Algebra und Funktionentheorie

Nolite te bastardes carborundorum

Prof. Riddle

31.Oktober.1981

Inhaltsverzeichnis

1 Grundlagen der Körpertheorie

Körper (Definition) Ein Tripel (K, +, ·), wobei K eine Menge und $+ : K \times K \to K$ und $\cdot : K \times K \to K$ Verknüpfungen auf K sind, heißt Körper, wenn folgende Bedingungen erfüllt sind:

- $(K, +)$ ist eine abelsche Gruppe
- $(K, \cdot)$ ist eine abelsche Gruppe
- Es gilt das Distributivgesetz: $a \cdot (b + c) = ab + ac$

Wir werden in Zukunft fast immer K statt $(K, +, \cdot)$ schreiben, weil das schneller geht und praktischer ist.

1.1 Körpererweiterungen

In der folgenden Vorlesung werden wir uns intensiv mit Körpererweiterungen, d.h. Körpern als Teilmengen von anderen Körpern befassen. Wir werden diese Struktur, genannt "Körpererweiterung" als eigenes Studienobjekt und Körpererweiterungen mit weiteren Eigenschaften betrachten und mit dem Studium der Gruppentheorie und Polynomen in Beziehung setzen.

Teilkörper (Definition) Sei E ein Körper. Eine **Teilmenge** K von E heißt Teilkörper von E, falls K mit den von E induzierten Verknüpfungen selbst wieder ein Körper ist.

Nachweis von Teilkörpereigenschaft (Aussage):
Sei E ein Körper und K eine Teilmenge von E. Dann sind äquivalent:

- K ist Teilkörper von E

- Es gilt:
  i) $a - b \in K \ \forall a, b \in K$
  ii) $ab^{-1} \in K \ \forall a \in K$ and $b \in K^x$
  iii) $1 \in K$

Körpererweiterung (Definition)
Sei E ein Körper und K ein Teilkörper von E. Dann nennen wir E eine Körpererweiterung von K und schreiben für diese Struktur: E/K.

Anmerkung
Im folgenden werden wir für Körpererweiterungen immer E/K schreiben und für das Komplement zweier Mengen A und B: $A\backslash B$, d.h. für Körpererweiterungen ' backward slash' und für Komplemente ''forward slash' .

Teilgebiete dieses Kapitels
Das Thema "Körpererweiterungen" in diesem Kapitel werden wir in drei Unterkapitel sortieren. Wir werden sehen, dass:

- Körpererweiterungen immer eine Vektorraumstruktur tragen
- Körpererweiterungen in einem Körper generiert werden können,. z.B. durch das Kompositum
- Wir mittels Körperautomorphismen eine Brücke zu Polynomen schlagen können

1.1.1 Körpererweiterungen generieren

Zwischenkörper (Definition)
Sei E/K eine Körpererweiterung. Ein Teilkörper L von E heißt **Zwischenkörper** der Körpererweiterung E/K, falls gilt: $E \supseteq L \supseteq K$.

Schnitte von Teilkörpern sind Teilkörper (Aussage)
Sei $(L_i)_{i \in I}$ eine Familie von Teilkörpern eines Körpers E. Dann ist:

$$\bigcap_{i \in I} L_i$$

auch ein Teilkörper von E.

Kompositum und andere (Definition) Sei E ein Körper und L, F Teilkörper von E. Dann

i) heißt $LF := \bigcap\{\text{Teilkörper von E, die L und F enthalten}\}$ das Kompositum von L und F in E

ii) Sei E/K Körpererweiterung, $b_1, .., b_n \in K$ so heißt

$$K(b_1, ..., b_n) := \bigcap \{\text{Teilkörper von E, die K und } b_1, .., b_n \text{ enthalten }\}$$

der von $b_1, ..., b_n$ über K erzeugte Teilkörper von E

Kompositum mit größerem Körper (Ausage)
Sei E/K eine Körpererweiterung, $a_1, ..., a_n \in E$ und L Zwischenkörper von E/K. Dann gilt: $(K(a_1, .., a_n))L = L(a_1, ..., a_n)$.
Beweis:
Dies ist leicht durch Anwendung der Definition beider Seiten der Gleichung zu zeigen.

Endlich erzeugt (Definition)
Gilt in der obigen Definition im Fall ii), dass: $K(b_1, ..., b_n) = E$, so nennen wir die Körpererweiterung E/K endlich erzeugt.

