Irreduzibles Polynom

In der Algebra, einem Teilgebiet der Mathematik, ist ein **irreduzibles Polynom** ein Polynom, das sich nicht als Produkt zweier nicht invertierbarer Polynome schreiben lässt und somit nicht in „einfachere“ Polynome zerfällt. Ihre Bedeutung für die Polynomringe ist in den meisten Fällen (Polynome über faktoriellen Ringen) mit der Bedeutung von Primzahlen für natürliche Zahlen gleich.

Inhaltsverzeichnis

Definition

Die Definition lässt sich bereits für Integritätsringe formulieren. Es ist bekannt, dass der Polynomring über einem Integritätsring selbst nullteilerfrei ist. Dies ist der Grund, dass die Definitionen von irreduziblen Elementen übernommen werden kann. Da in vielen Fällen nur Körper behandelt werden und die Definition dort einfacher ist, wird auch die Definition für diesen Spezialfall aufgeführt. In der allgemeinen Definition kann man sich trivialerweise auf eine Variable beschränken.

Definition allgemein für Integritätsringe

Es sei R ein Integritätsring. Dann heißt ein Polynom $f \in R[X]$ irreduzibel, wenn $f \neq 0$ nicht invertierbar in $R[X]$ ist und für $g, h \in R[X]$ und $f = gh$ entweder g oder h invertierbar ist.

Definition speziell für Körper

Es sei K ein Körper. Dann heißt ein Polynom $P \in K[X_1, \ldots, X_n]$ aus dem Polynomring in n Unbestimmten irreduzibel, wenn P nicht konstant ist und es keine nichtkonstanten Polynome $Q, R \in K[X_1, \ldots, X_n]$ gibt, so dass $P = Q \cdot R$ gilt. Falls solche Polynome existieren, so heißt P auch **reduzibel** oder zerlegbar.

Eine äquivalente Beschreibung lautet: Irreduzible Polynome sind genau die irreduziblen Elemente im Ring $K[X_1, \ldots, X_n]$.

Primpolynome und irreduzible Polynome im Vergleich

Ein Polynom $f \in R[X]$ heißt prim oder Primpolynom, wenn für alle $g, h \in R[X]$ mit der Eigenschaft $f|gh$ folgt: $f|g$ oder $f|h$. Ist der Ring sogar faktoriell, so ist auch $R[X]$ faktoriell (Satz von Gauß). Insbesondere sind alle Körper faktoriell und damit auch die zugehörigen Polynomringe.

Für Polynome über faktoriellen Ringen (also auch für Polynome über einem Körper) sind Primelemente auch irreduzible Elemente und umgekehrt. Es gilt zudem eine bis auf Assoziiertheit eindeutige Zerlegung von Polynomen in Primpolynome.

Es lassen sich in diesen faktoriellen Ringen die Irreduzibilität von Polynomen auch auf die Irreduzibilität von Polynomen über dem Quotientenkörper zurückführen. Dieses Problem ist aber nicht zwangsläufig einfacher zu lösen. Man beachte dazu, dass ein Polynom aus einem faktoriellen Ring R genau dann prim ist, wenn das Polynom entweder konstant einem Primelement ist, oder irreduzibel und primitiv (d. h. größter gemeinsamer Teiler aller Koeffizienten ist 1) in dem Quotientenkörper über R.

Irreduzibilitätskriterien

In sehr vielen Bereichen kommen Polynome in einer Variablen vor, deren Irreduzibilität weitere Folgerungen möglich macht, z. B. grundlegend in der Galoistheorie und exemplarisch als Anwendung das chromatische Polynom in der Graphentheorie. *(Siehe auch Minimalpolynom).* Wichtig ist es deshalb, einfache Entscheidungskriterien für die Irreduzibilität zur Hand zu haben.

Das Irreduzibilitätskriterium von Eisenstein

Das Eisensteinkriterium ist ein hinreichendes (aber nicht notwendiges) Kriterium für die Irreduzibilität eines Polynoms in einer erweiterten Koeffizientenmenge. Sei dazu A ein Integritätsring, $P = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0 \in A[X] \text{ mit } a_n \neq 0 \text{ und } n > 0$ ein Polynom mit Koeffizienten aus A und K der Quotientenkörper von A. Findet man ein Primelement $p \in A$, so dass gilt:

- $p \nmid a_n$,
- $p \mid a_i$ für $i = 0, 1, 2, \ldots, n-1$ sowie
- $p^2 \nmid a_0$,

dann ist P irreduzibel über $K[X]$. Es wird häufig angewendet für $A = \mathbb{Z}$ und $K = \mathbb{Q}$. Man kann die Bedingung der Teilbarkeit durch das Primelement p auch überall durch Enthaltensein in einem Primideal von A ersetzen.

Ist A faktoriell und das Polynom P primitiv, d. h. der größte gemeinsame Teiler aller Koeffizienten ist 1, dann ist P auch in $A[X]$ irreduzibel.

Reduktionskriterium

Es sei wieder A ein Integritätsring mit Quotientenkörper K und $p \in A$ ein Primelement. Ein Polynom $f = \sum_{k=0}^{n} a_k X^k \in A[X]$ mit $p \nmid a_n$ ist dann (nicht notwendigerweise genau dann) irreduzibel in $K[X]$, wenn das Polynom mit den modulo p reduzierten Koeffizienten in $A/pA[X]$ irreduzibel ist.

