhöchste Anforderungen an die Mathematik hinsichtlich der Auflösung von Gleichungssystemen. Dies ist keine einseitige Entwicklung. Die Nutzung von Computern hatte zweifellos einen entscheidenden Einfluß auf die Entwicklung der letzten Jahrzehnte des 20. Jahrhunderts, wovon auch die „reine“ Mathematik nicht unberührt blieb: Die Auflösung polynomialer Gleichungen konnte in gewisser Weise automatisiert werden. Das symbolische Rechnen (auch *Computeralgebra* genannt) wurde nicht nur zu einer Schlüsseltechno-

logie der heutigen Informationsgesellschaft, es eröffnet der mathematischen Forschung den Zugang zur Nutzung von Algorithmen, die vergangenen Generationen von Mathematikern zwar in Ansätzen bekannt waren, wegen ihrer Komplexität aber ohne die aktuellen technischen Hilfsmittel nicht genutzt werden konnten.
Wir sollten jedoch nicht erwarten, dass eines Tages Maschinen unsere Arbeit erledigen, sondern müssen uns im Gegenteil bewusst sein, dass wir vor Herausforderungen stehen, wie es sie in der Geschichte der Mathematik noch nicht gegeben hat. Bruno Buchberger, der für die Computeralgebra fundamentale Arbeit geleistet hat, bemerkte dazu, wer heute Mathematik studiere, befinde sich „... im ‚Auge des Hurricans' der modernen Entwicklung und nicht irgendwo in einem Hinterzimmer“ ... „Je algorithmischer und dann je effizienter man mathematische Probleme lösen will, umso mehr mathematische Theorie und umso schwierigere Beweise sind nötig und nicht umgekehrt“ (vgl. [DMV][1]).

Das vorliegende Kapitel kann nicht mehr sein als ein Einstieg in die Frage nach den Lösungen polynomialer Gleichungssysteme. Am Schluss wird klar, dass die Struktur der Lösungsmengen sehr viel subtiler ist, als es auf den ersten Blick vermutet werden mag. Die mathematische Disziplin, die sich insbesondere den qualitativen Aspekten des Studiums der Lösungsmengen widmet, ist die algebraische Geometrie. Die numerische Mathematik befasst sich dagegen mit dem Auffinden von Näherungslösungen; auch dazu können wir hier nur Andeutungen machen.

2.4 Teilbarkeitslehre im Polynomring $K[X]$

K bezeichnet einen festen Grundkörper. Wir untersuchen Teilbarkeitseigenschaften der Polynome im Ring $K[X]$. In einem wohl verstandenen Sinn ist dies das Studium der Lösungsmengen von Gleichungen in einer Unbekannten. Es wird insbesondere gezeigt, dass eine im Wesentlichen eindeutige Zerlegung in irreduzible Faktoren existiert; eine analoge Aussage kennen wir schon für ganze Zahlen, und auch ihr Beweis stimmt weitgehend mit dem bereits vertrauten Fall überein. 2/4/1

vgl. auch 1/2/28

Bezeichnungen.
Die lexikographische Ordnung der Monome in $K[X]$ ist durch

$$\ldots > X^t > X^{t-1} > \ldots > X^2 > X > 1$$

gegeben, und für $f = a_s X^s + a_{s-1} X^{s-1} + \ldots + a_1 X + a_0 \in K[X]$ mit $a_i \in K$, $a_s \neq 0$ setzen wir

$\mathrm{LC}(f) := a_s$ (*Leitkoeffizient* oder *Anfangskoeffizient*),

$\mathrm{LM}(f) := X^s$ (*Leitmonom oder Anfangsmonom*),

$\mathrm{LT}(f) := a_s X^s = \mathrm{LC}(f) \cdot \mathrm{LM}(f)$ (*Leitterm* oder *Anfangsterm*).

vgl. auch 2/2/1 für die analogen Notationen im Fall linearer Polynome

$\mathrm{LC}(f) = 1$ bedeutet, dass f ein normiertes Polynom ist. Im Unterschied zur Untersuchung linearer Polynome ist im vorliegenden Fall $\mathrm{LM}(f) > \mathrm{LM}(g)$ gleich bedeutend mit der Bedingung $\deg(f) > \deg(g)$.

Sind $f, g \in K[X] \setminus \{0\}$ und $s = \deg(f) \geq \deg(g) = t$, so setzen wir

$$\mathrm{S}(f,g) := f - \frac{\mathrm{LT}(f)}{\mathrm{LT}(g)} \cdot g = f - \frac{\mathrm{LC}(f)}{\mathrm{LC}(g)} X^{s-t} g.$$

[1] *Mitteilungen der Deutschen Mathematiker-Vereinigung*, 2/2000

Da sich die Terme höchsten Grades aufheben, ist $\deg(f) > \deg(\mathrm{S}(f,g))$.

Lemma. (*Division mit Rest*) 2/4/2

Sind $f, g \in K[X]$ *Polynome und* $g \neq 0$, *so existieren* $q, r \in K[X]$ *mit* $f = gq + r$ *und* $\deg(r) < \deg(g)$. Wir sagen auch, f *ist mit Rest* r *durch* g *teilbar* und schreiben dafür gelegentlich

$$f : g = q \quad \text{Rest} \quad r.$$

Diese Bezeichnung ist uns bereits vom Rechnen mit ganzen Zahlen vertraut.

Beweis. Der Fall $\deg(f) < \deg(g)$ ist trivial ($q = 0$ und $r = f$). Nun sei $\deg(f) \geq \deg(g)$. Wir fixieren g und nehmen induktiv an, die Behauptung gelte für Polynome kleineren Grades als $\deg(f)$, können also voraussetzen, dass insbesondere $\mathrm{S}(f,g) = q_1 g + r$ mit $\deg(r) < \deg(g)$ ist. Durch Einsetzen folgt

$$f = \mathrm{S}(f,g) + \frac{\mathrm{LT}(f)}{\mathrm{LT}(g)} \cdot g = (q_1 + \frac{\mathrm{LT}(f)}{\mathrm{LT}(g)}) \cdot g + r$$

und damit die Induktionsbehauptung. ❑

Der Induktionsanfang mit $f = 0$ ist durch den Fall $\deg(f) < \deg(g)$ bereits erledigt.