1.1.2 Körpererweiterungen implizieren Vektorraumstruktur

Vektorraumstruktur für Körpererweiterungen (Aussage)
Sei E/K eine Körpererweiterung, dann ist E ein K-Vektorraum. **Beweis**
Die Vektorraumaxiome sind leicht durch die Körpereigenschaften nachzuweisen und wird dem Leser überlassen. Hehehehe.

Grad einer Körpererweiterung (Definition)
Sei E/K eine Körpererweiterung, dann ist der **Grad der Körpererweiterung** E/K gegeben durch

$$[E : K] := dim_K E$$

Also der Dimension des K-Vektorraumes E.

Gradformel (Aussage)
Sei E/K eine Körpererweiterung und L ein Zwischenkörper dieser. Dann gilt die Formel:

$$[E : K] = [E : L] \cdot [L : K]$$

Beweis der Gradformel
Sei $(x_i)_{i \in I}$ eine L-Basis von E und $(y_j)_{j \in J}$ eine K-Basis von L. Dann ist $(x_i, y_j)_{i \in I, j \in J}$ eine K-Basis von E. Denn:

Erzeugendensystem
Sei $e \in E$ ein beliebiges Element. Da (x_i) eine L-Basis von E ist, existieren $\lambda_i \in L$ sodass

$$e = \sum \lambda_i x_i$$

Da (y_j) eine K-Basis von L ist, existieren $\mu_{ij} \in K$, sodass $\lambda_i = \sum_{j \in J} \mu_{ij} y_j$ für alle $i \in I$ und damit gilt:

$$e = \sum \mu_{ij} x_i y_j$$

Lineare Unabhängigkeit
Seien nun $\lambda_{ij} \in K$, sodass

$$\sum_{i \in I, j \in J} \lambda_{ij} y_j x_i = 0$$

Da (x_i) L-Basis von E ist und $(\lambda_{ij} y_i)$ Skalare in L sind, muss gelten:

$$\lambda_{ij} y_j = 0 \ \forall i \in I \text{ und } \forall j \in J$$

nach der Basiseigenschaft.
Damit muss gelten

$$\sum_{j \in J} \lambda_{ij} y_j = 0 \ \forall i \in I$$

Da (y_j) eine K-Basis von L ist, muss dann gelten:

$$\lambda_{ij} = 0 \ \forall i \in I, \ j \in J$$

Damit sind $(x_i y_j)$ linear unabhängige Vektoren in E.

Aus der Erzeugendeneigenschaft und der linearen Unabhängigkeit folgt die Behauptung.

Endliche Körpererweiterung (Definition)
Sei E/K eine Körpererweiterung und $[E : K] < \infty$, dann nennen wir E/K endlich.

Endliche Körpererweiterungen sind endlich erzeugt (Aussage) Sei E/K eine endliche Körpererweiterung. Dann ist sie auch endlich erzeugt.
Beweis
Sei $(b_1, ..., b_n)$ eine K-Basis von E mit $n \in \mathbb{N}$. Sei $e \in E$.
Es existieren $\lambda_i \in K$ mit

$$e = \sum \lambda_i b_i$$

für $i \in \{1, ..., n\}$ Da $\lambda_i \in K(b_1, .., b_n)$ und $b_1, ..., b_n \in K(b_1, .., b_n)$, ist damit $e \in K(b_1, .., b_n)$, da $K(b_1, .., b_n)$ nach Definition ein Körper ist (und damit endliche Summen und Produkte von Elementen desselben immer in diesem enthalten sind).

E/K endl. g.d.w E/L und L/K endl. (Aussage)
Klar mit Gradformel

1.1.3 Brücke zwischen Körperhomomorphismen und Polynomen

Körperhomomorphismus, (Körper-)Automorphismus
Seien K und K' Körper. Eine Abbildung $\sigma : K \to K'$ heißt Körperhomomorphismus, wenn folgende Bedingungen erfüllt sind:

- $\sigma(1) = 1$
- $\sigma(a + b) = \sigma(a) + \sigma(b)$
- $\sigma(ab) = \sigma(a)\sigma(b)$

Ein (Körper-)Automorphismus ist ein Körperhomomorphismus $\sigma K \to K'$, der bijektiv ist und für den gilt: $K = K'$.

