KAPITEL 3

Der algebraische Abschluss eines Körpers

Das folgende Ergebnis kennen wir bereits:

SATZ. *Ist K ein Körper und $f \in K[x]$ ein Polynom vom Grad ≥ 1, so gibt es eine endliche Körpererweiterung $L|K$, sodass f eine Nullstelle in L besitzt, d.h. es gibt ein $\alpha \in L$ mit $f(\alpha) = 0$. Man kann $L = K(\alpha)$ wählen.*

Beweis: Wenn wir die Behauptung für einen irreduziblen Teiler von f beweisen, dann folgt das Ergebnis natürlich für allgemeines f. Daher können wir o.E. annehmen, dass f irreduzibel ist. Wählen wir nun $L = K[x]/(f)$, ist α das Bild von x in L, so gilt $f(\alpha) = 0$. Dies beweist die Behauptung. ■

SATZ. *Ist K ein Körper und $f \in K[x]$ ein Polynom vom Grad ≥ 1, so gibt es eine endliche Körpererweiterung $Z|K$, sodass f über Z in Linearfaktoren zerfällt, d.h. es gibt $c \in K$ und $\alpha_1, \ldots, \alpha_n \in L$ mit*

$$f(x) = c(x - \alpha_1) \ldots (x - \alpha_n)$$

und

$$Z = K(\alpha_1, \ldots, \alpha_n)$$

gilt. Z heißt **Zerfällungskörper** *von f über K.*

Beweis: Nach dem letzten Satz finden wir einen Oberkörper L_1 von K und ein $\alpha_1 \in L$ mit $f(\alpha_1) = 0$. Dann können wir in $L_1[x]$ zerlegen $f(x) = (x - \alpha_1)f_1(x)$ mit $f_1 \in L_1[x]$. Ist f_1 nicht konstant, finden wir einen Oberkörper L_2 von L_1 und ein $\alpha_2 \in L_2$ mit $f_1(\alpha_2) = 0$. Über L_2 können wir zerlegen $f_1(x) = (x-\alpha_2)f_2(x)$ mit $f_2 \in L_2[x]$. Nach endlich vielen Schritten erhalten wir einen Oberkörper L_n und eine Zerlegung

$$f(x) = c(x - \alpha_1)(x - \alpha_2) \ldots (x - \alpha_n) \text{ mit } \alpha_1, \ldots, \alpha_n \in L_n.$$

Natürlich gilt die Zerlegung auch schon in

$$Z = K(\alpha_1, \ldots, \alpha_n) \subseteq L_n.$$

Es folgt die Behauptung. ■

$$\begin{array}{ccccc}
K(\alpha_1, \ldots, \alpha_n) & \subseteq & L_n & & f(x) = (x - \alpha_1) \ldots (x - \alpha_n) \\
\vdots & & \vdots & & \\
K(\alpha_1, \alpha_2) & \subseteq & L_2 & & f(x) = (x - \alpha_1)(x - \alpha_2)f_2(x) \\
| & & | & & \\
K(\alpha_1) & \subseteq & L_1 & & f(x) = (x - \alpha_1)f_1(x) \\
| & & | & & \\
K & = & K & & f(x)
\end{array}$$

Beispiele:

---

(1) Über $K = \mathbb{Q}$ betrachten das Polynom $f = (x^2-2)(x^2+1)$. Die Nullstellen in $\mathbb{C}$ sind offensichtlich $\pm\sqrt{2}$ und $\pm i = \pm\sqrt{-1}$. Wir erhalten die Zerlegung

$$f = (x-\sqrt{2})(x+\sqrt{2})(x-i)(x+i).$$

Zerfällungskörper ist offensichtlich

$$Z = \mathbb{Q}(\sqrt{2}, i).$$

(2) Wir betrachten $f = x^4 - 4 \in \mathbb{Q}[x]$. In $\mathbb{C}$ finden wir die Zerlegung

$$\begin{aligned} f &= x^4 - 4 = (x^2-2)(x^2+2) = (x^2-\sqrt{2}^2)(x^2 - i^2\sqrt{2}^2) = \\ &= (x-\sqrt{2})(x+\sqrt{2})(x-i\sqrt{2})(x+i\sqrt{2}). \end{aligned}$$

Also ist

$$\mathbb{Q}(\sqrt{2}, i)$$

ein Zerfällungskörper von $x^4 - 4$.