So wie für lineare Polynome gibt es auch im vorliegenden Fall ein grundlegendes Verfahren zum Auffinden einer Normalform.

Euklidischer Algorithmus 2/4/3

Es seien $f, g \in K[X] \setminus \{0\}$ und $\deg(f) \geq \deg(g)$. Ist $\mathrm{S}(f,g) \neq 0$, so ordnen wir (f,g) das Paar $(f_1, g_1) \in (K[X] \setminus \{0\})^2$ zu,

$$(f_1, g_1) := (\mathrm{S}(f,g), g) \quad \text{für} \quad \deg(\mathrm{S}(f,g)) \geq \deg(g) \quad \text{bzw.}$$
$$(f_1, g_1) := (g, \mathrm{S}(f,g)) \quad \text{für} \quad \deg(\mathrm{S}(f,g)) < \deg(g).$$

Dies ist – solange der erste Fall eintritt – die Aufeinanderfolge der Teilschritte einer Division mit Rest.

Konstruktionsgemäß ist $\deg(f) > \deg(f_1)$ oder $\deg(g) > \deg(g_1)$. Fahren wir entsprechend fort, so muss deshalb nach endlich vielen Schritten

$$(f,g) \mapsto (f_1, g_1) \mapsto \ldots \mapsto (f_i, g_i) \mapsto (f_{i+1}, g_{i+1}) \mapsto \ldots \mapsto (f_l, g_l)$$

das Verfahren abbrechen, also $\mathrm{S}(f_l, g_l)$ das Nullpolynom sein. $d := g_l$ heißt dann *letzter Teiler im euklidischen Algorithmus*.

Zusammenfassen von Teilschritten ergibt eine Folge von Divisionen mit Rest und damit eine weitere Interpretation für d.

Bemerkung. (*Kettendivision*) 2/4/4

Mit den obigen Bezeichnungen gilt:

(1) d ist der letzte von 0 verschiedene Rest einer Kettendivision, d.h. das letzte Polynom in einer Folge
$$(f,g) \mapsto (h_1, h_2) \mapsto \ldots \mapsto (h_i, h_{i+1}) \mapsto \ldots \mapsto (h_n, d),$$
die so entsteht: Beginnend mit (f,g) ordnen wir einem Paar $(h_i, h_{i+1}) \in (K[X] \setminus \{0\})^2$ mit $\deg(h_i) \geq \deg(h_{i+1})$ das Paar (h_{i+1}, r) zu, wobei r der Rest von h_i bei Division durch h_{i+1} ist. Das ist die „klassische Form" des euklidischen Algorithmus.

. . . eine Wiederholung von 1/2/26

(2) Es existieren Polynome $p, q \in K[X]$ mit $d = pf + qg$. Diese Eigenschaft folgt durch schrittweises Einsetzen aus dem angegebenen Verfahren zur Bestimmung von d.

Beispiel.

Für $f = X^4 + 3X^3 + X^2 - 3X - 2$ und $g = X^4 + 2X^3 - 4X^2 - 2X + 3$ ergibt der euklidische Algorithmus

$$(f,g) \mapsto (X^4 + 2X^3 - 4X^2 - 2X + 3, X^3 + 5X^2 - X - 5)$$

In der Aufgabensammlung finden Sie Hinweise zur systematischen Bestimmung von d als Vielfachensumme von f und g.

$\mapsto (X^3+5X^2-X-5, 12X^2-12)$,
und $d = 12X^2 - 12$ ist der letzte von 0 verschiedene Teiler. Aus
$f = 1 \cdot g + (X^3+5X^2-X-5)$ und $g = (X-3)\cdot(X^3+5X^2-X-5)+d$
folgt durch Einsetzen $d = (3-X)\cdot f + (X-2)\cdot g$.

Mit dem euklidischen Algorithmus lassen sich (zumindest prinzipiell) Gleichungssysteme in $K[X]$ lösen: Wir zeigen zunächst, dass zwei Polynome stets durch ein einziges ersetzt werden können, das dieselbe Nullstellenmenge besitzt. Dieser Fall ist repräsentativ für eine beliebige endliche Menge von Polynomen.

Bemerkung. *Es seien $f, g \in K[X]\setminus\{0\}$, $\deg(f) \geq \deg(g)$ und d der letzte Teiler im euklidischen Algorithmus für das Paar (f,g). Dann gilt für die Nullstellenmengen dieser Polynome $V(f,g) = V(d)$.* 2/4/5

Beweis. Mit den Bezeichnungen aus 2/4/3 sei $f_i = \mathrm{S}(f_i,g_i) + h\cdot g_i$, $h \in K[X]$. Nun gilt für beliebige $x \in K$:

$$f_i(x) = g_i(x) = 0 \iff \big(\mathrm{S}(f_i,g_i)\big)(x) = g_i(x) = 0,$$

und induktiv folgt

$$f(x) = g(x) = 0 \iff \big(\mathrm{S}(f_l,g_l)\big)(x) = g_l(x) = 0.$$

Für $g_l = d$ ist aber $\mathrm{S}(f_l,g_l)$ das Nullpolynom, daher ist die letztere Bedingung äquivalent zu $d(x) = 0$. Wir erhalten $d(x) = 0 \iff x \in V(f,g)$. ❏

Im obigen Beispiel ist $V(f,g) = V(d) = V(12(X+1)(X-1)) = \{1,-1\}$.
Es wird sich herausstellen, dass der gefundene Teiler d sogar größter gemeinsamer Teiler von f und g ist, wodurch 2/4/5 verfeinert wird.

