Vorlesung Lineare Algebra II

SoSe '20 hhu
K. Halupczok

§2: Normalformentheorie

l9: Zerlegung von Polynomen

Stichworte: Nullstelle / Linearfaktor, Zerlegung von Polynomen über alg. abg. Körpern in Linearfaktoren, irreduzible und reduzible Polynome, Zerlegung in irreduzible Faktoren, Lemma von Euklid

---

In diesem Abschnitt möchten wir die Zerlegung von Polynomen in ein Produkt von "einfacheren", nicht weiter zerlegbaren Polynomen untersuchen. (Nach Einsetzen eines Endomorphismus kann dann auch dieser in "einfachere" zerlegt werden, deren Kerne liefern uns dann die für die Normalformproblematik gesuchte Zerlegung eines Vektorraums in invariante Unterräume, vgl. l10.)

Wir hatten bemerkt in 7.3, dass jeder Körper K insb. eine K-Algebra ist. Dann können wir also in ein Polynom $p \in K[T]$ ein Körperelement λ einsetzen und erhalten wieder ein Körperelement. Wir kommen so zum Begriff "Nullstelle" und dem "Abspalten" eines Linearfaktors $T-\lambda$ in p einer Nullstelle λ von p. Auf diese Art erhalten wir die Komplette Zerlegung eines Polynoms $p \in K[T]$ in ein Produkt von Linearfaktoren, sofern der Körper K algebraisch abgeschlossen ist (wie etwa $K=\mathbb{C}$). Dieser Zerlegungssatz lässt sich auf Polynome über nicht algebraisch abgeschlossene Körper erweitern.

Beginnen wir mit den schon bekannten Grundlagen (vgl. L8, insb. L8.29 – L8.34):

9.1. **Def.:** $\lambda \in K$ heißt **Nullstelle** eines Polynoms $p \in K[T]$, wenn $p(\lambda)=0$ ist.

9.2. **Lemma:** $\lambda \in K$ ist genau dann Nullstelle von p, wenn $T-\lambda$ Teiler von p ist.

Bew.: „$\Leftarrow$": ist $p=(T-\lambda)\cdot q$, so folgt $p(\lambda)=(\lambda-\lambda)\cdot q(\lambda)=0$.

„$\Rightarrow$": Nach Satz 8.3 von der Division mit Rest gibt es eine Darstellung $p=q\cdot(T-\lambda)+r$ mit $\deg(r)<\deg(T-\lambda)=1$. Demnach muss r ein konstantes Polynom sein. Wegen $p(\lambda)=0$ ist $r=p(\lambda)-q(\lambda)\cdot(\lambda-\lambda)=0$. □

vgl. L8.32/L20.27

Da in einem algebraisch abgeschlossenen Körper (wie etwa $\mathbb{C}$) laut Definition jedes nicht konstante Polynom eine Nullstelle hat, folgt:

9.3. **Satz (Zerlegung von Polynomen in Linearfaktoren über algebraisch abg. Körpern):**
Ist K algebraisch abgeschlossener Körper, $p \in K[T]$, $\deg(p) = n \geq 1$, so existieren Körperelemente $\lambda_1, \dots, \lambda_n$ so, dass

$$p = \alpha_n \cdot (T - \lambda_1) \cdot (T - \lambda_2) \cdots (T - \lambda_n),$$

(← die Faktoren vom Grad 1 heißen Linearfaktoren)

wo α_n der höchste Koeffizient von p ist, und jedes λ_i eine Nullstelle von p (nicht notwendig verschieden!).

Bew.: Da K algebraisch abgeschlossen und $n \geq 1$, hat p eine Nullstelle λ_1.
Dann ist $p = p_1 \cdot (T - \lambda_1)$ und $\deg(p_1) = \deg(p) - 1 = n - 1$.
- Ist $n = 1$, so ist p_1 konstant, also $p_1 = \alpha_n$.
- Ist $n > 1$, so ist $\deg(p_1) \geq 1$ und somit hat p_1 eine Nullstelle λ_2 und eine Darstellung $p_1 = p_2 (T - \lambda_2)$, d.h. $p = p_2 \cdot (T - \lambda_1)(T - \lambda_2)$. Jetzt induktiv argumentieren. □

9.4. **Bsp.:** 1.) $T^3 + T = T \cdot (T^2 + 1) \in \mathbb{R}[T]$ nicht weiter zerlegbar, aber über $\mathbb{C}$ in Linearfaktoren: $T^3 + T = T \cdot (T - i)(T + i) = (T - 0) \cdot (T - i) \cdot (T + i)$.

2.) $2T^5 + 30T^3 - 60T^2 + 90 \in \mathbb{R}[T]$ hat wegen dem Zwischenwertsatz der Analysis (mindestens) eine Nullstelle. Mit algebraischen Methoden kann keine angegeben werden, hier müssen numerische Methoden verwendet werden. (→ Algebra, Numerik, ...)

3.) Das Polynom in 2.), über $\mathbb{Q}[T]$ aufgefasst, kann dort nicht weiter zerlegt werden (→ Algebra...).