FOLGERUNG. *Sei K ein Körper und $f_1, \ldots, f_n \in K[x]$ Polynome vom Grad ≥ 1. Dann gibt es eine endliche Körpererweiterung $L|K$, sodass alle Polynome f_i in $L[x]$ in Linearfaktoren zerfallen.*

Beweis: Man wende den vorangegangenen Satz auf das Produktpolynom $f(x) = f_1(x)f_2(x)\ldots f_n(x) \in K[x]$ an. Der Zerfällungskörper von f kann als Körper L gewählt werden. ■

Gibt es auch eine Körpererweiterung von K, in der alle nichtkonstanten Polynome in Linearfaktoren zerfallen? Ein solches Phänomen kennen wir vom Körper der komplexen Zahlen $\mathbb{C}$.

DEFINITION. *Ein Körper K heißt* **algebraisch abgeschlossen**, *wenn eine der folgenden äquivalenten Bedingungen erfüllt ist:*

(1) *Jedes Polynom $f \in K[x]$ vom Grad ≥ 1 hat eine Nullstelle in K.*
(2) *Jedes Polynom $f \in K[x]$ vom Grad ≥ 1 zerfällt in Linearfaktoren, d.h. es gibt $c \in K^*$ und $\alpha_1, \ldots, \alpha_n \in K$ mit*
$$f = c(x-\alpha_1)\ldots(x-\alpha_n).$$
(3) *K besitzt keine echten algebraischen Erweiterungen, d.h. ist $L|K$ eine algebraische Körpererweiterung, so gilt schon $L = K$.*

Beweis der Äquivalenz der Bedingungen in der Definition:

- (1)$\Longrightarrow$(2) Hat f eine Nullstelle $\alpha_1 \in K$, so erhalten wir durch Polynomdivision ein Polynom $f_2 \in K[x]$ mit $f(x) = (x-\alpha)\cdot f_2(x)$. Jetzt wenden wir das gleiche Verfahren auf f_2 an. Nach endlich vielen Schritten erhalten wir eine Darstellung
$$f(x) = (x-\alpha_1)(x-\alpha_2)\ldots(x-\alpha_n)\cdot c \text{ mit } c \in K^*.$$
- (2)$\Longrightarrow$(1) Dies ist klar.
- (2)$\Longrightarrow$(3) Sei $L|K$ eine algebraische Körpererweiterung. Sei $\alpha \in L$. Das Minimalpolynom $m_{\alpha,L} \in K[x]$ zerfällt in Linearfaktoren und hat α als Nullstelle, woraus sofort $\alpha \in K$ folgt. Damit ergibt sich $L = K$.
- (3)$\Longrightarrow$(1) K besitze keine echten algebraischen Erweiterungen. Sei $f \in K[x]$ ein Polynom vom Grad ≥ 1. Da wir eine Nullstelle von f suchen, können wir o.E. annehmen, dass f irreduzibel ist. Dann definiert $K[x]/(f)$ eine algebraische Körpererweiterung von K vom Grad $\text{grad}(f)$. Es folgt nach Voraussetzung $\text{grad}(f) = 1$, d.h. $f = c(x-\alpha)$ mit $c, \alpha \in K$. Dann ist $\alpha \in K$ eine Nullstelle von f. ■

SATZ (Fundamentalsatz der Algebra). *Der Körper $\mathbb{C}$ der komplexen Zahlen ist algebraisch abgeschlossen.*

Anmerkung zu verschiedenen Beweisen:

- Man kann den Satz mit funktionentheoretischen Methoden beweisen. Im Funktionentheorie-Buch von Freitag/Busam[1] sind mehrere Beweise zu finden.

[1] E. Freitag, R. Busam. Funktionentheorie 1. Vierte Auflage. Springer, 2006.