Die Bemerkung und ihr Beweis erinnern an den gaußschen Algorithmus. Allerdings haben wir verschiedene Probleme bei der Interpretation des Resultats. 2/4/6

- Die Bestimmung der Nullstellen eines Polynoms kann schwierig, in einem gewissen (hier nicht präzisierten) Sinn sogar unmöglich sein.
- Es ist zweckmäßig, den Nullstellen „Vielfachheiten“ zuzuordnen, denn obwohl etwa die Polynome $f(X) = (X-1)^5$ und $g(X) = X-1$ nur eine einzige Nullstelle besitzen (nämlich $x = 1$), besteht ein qualitativer Unterschied zwischen beiden Fällen.
- Anders als lineare Polynome müssen Polynome vom Grad > 1 keine Nullstellen in einem gegebenen Grundkörper haben. Ein schon früher erwähntes Beispiel dafür ist das Polynom $X^2+1 \in \mathbb{R}[X]$.

Kennen wir wenigstens eine der Nullstellen kennen, so hilft ein Trick.

Bemerkung. (*Ausklammern von Linearfaktoren*) 2/4/7

(1) $x \in K$ sei eine Nullstelle von $f \in K[X]\setminus\{0\}$, d.h. $f(x) = 0$. Dann existiert ein Polynom $q \in K[X]$ mit $f = q\cdot(X-x)$.

(2) *hornersches Schema*: Ist $f = a_nX^n + \ldots + a_1X + a_0 \in K[X]$ mit $a_0, \ldots, a_n \in K$ ein Polynom vom Grad $n \geq 1$, so ergibt sich die Zahl $f(x)$ für beliebige $x \in K$ durch folgende Vorschrift. Wir setzen

$$b_0 := a_n,\quad b_i := b_{i-1}x + a_{n-i} \quad \text{für } i = 1, \ldots, n$$

und erhalten $f(x) = b_n$. Gilt überdies $f(x) = 0$, so ist

$$f = q\cdot(X-x) \text{ mit } q := b_0X^{n-1} + b_1X^{n-2} + \ldots + b_{n-2}X + b_{n-1}.$$

Dieses Vorgehen erlaubt die Bestimmung von $f(x)$ mit einer geringen Anzahl aufwändiger Rechenoperationen (Multiplikationen).

(3) Unter der Voraussetzung (1) existiert eine größte natürliche Zahl m, für die $(X-x)^m$ ein Teiler von f ist. In diesem Fall ist $f = h\cdot(X-x)^m$ mit $h(x) \neq 0$. Die Zahl m wird *Vielfachheit* (*Multiplizität*) der Nullstelle x von f genannt.

(4) Für ein Polynom $f = (X-a_1)\cdot\ldots\cdot(X-a_n)$ ergibt sich die Nullstellenmenge als $V(f) = \{a_1, \ldots, a_n\}$.

Beweis. (1) folgt aus (2). Wir bemerken unabhängig davon, dass dies noch einfacher durch Division mit Rest erhalten werden kann, denn ist $f = q\cdot(X-x)+r$ mit $\deg(r) < \deg(X-x) = 1$, so muss r ein konstantes Polynom sein; Einsetzen von x in $r = f - q\cdot(X-x)$ ergibt $r = 0$.

(1) kann leicht auch direkt erhalten werden: Ist $f = q\cdot(X-x)+r$ mit $\deg(r) < \deg(X-x) = 1$, so folgt $r \in K$. Einsetzen von x in $r = f - q\cdot(X-x)$ ergibt $r = 0$.

Zum Beweis von (2) wird zunächst induktiv geprüft (Übungsaufgabe), dass

$$b_i = a_n x^i + a_{n-1}x^{i-1} + \ldots + a_{n-i}\,, \quad (i = 0, \ldots, n)$$

ist, damit folgt insbesondere $b_n = f(x)$. Weiter gilt

$$\begin{aligned} q\cdot(X-x) &= (b_0X^{n-1} + b_1X^{n-2} + \ldots + b_{n-2}X + b_{n-1})\cdot(X-x) \\ &= b_0X^n + b_1X^{n-1} + \ldots + b_{n-1}X \\ &\qquad -b_0xX^{n-1} - \ldots - b_{n-2}xX - b_{n-1}x \\ &= b_0X^n + \underbrace{(b_1 - b_0x)}_{a_{n-1}}X^{n-1} + \ldots + \underbrace{(b_{n-1} - b_{n-2}x)}_{a_1}X - b_{n-1}x, \end{aligned}$$

woraus sich im Fall $0 = f(x)$ wegen $b_n = 0$ sofort $a_0 = b_n - b_{n-1}x = -b_{n-1}x$ als konstanter Term der rechten Seite ergibt, daher $q\cdot(X-x) = f$.

(3) erhalten wir durch wiederholte Anwendung von (1).

(4) folgt, da im Grundkörper K ein Produkt $(x-a_1)\cdot\ldots\cdot(x-a_n)$ genau dann gleich 0 ist, wenn wenigstens einer der Faktoren verschwindet, also $x - a_i = 0$ gilt für einen Index i. ❑

Satz. 2/4/8

(1) *Ist $f \in K[X]$ nicht das Nullpolynom, so ist seine Nullstellenmenge $V(f)$ endlich, denn dann ist f ein Produkt $f = (X-a_1)\cdot\ldots\cdot(X-a_s)\cdot h$ mit $V(h) = \emptyset$.*

(2) *Sind $f, g \in K[X]$ Polynome und $f(x) = g(x)$ für unendliche viele $x \in K$, so ist $f = g$ (Identitätssatz für Polynome).*

Beweis. Der erste Teil der Behauptung folgt durch wiederholtes Ausklammern linearer Faktoren nach der vorhergehenden Bemerkung 2/4/7 (1). Zum Beweis von (2) wird (1) auf $f-g$ angewendet: Ist $V(f-g)$ unendlich, so muss $f-g$ das Nullpolynom sein. ❑

Im Fall eines endlichen Grundkörpers lassen sich die Nullstellen von Polynomen beispielsweise durch systematisches Probieren ermitteln. Über den für uns besonders wichtigen Körpern der komplexen und der reellen Zahlen können wir die Typen irreduzibler Polynome angeben.