Beispiele

- Über Körpern gilt:
  - Jedes Polynom vom Grad 1 ist irreduzibel. Besitzt ein irreduzibles Polynom eine Nullstelle, so hat es Grad 1.
  - Insbesondere hat jedes irreduzible Polynom über einem algebraisch abgeschlossenen Körper wie $\mathbb{C}$ Grad 1.
  - Jedes Polynom über K vom Grad 2 oder vom Grad 3 ist genau dann irreduzibel, wenn es keine Nullstelle in K hat.[1]
- Jedes irreduzible Polynom über den reellen Zahlen hat Grad 1 oder 2, folglich entweder die Form $aX + b$ mit $a \neq 0$ oder $aX^2 + bX + c$ mit $b^2 - 4ac < 0$. Das hängt damit zusammen, dass der algebraische Abschluss $\mathbb{C}$ Grad 2 über $\mathbb{R}$ hat.

- $f(X) \in \mathbb{Z}[X]$ irreduzibel über $\mathbb{Z} \Leftrightarrow f(X) = \pm p$ für eine Primzahl aus $\mathbb{Z}$, oder $f(X)$ ist primitiv und irreduzibel über $\mathbb{Q}[X]$

- $X^p - X + 1 \in \mathbb{F}_p[X]$ ist irreduzibel. Um dies einzusehen, zeigt man, dass alle irreduziblen Faktoren $r_1(X) \cdot r_2(X) \cdots r_k(X)$ des Polynoms den gleichen Grad haben. Da p prim ist, muss das Polynom dann entweder irreduzibel sein, oder in Linearfaktoren zerfallen. Letzteres kann aber nicht sein, da das Polynom $\mathbb{F}_p$ keine Nullstelle besitzt. Um nun zu zeigen, dass all $r_i(X)$ den gleichen Grad haben, kann man eine Nullstelle α im Zerfällungskörper des Polynoms betrachten. Da das Polynom invariant unter der von $X \mapsto X + 1$ induzierten Abbildung ist, sind auch $\alpha + 1, \ldots, \alpha + p - 1$ Nullstellen. Im Zerfällungskörper hat das Polynom also die Gestalt $(X - \alpha)(X - (\alpha + 1)) \cdots (X - (\alpha + p - 1))$. Für jeden irreduziblen Faktor $r_i(X)$ gibt es somit ein $s \in \mathbb{F}_p$, so dass α Nullstelle des verschobenen Polynoms $r_i'(X) := r_i(X + s)$ ist. Mit $r_i(X)$ ist auch $r_i'(X)$ irreduzibel, d. h. alle irreduziblen Faktoren $r_j(X)$ haben den gleichen Grad wie das Minimalpolynoms von α.

- Das Polynom $8X^7 + 7X^4 + 21X^2 - 15X + 22 \in \mathbb{Z}[X]$ ist irreduzibel, denn es ist primitiv und ein irreduzibles Polynom in den rationalen Zahlen. Man wende dazu das Reduktionskriterium an. Das Polynom mit den reduzierten Koeffizienten modulo 7 ist dabei $X^7 - X + 1 \in \mathbb{F}_7[X]$, und dies ist irreduzibel.

- $2X^5 + 30X^3 - 60X^2 + 90 \in \mathbb{Q}[X]$ ist irreduzibel. Dies folgt aus dem Eisensteinkriterium nur mit dem Primelement $p = 5$.

- Für eine Primzahl p ist das Polynom $X^n - p$ für $n \in \mathbb{N}$, $n \geq 1$, irreduzibel über $\mathbb{Q}$. Das Minimalpolynom von $\sqrt[n]{p}$ über $\mathbb{Q}$ ist also $X^n - p$. Als Folgerung ergibt sich beispielsweise, dass die Quadratwurzel aus 2 eine irrationale Zahl ist (oder eine n-te Wurzel aus einer Primzahl mit $n > 0$).

- $X^p - Y \in \mathbb{F}_p[X, Y]$ (oder als Element aus $(\mathbb{F}_p(Y))[X]$ - man beachte, dass es primitiv ist.) ist irreduzibel (Eisensteinsches Kriterium). Das Primelement ist dabei $Y \in \mathbb{F}_p[Y]$. Dieses Polynom ist allerdings nicht separabel, d. h., es hat im algebraischen Abschluss von $\mathbb{F}_p(Y)$ eine mehrfache Nullstelle. Dieses Phänomen tritt nicht in $\mathbb{Q}$ auf.

Literatur

- Christian Karpfinger, Kurt Meyberg: *Algebra. Gruppen – Ringe – Körper* 2. Auflage. Spektrum Akademischer Verlag, Heidelberg 2010, ISBN 978-3-8274-2600-0, Kapitel 18.

Weblinks

- MathWorks: Factor a polynomial into irreducible polynomials

Einzelnachweise

1. Ed Dubinsky, Uri Leron: *Learning abstract algebra with ISETL*. S. 232 (Satz 6.17).