Untergliederung des Themas Körperhomomorphismen Wir werden Körperhomomorphismen in zwei Teile gliedern. Der erste Teil befasst sich mit allgemeinen Eigenschaften von Körperhomomorphismen, dessen Wissen oft nützlich ist. Der zweite Teil befasst sich mit Automorphismen, deren Gruppenstruktur und Relevanz für Polynome. Hier finden wir die erste Brücke zwischen Automorphismen und Polynomen über deren Nullstellen.

Allgemeine Eigenschaften von Körperhomomorphismen

Alle Körperhomomorphismen sind injektiv (Aussage)
Sei $\sigma : K \to K'$ ein Körperhomomorphismus, dann ist σ injektiv.

Beweis:
Da σ ein Körperhomomorphismus ist, ist es auch ein Gruppenhomomorphismus zwischen den abelschen Gruppen $(K, +)$ und $(K', +)$. Angenommen es existiert $x \in ker(\sigma)\backslash\{0\}$, dann gilt in K':

$$1 = \sigma(1) = \sigma(xx^{-1}) = \sigma(x)\sigma(x^{-1}) = 0\sigma(x^{-1}) = 0$$

Demnach $0 = 1$. Da K' ein Körper ist, muss $0 \neq 1$ gelten und wir haben einen Widerspruch.
Demnach ist $ker(\sigma) = \{0\}$ und nach dem *Monomorphiekriterium* ist σ injektiv.

Einbettung (Definition)
Ein Körperhomomorphismus wird aufgrund der obigen Aussage über dessen Injektivität auch Einbettung genannt.

Einfache Aussagen zu Körperhomomorphismen (Aussagen)
Seien $\sigma : K \to K'$ und $\mu : K \to L$ Körperhomomorphismen, dann ist wahr:

i) $\{a \in K : \sigma(a) = \mu(a)\}$ ist Teilkörper von K

ii) $\sigma(K)$ ist Teilkörper von K'

Beweis:
Zu i): Der Beweis geht einfach mit dem Charakterisierungslemma zu Teilkörpern (ganz am Anfang des Kapitels 1)
Zu ii) Charakterisierungslemma zu Teilkörpern

Diese Beweise werden dem motivierten Leser (der du sicher bist) als Übungsaufgabe überlassen.

Körperhomomorphismen und Kompositum (Aussage)
Seien L und F Teilkörper eines Körpers E und K ein Körper. Sei $\sigma : E \to K$ eine Einbettung. Dann gilt:

i) $\sigma(LF) = \sigma(L)\sigma(F)$

ii) Seien $a_1, .., a_n \in E$, dann: $\sigma(L(a_1, ..., a_n)) = \sigma(L)(\sigma(a_1), .., \sigma(a_n))$

iii) $\sigma(L \cap F) = \sigma(L) \cap \sigma(F)$

Beweis:
Zu i): Wir verwenden die Kompositumseigenschaft.
($\supseteq$): Wegen $L \subseteq LF$ und $F \subseteq LF$ gilt:

$$\sigma(L) \subseteq \sigma(LF), \text{ sowie } \sigma(F) \subseteq \sigma(LF)$$

damit gilt nach der Definition des Kompositums als kleinster Teilkörper von K, der $\sigma(L)$ und $\sigma(F)$ enthält:

$$\sigma(L)\sigma(F) \subseteq \sigma(LF)$$

($\subseteq$): Da gilt:

$$L,\ F \subseteq \sigma^{-1}(\sigma(L)\sigma(F))$$

und $\sigma^{-1}(\sigma(L)\sigma(F))$ ein Teilkörper von E ist. (Da σ injektiv und somit σ^{-1} als Einbettung von $\sigma(E) \to E$ gesehen werden kann.)
Damit ist nach Definition des Kompositums von L und F:

$$\sigma^{-1}(\sigma(L)\sigma(F)) \supset LF$$

Damit folgt durch nochmalige Anwendung von σ und dessen Injektivität:

$$\sigma(L)\sigma(F) \supset \sigma(LF)$$

insgesamt gilt also die Gleichheit in i).

Zu ii): Der Beweis folgt analog zu i), indem wir F durch $a_1, ..., a_n$ ersetzen und die Schritte passend durchgehen.

Zu iii): Dies folgt aus der Injektivität von σ und ist leicht nachzuprüfen, siehe Ana 1 Kurs.