Der Begriff des irreduziblen Ringelements wird hier im Spezialfall des Polynomrings untersucht.

Satz. *$f \in K[X]$ sei ein normiertes Polynom vom Grad $n > 0$.* 2/4/9

(1) *Ist $K = \mathbb{C}$, so existieren* (nicht notwendig verschiedene) *Zahlen $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$ mit $f = (X-\alpha_1)\cdot\ldots\cdot(X-\alpha_n)$.*

D.h. in $\mathbb{C}[X]$ sind genau die linearen Polynome irreduzibel.

(2) *Ist $K = \mathbb{R}$, dann existieren $r, s \in \mathbb{N}$ mit $r + 2s = n$ sowie Zahlen $a_1, \ldots, a_r, b_1, \ldots, b_s, c_1, \ldots, c_s \in \mathbb{R}$ mit $f = (X-a_1)\cdot\ldots\cdot(X-a_r)\cdot(X^2+2b_1X+c_1)\cdot\ldots\cdot(X^2+2b_sX+c_s)$, wobei die Polynome $X^2+2b_iX+c_i$ keine* (reellen) *Nullstellen besitzen* (d.h. $b_i^2 < c_i$, $1 \le i \le s$).

D.h. in $\mathbb{R}[X]$ sind genau die linearen Polynome sowie die quadratischen Polynome ohne reelle Nullstellen irreduzibel.

Beweis. Der Fall (1) ergibt sich unter Benutzung der vorigen Bemerkung aus dem Fundamentalsatz der Algebra (vgl. 1/2/8).

Unter (2) betrachten wir das Polynom f zunächst als Element von $\mathbb{C}[X]$. Die Zahlen $\alpha_i \in \mathbb{C}$, die sich dann gemäß (1) finden lassen, werden so angeordnet: $\alpha_1, \ldots, \alpha_s \in \mathbb{R}$ und $\alpha_{r+1}, \ldots, \alpha_n \notin \mathbb{R}$. Ist weiter α eine der zuletzt genannten nicht reellen Nullstellen von f, dann muss wegen $f(\alpha) = 0$ auch $f(\overline{\alpha}) = 0$ sein (die komplexe Konjugation ist mit Addition und Multiplikation vertauschbar, insbesondere also $0 = \overline{f(\alpha)} = \overline{\sum_i a_i\alpha^i} = \sum_i \overline{a_i} \cdot \overline{\alpha}^i = \sum_i a_i\overline{\alpha}^i = f(\overline{\alpha})$, wenn $a_i \in \mathbb{R}$ die Koeffizienten von f sind). Daher kommen die nicht reellen Nullstellen α des Polynoms f stets in Paaren $(\alpha, \overline{\alpha})$ mit $\alpha \neq \overline{\alpha}$ vor. Folglich ist $(X - \alpha_{r+1}) \cdot \ldots \cdot (X - \alpha_n)$ (nach evtl. Umsortieren und Ausmultiplizieren) ein Produkt von Faktoren

$$(X - \alpha) \cdot (X - \overline{\alpha}) = (X^2 - (\alpha + \overline{\alpha})X + \alpha\overline{\alpha}) ,$$

wobei $\alpha + \overline{\alpha} = 2\mathrm{Re}(\alpha) \in \mathbb{R}$ und $\alpha\overline{\alpha} = |\alpha|^2 \in \mathbb{R}$. ❑

Mit den im Kap. 1 (1/2/19 - 1/2/25) eingeführten Begriffen der Teilbarkeitslehre werden nun ganz allgemein Faktorzerlegungen von Polynomen untersucht. Wir erinnern daran, dass die Einheiten in $K[X]$ genau die von 0 verschiedenen konstanten Polynome sind. Assoziiertheit bedeutet daher, dass sich Polynome nur um einen konstanten Faktor $\neq 0$ unterscheiden.

Irreduzibilität ist nicht immer leicht zu prüfen, wir erwähnen hier die einfachsten Fälle.

Lemma. *$f \in K[X]$ sei ein nichtkonstantes Polynom.* 2/4/10

(1) $\deg(f) = 1 \;\Rightarrow\; f$ *ist irreduzibel.*

(2) *Es sei* $\deg(f) \in \{2, 3\}$, *so gilt*:
f *ist irreduzibel* $\iff$ f *besitzt keine Nullstelle in* K.

Beweis. Aus $f = g \cdot h$ folgt $\deg(f) = \deg(g) + \deg(h)$ mit $\deg(g) \geq 0$ und $\deg(h) \geq 0$. Im Fall (1) zeigt dies $g \in K^*$ oder $h \in K^*$. Ist im Fall (2) weder g noch h konstant, so muss eines der Polynome g, h linear sein, also f eine Nullstelle besitzen. ❑

Beispiele.

1. $f = X^3 + X^2 + 1 \in \mathbb{F}_2[X]$ ist irreduzibel, denn $\deg(f) = 3$ und f hat keine Nullstelle in $\mathbb{F}_2$. Um Letzteres einzusehen, bestimmen wir alle Werte $f(x)$ mit $x \in \mathbb{F}_2$: Es ist $f(0) = f(1) = 1$.
2. $f = X^3 - 2 \in \mathbb{Q}[X]$ ist irreduzibel, denn eine Nullstelle in $\mathbb{Q}$ wäre auch Nullstelle des Polynoms f, betrachtet als Element von $\mathbb{R}[X]$. In diesem Ring gilt aber $f = (X - \sqrt[3]{2})(X^2 + \sqrt[3]{2}X + \sqrt[3]{4})$, und der zweite Faktor besitzt keine reelle Nullstelle, d.h. $\sqrt[3]{2} \notin \mathbb{Q}$ ist einzige reelle Nullstelle von f.