- Im „Buch der Beweise“[2] findet sich in Kapitel 21 ein Beweis, der nach Aussagen der Autoren nur einige elementare Eigenschaften von Polynomen und komplexen Zahlen verwendet.
- Wenn wir in der Vorlesung Galoistheorie behandeln, können wir den Satz auch mit algebraischen Methoden beweisen.

Der folgende Satz zeigt eine Möglichkeit, an einen algebraisch abgeschlossenen Körper zu kommen, wenn man bereits einen algebraisch abgeschlossenen Körper kennt.

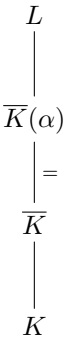
SATZ. *Sei K ein Körper und L ein algebraisch abgeschlossener Oberkörper von K, d.h. $K \subseteq L$. Sei*

$$\overline{K} = \{\alpha \in L : \alpha \text{ algebraisch über } K\}.$$

Dann ist $\overline{K}$ ein Körper, algebraisch abgeschlossen und algebraisch über K. (Der Körper $\overline{K}$ ist ein algebraischer Abschluss von K, wie nachfolgend definiert wird.)

Beweis:

- Wir haben bereits früher gezeigt, dass $\overline{K}$ ein Körper ist.
- Nach Konstruktion ist $\overline{K}$ algebraisch über K.
- Warum ist $\overline{K}$ algebraisch abgeschlossen? Sei $f \in \overline{K}[x]$ ein Polynom vom Grad ≥ 1. Wir müssen zeigen, dass f eine Nullstelle in $\overline{K}$ hat. Wegen $f \in L[x]$ gibt es ein $\alpha \in L$ mit $f(\alpha) = 0$. Dann ist α algebraisch über $\overline{K}$. Da $\overline{K}$ algebraisch über K ist, ist auch α algebraisch über K, also $\alpha \in \overline{K}$.



  Dies wollten wir zeigen. ■

DEFINITION. *Ein Körper $\overline{K}$ heißt ein* **algebraischer Abschluss** *eines Körpers K, wenn $\overline{K}$ ein algebraischer Oberkörper von K ist und algebraisch abgeschlossen ist.*

Beispiele:

(1) Da $\mathbb{C}$ algebraisch abgeschlossen ist, ist

$$\overline{\mathbb{Q}} = \{\alpha \in \mathbb{C} : \alpha \text{ algebraisch über } \mathbb{Q}\}$$

ein algebraischer Abschluss von $\mathbb{Q}$. ($\mathbb{C} \setminus \overline{\mathbb{Q}}$ ist die Menge der (über $\mathbb{Q}$) transzendenten Zahlen.)

(2) Da $\mathbb{C}$ algebraisch abgeschlossen ist und $\mathbb{C} = \mathbb{R}(i)$ algebraisch über $\mathbb{R}$ ist, ist $\mathbb{C}$ ein algebraischer Abschluss von $\mathbb{R}$.

Bemerkung: Man kann zeigen, dass $\mathbb{Q}$ und $\overline{\mathbb{Q}}$ abzählbar sind. Da $\mathbb{R}$ und damit auch $\mathbb{C}$ überabzählbar sind, folgt

$$\overline{\mathbb{Q}} \neq \mathbb{C}.$$

Leider ist nicht jeder Körper in natürlicher Weise in einem algebraisch abgeschlossenen Körper enthalten. Wir skizzieren jetzt einen Weg, wie man zu einem Körper einen algebraisch abgeschlossener Oberkörper konstruieren kann.

[2] M. Aigner, G. M. Ziegler. Das BUCH der Beweise. 5. Auflage. Springer, 2018.