Automorphismen und deren Gruppenstruktur
Wir erinnern uns an die Definition eines Körperautomorphismus. Auf diesen ist eine Gruppenstruktur mit der Komposition von Abbildungen $\circ$ definiert.
Aut(K) bilden eine Gruppe (Aussage)
Sei K ein Körper, dann is $(Aut(K), \circ)$ eine Gruppe.
Beweis:

Betrachte die Gruppe aller Abbildungen von K nach K mit der Komposition. Dann wende das Untergruppenkriterium an.

Aut(E/K) (Definition)
Sei E/K eine Körpererweiterung, dann ist:

$$Aut(E/K) := \{\sigma : \sigma\text{ist Automorphismus von E mit } \sigma_{|K} = id_K\}$$

Aut(E/K) ist Gruppe (Aussage)
$Aut(E/K)$ ist eine Untergruppe von $Aut(E)$
Beweis:
Untergruppenkrtierium

Brückensatz Automorphismen zu Nullstellen (Aussage)
Seien E/K sowie F/K Körpererweiterungen. Sei $\sigma : E \to F$ eine Einbettung und $f = \sum a_i X^i \in K[X]$ ein Polynom mit Nullstelle $\beta \in E$ und $deg(f) = n \in \mathbb{N}$.
Dann ist $\sigma(\beta)$ eine Nullstelle von f in F.
Beweis:
Es gilt:

$$f(\sigma(\beta)) = \sum a_i \sigma(\beta)^i = \sum a_i \sigma(\beta^i) = \sum \sigma(a_i \beta^i) = \sigma(\sum a_i \beta^i) = \sigma(0) = 0$$

Anmerkung
Wir werden diesen Satz nun auf die Situation: $E = K(\beta)$ für eine Körpererweiterung E/K anwenden (β hier Nullstelle von $f \in K[X]$). Hier werden wir sehen, dass wir eine injektive Abbildung der $\sigma \in Aut(E/K)$ auf die Menge der Nullstellen von f in E finden können. So können wir also mit der Nullstelle β und den Elementen in $Aut(E/K)$ neue Nullstellen generieren, falls $\#Aut(E/K) > 1$ ist. Die Idee ist K mittels Adjunktion weiterer Nullstellen zu erweitern, sodass wir dann alle Nullstellen von f finden. (Glaube ich)

Anwendung des obigen Satzes auf E=K(β) (Aussage)
Sei E/K eine Körpererweiterung, $f \in K[X]$ mit Nullstelle $\beta \in E$, sodass gilt: $E = K(\beta)$.
Dann ist die Abbildung $Aut(E/K) \to \{\text{Nullstellen von f in E}\}$, wobei $\sigma \mapsto \sigma(\beta)$, eine Injektion.
Beweis:
Seien $\sigma, \tau \in Aut(E/K)$ mit $\sigma(\beta) = \tau(\beta)$. Aus Obigem wissen wir:

$$M := \{a \in E : \sigma(a) = \tau(a)\}$$

ist ein Teilkörper von E. Wegen $\beta \in M$ und $K \subset M$ gilt $M \supseteq K(\beta)$. Also damit

$$M \supseteq K(\beta) = E$$

also $M = E$.
Damit ist $\sigma = \tau$.

Anmerkung: (Aussage)
Damit gilt natürlich auch $\#Aut(E/K) \leq$ {Nullstellen von f in E}

Können wir immer eine Körpererweiterung von K finden, in der eine Nullstelle von f existiert? Oben haben wir erwähnt, dass wir (auf eindeutige Weise) weitere Nullstellen von $f \in K[X]$ finden können, indem wir Automorphismen einer Körpererweiterung auf diese Nullstelle anwenden. Woher wissen wir aber, dass es auch immer eine solche Körpererweiterung gibt, in der wir eine Nullstelle für f finden? Wenn das nicht gilt, wäre unser obiges Resultat zwar schön, aber vielleicht nicht für alle Situationen hilfreich (wenn z.B. gar keine Körpererweiterung mit einer Nullstelle von f existiert).
Unsere Sorge ist unbegründet, wir können immer eine Körpererweiterung von K finden, sodass f in dieser eine Nullstelle besitzt (und damit immer obigen Satz anwenden, um nach neuen Nullstellen zu suchen). Um dies zu beweisen, werden wir die Ringtheorie lernen und entwickeln.