Nicht immer lässt sich Irreduzibilität so leicht feststellen:

3*. $f = X^5 - 10X - 2 \in \mathbb{Q}[X]$ ist irreduzibel. Zum Nachweis wird zunächst gezeigt, dass eine Faktorzerlegung $f = gh$ in zwei echte Teiler g und h zur Folge hat, dass auch zwei normierte echte Teiler von f in $\mathbb{Z}[X]$ existieren, deren Produkt f ist.
Danach hilft ein Trick: Von den beiden Teilern besitzt genau einer einen konstanten Term, der durch 2 teilbar ist, und mittels Teilbarkeitseigenschaften ganzer Zahlen folgt daraus, dass auch alle übrigen Koeffizienten dieses Faktors gerade sind. Das ist wegen der Normiertheit unmöglich.

Die nachfolgenden Überlegungen zur Teilbarkeitslehre von Polynomen verlaufen sehr ähnlich zum bereits behandelten Fall der ganzen Zahlen.

Satz. (*Existenz des größten gemeinsamen Teilers*) 2/4/11

Sind $f, g \in K[X] \setminus \{0\}$ *und o.B.d.A.* $\deg(f) \geq \deg(g)$, *so ist der letzte von* 0 *verschiedene Teiler im euklidischen Algorithmus* 2/4/3 *ein größter gemeinsamer Teiler von* f *und* g.

Beweis. d sei der letzte von 0 verschiedene Rest in der Kettendivision. Wie durch Einsetzen zu sehen ist, teilt d dann sowohl f als auch g.
Da d nach 2/4/4 (2) Vielfachensumme von f und g ist, muss jeder Teiler beider Polynome auch d teilen. ❏

Natürlich existiert ein größter gemeinsamer Teiler d der Polynome f und g auch ohne die obige Einschränkung $f, g \neq 0$. Sind f und g nicht beide null, so wird das eindeutig bestimmte normierte Polynom, das zu d assoziiert ist, mit dem Symbol $\mathrm{ggT}(f,g)$ bezeichnet. Der Vollständigkeit halber ist noch $\mathrm{ggT}(0,0) := 0$ zu setzen. 2/4/12
$\mathrm{ggT}(f,g)$ heißt von nun an *der* größte gemeinsame Teiler von f und g.

Offensichtlich ist $\mathrm{ggT}(f,0) \sim f$.

Bemerkung – Bezeichnung. (ggT *als Vielfachensumme*)

Vollkommen analog zum bisher verwendeten Begriff lässt sich der größte gemeinsame Teiler für mehr als zwei Polynome definieren, und es ergibt sich, dass zu beliebigen $f_1, \ldots, f_n \in K[X]$ Polynome $q_1, \ldots, q_n \in K[X]$ existieren, die der Gleichung

$$\mathrm{ggT}(f_1, \ldots, f_n) = q_1 f_1 + \ldots + q_n f_n$$

genügen.

Wir wissen bereits, dass für $f, g \in K[X]$ der größte gemeinsame Teiler stets existiert, und $\mathrm{ggT}(f,g) = pf + qg$ mit geeigneten Polynomen $p, q \in K[X]$.

Der Beweis des Hauptresultats in diesem Abschnitt beruht auf dem folgenden Satz, der ebenso bewiesen wird wie die analoge Aussage in 1/2/27.

Satz. (*Lemma von Euklid*) 2/4/13

Ist $p \in K[X]$ *irreduzibel, so gilt für beliebige Polynome* $f, g \in K[X]$:
$p|(f \cdot g) \implies p|f \ \vee \ p|g$.

Jedes nicht konstante Polynom ist ein Produkt irreduzibler Polynome, denn falls ein echter Teiler existiert, hat dieser einen kleineren Grad, woraus sich induktiv die Existenz einer solchen Faktorzerlegung ergibt. 2/4/14
Nun folgt ein vertrauter Schluss: Sind $p_1 \cdot \ldots \cdot p_m = q_1 \cdot \ldots \cdot q_n$ zwei Zerlegungen desselben Polynoms in irreduzible Faktoren p_i bzw. q_j, so muss nach dem Lemma von Euklid p_1 eines der Polynome q_j teilen. Da p_1 keine Einheit ist, folgt $p_1 \sim q_j$. Wir erhalten induktiv $m = n$ und nach Permutation der q_j auch $p_i \sim q_i$ für $i = 1, \ldots, m$, damit also den folgenden

Satz. (*Faktorzerlegung in* $K[X]$)

Jedes Polynom $f \in K[X] \setminus K$ *ist Produkt irreduzibler Polynome; diese sind bis auf Reihenfolge und Multiplikation mit Elementen aus* K^* *eindeutig bestimmt.*

Endliche algebraische Körpererweiterungen* 2/4/15

Die zuvor behandelte Teilbarkeitslehre in $K[X]$ hilft bei der Konstruktion bisher nicht betrachteter Typen von Erweiterungskörpern, die im Fall $K = \mathbb{Q}$ auch *algebraische Zahlkörper* heißen.
Der anspruchsvollere Leser findet hier eine Einführung – für die erste Anwendungen bei der Klassifikation von Endomorphismen reicht jedoch auch die vereinfachte Fassung dieser Texte (wählen Sie die Option „vereinfacht" = 3).
Ausgangspunkt ist das folgende Problem:
Ein Polynom $f \in K[X] \setminus K$ muss nicht immer eine Nullstelle in K besitzen. Können wir nach Körpererweiterung stets eine solche finden?