LEMMA. *Sei K ein Körper. Dann gibt es einen Oberkörper L von K, sodass jedes Polynom $f \in K[x]$ vom Grad ≥ 1 eine Nullstelle in L hat.*

Beweis:

(1) Wir betrachten folgende Menge von Polynomen

$$M = \{f \in K[x] : \operatorname{grad}(f) \geq 1\}.$$

Jedem Polynom $f \in M$ ordnen wir eine Unbestimmte x_f zu und bilden den Polynomring (in unendlich vielen Unbestimmten)

$$R = K[\{x_f : f \in M\}].$$

(2) Wir betrachten das von den Polynomen $f(x_f)$ erzeugte Ideal in R:

$$\mathfrak{a} = (\{f(x_f) : f \in M\}) \subseteq R.$$

(a) Wir zeigen, dass $\mathfrak{a} \neq R$ gilt. Angenommen, es wäre $\mathfrak{a} = R$, dann wäre $1 \in \mathfrak{a}$, d.h. es gäbe endlich viele Polynome $f_1, \ldots, f_n \in M$ und Polynome $g_1, \ldots, g_n \in R$ mit

$$g_1 f(x_{f_1}) + \ldots g_n f(x_{f_n}) = 1.$$

Da die Polynome g_i natürlich nur endlich viele Unbestimmte x_f enthalten, können wir nach eventueller Vergrößerung von n annehmen, dass $g_1, \ldots, g_n$ Polynome in $x_{f_1}, \ldots, x_{f_n}$ sind. Wir schreiben $x_1 = x_{f_1}, \ldots, x_n = x_{f_n}$. Dann wird obige Gleichung zu

$$\sum_{i=1}^{n} g_i(x_1, \ldots, x_n) f_i(x_i) = 1.$$

(b) Nach einem vorangegangenen Satz gibt es eine Körpererweiterung $\widetilde{L}$, sodass $\alpha_1, \ldots, \alpha_n \in \widetilde{L}$ existieren mit

$$f_1(\alpha_1) = \cdots = f_n(\alpha_n) = 0.$$

Setzen wir jetzt $x_1 = \alpha_1, \ldots, x_n = \alpha_n$ in die Gleichung

$$\sum_{i=1}^{n} g_i(x_1, \ldots, x_n) f_i(x_i) = 1$$

ein, so erhalten wir einen Widerspruch.

Damit haben wir

$$\mathfrak{a} \subsetneq R$$

gezeigt.

(3) Nach der allgemeinen Theorie kommutativer Ringe gibt es ein maximales Ideal $\mathfrak{m}$ mit

$$\mathfrak{a} \subseteq \mathfrak{m} \subsetneq R.$$

Dann ist $L = R/\mathfrak{m}$ ein Körper. Die natürliche Abbildung $K \to R \to R/\mathfrak{m}$ ist injektiv, sodass wir K als Unterkörper von L auffassen können.

(4) Sei ξ_f das Bild von x_f in $R/\mathfrak{m}$. Aus $f(x_f) \in \mathfrak{a} \subseteq \mathfrak{m}$ folgt $f(x_f) \equiv 0 \bmod \mathfrak{m}$. Damit folgt $f(\xi_f) = 0$. Im Körper L hat also jedes Polynom $f \in K[x]$ vom Grad ≥ 1 eine Nullstelle. Dies wollten wir zeigen. ■

LEMMA. *Sei K ein Körper. Dann gibt es einen algebraisch abgeschlossenen Oberkörper L von K.*

Beweis:

(1) Wir starten mit $L_0 = K$ und konstruieren mit Hilfe des vorangegangenen Lemmas Körper L_i mit

$$L_0 \subseteq L_1 \subseteq L_2 \subseteq L_3 \subseteq L_4 \subseteq \ldots$$

Ist L_i bereits konstruiert, so finden wir mit dem vorangegangenen Lemma einen Oberkörper L_{i+1}, sodass jedes Polynom $f \in L_i[x]$ vom Grad ≥ 1 eine Nullstelle in L_{i+1} hat.

(2) Sei
$$L = \bigcup_{i=0}^{\infty} L_i.$$
L ist in natürlicher Weise ein Körper: Seien $\alpha, \beta \in L$.
- Es gibt einen Index i mit $\alpha, \beta \in L_i$. Dann sind in L_i die Elemente $\alpha + \beta$ und $\alpha\beta$ definiert, ebenso $\frac{1}{\alpha}$ im Fall $\alpha \neq 0$.
- Sind $\alpha, \beta \in L_j$ für einen anderen Index j, so ist auch in L_j $\alpha + \beta$ und $\alpha\beta$ definiert, was aber wegen $L_i \subseteq L_j$ oder $L_j \subseteq L_i$ zum selben Ergebnis führt.

(3) Wir wollen zeigen, dass L algebraisch abgeschlossen ist. Sei in $f \in L[x]$ ein Polynom vom Grad ≥ 1. Da f nur endliche viele Koeffizienten hat, gibt es einen Index i mit $f \in L_i[x]$. Dann gibt es aber ein $\alpha \in L_{i+1} \subseteq L$ mit $f(\alpha) = 0$. Also hat f eine Nullstelle in L. Es folgt die Behauptung. ■

FOLGERUNG. *Jeder Körper K besitzt einen algebraischen Abschluss $\overline{K}$, d.h. einen Oberkörper, der algebraisch abgeschlossen ist und algebraisch über K ist.*

SATZ. *Sei K ein Körper und $\overline{K}$ ein algebraischer Abschluss von K. Ist $L|K$ eine algebraische Körpererweiterung, so gibt es einen zu L isomorphen Zwischenkörper $\widetilde{L}$ der Körpererweiterung $\overline{K}|K$:*
$$L \simeq \widetilde{L} \quad \text{und} \quad K \subseteq \widetilde{L} \subseteq \overline{K}.$$
Wir können uns L also als Unterkörper von $\overline{K}$ vorstellen.

Beweis: Im nächsten Kapitel. ■

Bemerkung: Sei K ein endlicher Körper. Dann ist der natürliche Ringhomomorphismus $\mathbb{Z} \to K$ natürlich nicht injektiv. Der Kern ist ein Primideal (p) mit einer Primzahl p. Dadurch erhält man eine injektive Abbildung $\mathbb{F}_p = \mathbb{Z}/(p) \to K$, wir können also $\mathbb{F}_p$ als Teilmenge von K auffassen:
$$\mathbb{F}_p = \{0, 1, 2, \ldots, p-1\} \subseteq K.$$
K hat dann Charakteristik p.

SATZ. *Sei K ein endlicher Körper von Charakteristik p.*
(1) *Ist $[K : \mathbb{F}_p] = d$, so gilt $|K| = p^d$.*
(2) *Ist $\overline{\mathbb{F}}_p$ ein algebraischer Abschluss von $\mathbb{F}_p$, der K enthält, so gilt*
$$K = \{a \in \overline{\mathbb{F}}_p : a^{p^d} = a\}.$$

Beweis:

(1) Da K endlich ist, ist K eine endliche Erweiterung von $\mathbb{F}_p$. Ist $[K : \mathbb{F}_p] = d$ die Dimension von K als $\mathbb{F}_p$-Vektorraum, ist $\omega_1, \ldots, \omega_d \in K$ eine $\mathbb{F}_p$-Basis von K, so gilt
$$K = \{a_1\omega_1 + \cdots + a_d\omega_d : a_1, \ldots, a_d \in \mathbb{F}_p\}.$$
Daraus sieht man sofort $|K| = p^d$.

(2) Wir haben nun $\mathbb{F}_p \subseteq K \subseteq \overline{\mathbb{F}}_p$. Ist $a \in K \setminus \{0\}$, so ist $a^{|K|-1} = 1$, also $a^{p^d-1} = 1$ und damit
$$a^{p^d} = a.$$
Die Gleichung gilt auch für $a = 0$. Damit folgt
$$K \subseteq \{a \in \overline{\mathbb{F}}_p : a^{p^d} = a\}.$$
Da die Gleichung $x^{p^d} = x$ höchstens p^d Lösungen hat, gilt
$$|\{a \in \overline{\mathbb{F}}_p : a^{p^d} = a\}| \leq p^d,$$

woraus dann natürlich die Gleichung

$$K = \{a \in \overline{\mathbb{F}}_p : a^{p^d} = a\}$$

folgt. ■

Bemerkung: Teil (2) des vorangegangenen Satzes zeigt, dass es in $\overline{\mathbb{F}}_p$ höchstens einen Körper mit p^d Elementen gibt. Dass tatsächlich ein Körper existiert, werden wir später zeigen.