Für einen Unterkörper K der komplexen Zahlen folgt das aus dem Fundamentalsatz der Algebra. Ist z.B. $f = x^2 - 2 \in \mathbb{Q}[X]$, so genügt es, den Erweiterungskörper $K' = \{a + b\sqrt{2}\,|\,a, b \in \mathbb{Q}\} \subseteq \mathbb{R}$ von $\mathbb{Q}$ zu wählen. Allgemein lässt sich zu $f \in K[X] \setminus K$ ein „kleinster" Körper $K' \supseteq K$ konstruieren, für den f (als Element von $K'[X]$) in Linearfaktoren zerfällt; dies ist der *Zerfällungskörper* von f. Er ist dem exakten Rechnen (z.B. mit einem Computer) besser zugänglich als die Körper $\mathbb{R}$ oder $\mathbb{C}$, sofern die Operationen in K beherrscht werden.
Da die genannten Spezialfälle bereits für viele der späteren Anwendungen ausreichen, kann der weitere Text auch ohne die anschließend erläuterte Konstruktion des Zerfällungskörpers verstanden werden – beispielsweise dann, wenn Ihnen die Untersuchung von Vektorräumen über dem Grundkörper der reellen oder der komplexen Zahlen genügt. Auf die Bemerkungen zu mehrfachen Nullstellen in Erweiterungskörpern (vgl. 2/4/20 und 2/4/21) sollte jedoch nicht verzichtet werden.

Lemma 1 (*Ideale in* $K[X]$)

Jedes Ideal $\boldsymbol{a}$ *im Polynomring* $K[X]$ *einer Unbestimmten über dem Körper* K *ist Hauptideal, d.h. es existiert ein Polynom* $f \in K[X]$, *für das* $\boldsymbol{a} = (f)$ *gilt. Im Fall* $\boldsymbol{a} \neq \boldsymbol{0}$ *ist* f *ein Polynom kleinsten Grades unter den von* 0 *verschiedenen Elementen in* $\boldsymbol{a}$ (*und bis auf Multiplikation mit Elementen aus* K^* *eindeutig bestimmt*).

Beweis. O.B.d.A. ist $\boldsymbol{a} \neq \boldsymbol{0}$. Wird $f \in \boldsymbol{a} \setminus \{0\}$ von minimalem Grad gewählt, so gilt für ein beliebiges Element $h \in \boldsymbol{a}$ offensichtlich $h = qf + r$ mit geeigneten Polynomen $q, h \in K[X]$, $\deg(r) < \deg(f)$ (Division mit Rest). Aus $r = h - qf \in \boldsymbol{a}$ folgt wegen der Minimalität von $\deg(f)$ überdies $r = 0$, daher $h = qf$ und wir erhalten $\boldsymbol{a} \subseteq (f)$. Die Inklusion $\boldsymbol{a} \supseteq (f)$ ist trivial. ❑

$K' \supseteq K$ sei nun ein Erweiterungskörper des Grundkörpers K und $\alpha \in K'$ Nullstelle eines nichtkonstanten Polynoms aus $K[X]$. Die durch α erzeugte K-Algebra $K[\alpha]$ ist ein Unterring von K', der als Bild des Einsetzungshomomorphismus

$$\varphi : K[X] \to K', \quad X \mapsto \alpha$$

entsteht (vgl. 1/2/18). Anschließend wird gezeigt, dass $K[\alpha]$ unter der obigen Voraussetzung sogar ein Körper ist, der *durch* α *erzeugte Unterkörper* des Körpers K'.

$\mathbb{Q}[\sqrt[3]{2}] = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in \mathbb{Q}\}$ ist durch die Nullstelle $\sqrt[3]{2}$ des (nach 2/4/10 Beisp. 2 über $\mathbb{Q}$ irreduziblen) Polynoms $X^3 - 2$ erzeugt.

Zunächst ergibt sich nach dem Homomorphiesatz für Ringe

$$K[\alpha] = \mathrm{im}(\varphi) \cong K[X]/\ker(\varphi).$$

Das Ideal $\boldsymbol{a} := \ker(\varphi) = \{f \in K[X] \mid f(\alpha) = 0\}$ enthält nach Lemma 1 ein eindeutig bestimmtes normiertes Polynom $p \neq 0$ von kleinstem Grad, es heißt *Minimalpolynom* von α und erzeugt das Ideal $\boldsymbol{a}$. Das Minimalpolynom

Wir merken uns: Das *Minimalpolynom* ist normiert, irreduzibel und dadurch eindeutig bestimmt unter den Polynomen mit einer gegebenen Nullstelle.

ist stets irreduzibel, denn aus $p = g\cdot h$ folgt durch Einsetzen $0 = p(\alpha) = g(\alpha)\cdot h(\alpha)$, daher $g(\alpha) = 0$ oder $h(\alpha) = 0$ im Körper K', d.h. $g \in \boldsymbol{a}$ oder $h \in \boldsymbol{a}$ und folglich $p|\, g$ oder $p|\, h$. Wir erhalten $p \sim g$ oder $p \sim h$.

Für das Minimalpolynom p gilt $K[\alpha] \cong K[X]/(p)$. Dass jedes normierte, irreduzible Polynom als Minimalpolynom auftreten kann, entnehmen wir dem folgenden

Lemma 2 *Für jedes irreduzible Polynom $p \in K[X]$ ist der Faktorring $K[X]/(p)$ ein Körper.* 2/4/16

Beweis. Es ist zu zeigen, dass für jede von $\overline{0}$ verschiedene Klasse $\overline{f} \in K[X]/(p)$ ein inverses Element bezüglich der Multiplikation existiert. Da $f \notin (p)$, sind f und p teilerfremd, also $g \cdot f + h \cdot p = 1$ für geeignete Polynome $g, h \in K[X]$; nach Übergang zu den Klassen folgt aus $\overline{h\cdot p} = \overline{0}$ sofort $\overline{f} \cdot \overline{g} = \overline{1}$ im Faktorring $K[X]/(p)$. ❑

Durch die Komposition $K \to K[X] \to K[X]/(p)$ des Strukturmorphismus von $K[X]$ mit dem kanonischen Homomorphismus wird $K[X]/(p)$ zur K-Algebra. Ihr Strukturmorphismus ist injektiv, denn der Kern eines Ringhomomorphismus ist stets ein Ideal, und der Körper K besitzt außer $\mathbf{0}$ nur das Ideal K, das wegen $1 \mapsto 1$ nicht als Kern infrage kommt. Die Injektivität von $K \to K[X]/(p)$ gibt wieder Anlass, den Körper K mit seinem Bild in $K[X]/(p)$ zu identifizieren.

Satz. 2/4/17

(1) *Für alle irreduziblen Polynome $p \in K[X]$ existiert ein Erweiterungskörper $K' = K[\alpha]$ von K, der durch eine Nullstelle $\alpha \in K'$ von p erzeugt wird.*

(2) *Ist $K'' \supseteq K$ ein Erweiterungskörper und $\alpha \in K''$ Nullstelle eines irreduziblen Polynoms $p \in K[X]$, so ist $K[\alpha]$ als K-Algebra zum Körper $K[X]/(p)$ isomorph, d.h. im Wesentlichen eindeutig bestimmt.*

Beweis. Zu (1) genügt es, in der vorhergehenden Überlegung $\alpha = \overline{X}$ als Klasse von X im Faktorring $K[X]/(p)$ zu wählen.
(2) folgt aus dem Homomorphiesatz entsprechend der Anmerkung nach Lemma 1. ❑

Nun sind beliebige Polynome $f \in K[X] \setminus K$ Produkte irreduzibler Polynome. Ist α Element eines Erweiterungskörpers von K, so ist die Bedingung $f(\alpha) = 0$ äquivalent dazu, dass α Nullstelle (mindestens) eines der irreduziblen Faktoren ist. Es folgt

Korollar. (*Satz von Kronecker*) 2/4/18

Jedes nichtkonstante Polynom aus $K[X]$ besitzt eine Nullstelle in einem geeigneten Erweiterungskörper von K.

Durch induktive Anwendung des Satzes auf alle Nullstellen eines Polynoms ergibt sich die Existenz eines Körpers, in dem es in Linearfaktoren zerfällt.

Korollar – Definition. (*Zerfällungskörper*) 2/4/19

Ist $f \in K[X]$ ein nichtkonstantes Polynom, so existiert ein Erweiterungskörper Q von K, über dem f in ein Produkt linearer Polynome zerfällt. Sind

Natürlich wird damit klar, dass der Zerfällungskörper der kleinste Unterkörper von Q ist, der alle Nullstellen α_i enthält.

$\alpha_1, \ldots, \alpha_t$ alle Nullstellen von f in Q, so ist $K' = K[\alpha_1, \ldots, \alpha_t] \subseteq Q$ ein Unterkörper, er heißt *Zerfällungskörper* des Polynoms f.
Ein Zerfällungskörper von f ist als K-Algebra bis auf Isomorphie eindeutig bestimmt.

Beweis. Die Existenz von K' ergibt sich aus der vorhergehenden Überlegung; wir zeigen die Eindeutigkeit.
Dazu betrachten wir Tripel (K, f, K'), bestehend aus einem Körper K, einem nichtkonstanten Polynom $f \in K$ und einer K-Algebra K', die Zerfällungskörper von $f \in K[X]$ ist.
Es genügt zu zeigen:

$(*)$ Ist (K, f, K') ein solches Tripel, dann existiert für jedes weitere Tripel (K, f, K'_1) mit den zuvor angegebenen Eigenschaften ein Isomorphismus $K' \to K'_1$ von K-Algebren.

Der Beweis wird durch vollständige Induktion über die Anzahl $\mathrm{n}(K, f, K') := |\{\alpha \mid \alpha \in K' \setminus K \,, f(\alpha) = 0\}|$ der nicht in K liegenden Nullstellen von f erbracht.
Der Fall $\mathrm{n}(K, f, K') = 0$ ist trivial, da dann $K = K'$ folgt.
Es sei $n > 0$. Wir setzen induktiv voraus, $(*)$ sei für jedes Tripel (K, f, K') mit $\mathrm{n}(K, f, K') < n$ erfüllt.
Wir fixieren eine Nullstelle $\alpha_1 \in K' \setminus K$ von f. (K, f, K'_1) sei ein weiteres Tripel der genannten Art, d.h. K'_1 ebenfalls Zerfällungskörper von f. Wir wählen nun eine Nullstelle $\beta \in K'_1$ des Minimalpolynoms von α_1. Nach Satz 2/4/17 lässt sich ein K-Isomorphismus $\varphi : K[\alpha_1] \to K[\beta]$ finden, für den das folgende Diagramm kommutiert.

Das Minimalpolynom von α_1 ist natürlich ein Teiler von f.

$$\begin{tikzcd}
& K \arrow[dl, "\subseteq"'] \arrow[dr, "\subseteq"] & \\
K[\alpha_1] \arrow[rr, "\varphi"] \arrow[d, "\subseteq"'] \arrow[drr, dotted, "\eta"] & & K[\beta] \arrow[d, "\subseteq"] \\
K' \arrow[rr, dotted, "\psi"] & & K'_1
\end{tikzcd}$$

Nun ist K' offensichtlich Zerfällungskörper des Polynoms f, betrachtet als Element von $(K[\alpha_1])[X]$ und es gilt $\mathrm{n}(K[\alpha_1], f, K') < n$. Ebenso können wir die durch η definierte $K[\alpha_1]$-Algebra K'_1 als Zerfällungskörper von f ansehen. Aus der Induktionsvoraussetzung folgt daher die Existenz eines Isomorphismus $\psi : K' \to K'_1$ von $K[\alpha_1]$-Algebren. ❏

Der injektive Homomorphismus η wird als Inklusion verstanden.

Obwohl ein Zerfällungskörper nur bis auf Isomorphie eindeutig ist, wird oft nachlässig von *dem* Zerfällungskörper gesprochen.

Ist $K = \mathbb{R}$ der Körper der reellen Zahlen, so hat ein Polynom $f \in \mathbb{R}[X]$ als Zerfällungskörper entweder den Körper $\mathbb{R}$ selbst (f zerfällt in reelle Linearfaktoren) oder den Körper $\mathbb{C}$ der komplexen Zahlen (falls f eine nichtreelle Nullstelle besitzt).

In vielen Fällen lassen sich Aussagen über den Zerfällungskörper machen, 2/4/20

ohne ihn „explizit“ anzugeben.
Die folgende, über beliebigen Grundkörpern ausführbare Konstruktion heißt auch *formales Differenzieren.*

Bemerkung – Definition. (*Ableitung eines Polynoms*)
Ist $f = \sum_{i=0}^{n} a_i X^i \in K[X]$, so setzen wir

$$f' := \sum_{i=1}^{n} i a_i X^{i-1}$$

und nennen das Polynom f' *Ableitung* von f. Die durch

$$\frac{\mathrm{d}}{\mathrm{d}X} : K[X] \to K[X], \quad f \mapsto \frac{\mathrm{d}f}{\mathrm{d}X} := f'$$

definierte Abbildung hat dann folgende Eigenschaften:

(1) $f' = 0$ falls f konstant ist, d.h. wenn $f \in K$.

(2) $(f+g)' = f' + g'$ für $f, g \in K[X]$.

(3) $(f \cdot g)' = f' \cdot g + f \cdot g'$ für $f, g \in K[X]$ (*Produktregel*), insbesondere gilt

$(a \cdot f)' = a \cdot f'$ für $a \in K$.

Die Definition ergibt über dem reellen oder komplexen Grundkörper Abbildungen, die dem gleichnamigen Begriff aus der Analysis entsprechen.
Vorsicht ist geboten, wenn ein Exponent durch die Charakteristik des Grundkörpers teilbar ist; so gilt beispielsweise $f' = 0$ für das nichtkonstante Polynom $f = X^2 \in \mathbb{F}_2[X]$.

Bemerkung. (*mehrfache Nullstellen in Erweiterungskörpern*) 2/4/21
Ist $K' \supseteq K$ ein Erweiterungskörper, in dem das nichtkonstante Polynom $f \in K[X]$ in Linearfaktoren zerfällt, so besitzt f in K' genau dann keine mehrfache Nullstelle, wenn $\mathrm{ggT}(f, f') = 1$.

Beweis. Der euklidische Algorithmus zeigt, dass der größte gemeinsame Teiler zweier Polynome über K derselbe ist, wenn er über einem Erweiterungskörper von K bestimmt wird. Die nachfolgende Rechnung wird in $K'[X]$ ausgeführt.

Zunächst zeigen wir ($\Leftarrow$): Ist a eine mehrfache Nullstelle von f, d.h. $f = (X-a)^2 \cdot g$ mit $a \in K'$ und $g \in K'[X]$, so folgt

$$f' = 2 \cdot (X-a) \cdot g + (X-a)^2 \cdot g', \quad \text{daher} \quad (X-a) \mid \mathrm{ggT}(f, f'), \quad ⚡.$$

($\Rightarrow$): Es sei $\mathrm{ggT}(f, f') \neq 1$. f ist über K' Produkt linearer Polynome, daher existiert für f und f' eine gemeinsame Nullstelle $a \in K'$.
Aus $f' = (X-a) \cdot h$ und $f = (X-a) \cdot g$ folgt

$$(X-a) \cdot h = \big((X-a) \cdot g\big)' = g + (X-a) \cdot g',$$

daher $(X-a) \mid g$, d.h. $(X-a)^2 \mid f$, ⚡. ❑

Die Bemerkung 2/4/21 erlaubt es, ohne Kenntnis der Nullstellen konstruktiv zu prüfen, ob ein Polynom in wenigstens einer der Erweiterungen des Grundkörpers mehrfache Nullstellen besitzt.

Schwerpunkte zum gewählten Stoff

- Leitmonome, Division mit Rest [2/4/1 – 2/4/2]
- Euklidischer Algorithmus (Kettendivision) für Polynome einer Unbestimmten [2/4/1 – 2/4/4]
- Nullstellen von Polynomen in einer Unbestimmten (Ausklammern von Linearfaktoren, Multiplizität einer Nullstelle) [2/4/5 – 2/4/7]
- Identitätssatz für Polynome [2/4/8]
- Irreduzible Faktoren reeller bzw. komplexer Polynome [2/4/9]
- Beispiele irreduzibler Polynome [2/4/10]
- Existenz und Eindeutigkeit der Faktorzerlegung in $K[X]$ [2/4/11 – 2/4/14]
- Zerfällungskörper eines Polynoms [2/4/15]
- *Im Polynomring $K[X]$ einer Unbestimmten über dem Körper K ist jedes Ideal Hauptideal [2/4/15]
- *Faktorringe nach irreduziblen Polynomen aus $K[X]$ sind Körper [2/4/16]
- *Satz von Kronecker, Existenz und Eindeutigkeit des Zerfällungskörpers eines Polynoms [2/4/17 – 2/4/19]
- Die formale Ableitung eines Polynoms und mehrfache Nullstellen in Erweiterungskörpern [2/4/20 – 2/4/21]

Sachverzeichnis