Fasst man gleiche Linearfaktoren in Satz 9.3 zusammen, folgt:

9.5. **Korollar:** Über einem algebraisch abgeschlossenen Körper besitzt jedes normierte Polynom p vom Grad n eine Darstellung $p = \prod_{j=1}^{m} (T - \lambda_j)^{\nu_j}$ mit sämtlich verschiedenen $\lambda_j \in K$ und Exponenten $\nu_j \in \mathbb{N}$.

9.6. **Def.:** Die ν_j in Kor. 9.5 heißen die Ordnungen der λ_j als Nullstellen von p. (bzw. Vielfachheit von λ_j)

Zeigen Sie zur Übung den folgenden Satz als Konsequenz:

9.7 Satz: Über einem algebraisch abgeschlossenen Körper sind zwei Polynome genau dann teilerfremd, wenn sie keine gemeinsame Nullstelle haben.

Bew.: (ü)

Da viele Körper, u.a. $\mathbb{Q}$ und $\mathbb{R}$, nicht algebraisch abgeschlossen sind, wollen wir noch untersuchen, in welcher Form die Aussage von Kor. 9.5 dort gilt.

9.8 Bsp.: Sei $p(T) = T^4 - 2$. Als Polynom in $\mathbb{C}[T]$ können wir es zerlegen in
$$p(T) = (T - \sqrt[4]{2})(T + \sqrt[4]{2})(T - i\sqrt[4]{2})(T + i\sqrt[4]{2}),$$
in $\mathbb{R}[T]$ finden wir noch die Darstellung
$$p(T) = (T^2 - \sqrt{2})(T^2 + \sqrt{2}),$$
während in $\mathbb{Q}[T]$, abgesehen von Trivialitäten wie $p(T) = \frac{1}{3} \cdot (3(T^4 - 2))$, überhaupt keine Zerlegung in Faktoren möglich ist.
Die Zerlegbarkeit in Faktoren hängt also stark von dem Körper K ab!

9.9 Def. (irreduzibles Polynom): Ein Polynom $p \in K[T] \setminus K$ heißt irreduzibel (über K), wenn p nur triviale Teiler besitzt, d.h. wenn gilt:
Ist $q \in K[T]$ ein Teiler von p, so ist $q(T) = \alpha \in K$ oder $q(T) = \alpha \cdot p(T)$ für ein $\alpha \in K$. Ein Polynom, das nicht irreduzibel ist, heißt reduzibel.

(ü) Ist 0 irred.?

Unser Zerlegungssatz 9.3/Kor. 9.5 kann dann wie folgt verallgemeinert werden:

9.10 Satz (Zerlegung von Polynomen in irreduzible Faktoren):
Jedes normierte Polynom $p \in K[T]$ vom Grad $n \geq 1$ besitzt eine (bis auf die Nummerierung der Faktoren) eindeutige Zerlegung

(⊛) $p(T) = \prod_{j=1}^{m} q_j(T)^{\nu_j}$, wobei die q_j normierte, p.w.v. irreduzible Polynome vom Grad ≥ 1 sind,

wobei die Exponenten $\nu_j \geq 1$ sind, und wobei $\sum_{j=1}^{m} \nu_j \deg(q_j) = n$ ist.

sofort klar mit (⊛)

9.11. **Beweis** der Existenz der Zerlegung ⊛ durch vollst. Induktion über $n = \deg(p)$:

- Ist $n = 1$, so hat p die Form $p(T) = T - \lambda$, und dies ist mit $m = 1$, $v_1 = 1$, $q_1(T) = T - \lambda$ die behauptete Darstellung ⊛.
- Induktionsschritt: Sei $n > 1$ und für Polynome vom Grad $< n$ die Aussage schon gezeigt (Induktionsannahme). Es treten zwei Fälle auf:
  1. p ist irreduzibel: Dann liefert $m = 1$, $v_1 = 1$, $q_1 = p$ die gewünschte Darstellung.
  2. p ist reduzibel: $p = p_1 \cdot p_2$ mit $1 \leq \deg(p_1), \deg(p_2) < n$, und p_1, p_2 normiert. Dann können wir beide Faktoren nach Induktionsannahme als Produkt irreduzibler normierter Polynome schreiben, dann also auch $p = p_1 \cdot p_2$; eventuell auftretende gleiche Faktoren können wir zu Potenzen zusammenfassen. □ Ex. ✓

Für den Beweis der Eindeutigkeit ziehen wir folgendes Lemma heran:

9.12. **Lemma** (Lemma von Euklid für Polynome):

In $K[T]$ ist jedes irreduzible Polynom $q \in K[T]$ prim,
d.h. sind $p_1, p_2, q \in K[T]$, q irreduzibel und ist q ein Teiler von $p_1 \cdot p_2$,
so teilt q schon einen der Faktoren: $q \mid p_1 \vee q \mid p_2$.
(Kurz: q irreduzibel, $q \mid p_1 p_2 \Rightarrow q \mid p_1 \vee q \mid p_2$)

Beweis: Nehmen wir an, $q \mid p_1 \cdot p_2$, aber $q \nmid p_1$. Es sei o.E. $p_1 \neq 0 \neq p_2$.
Bilde $d := ggT(p_1 p_2, q p_2)$.
Da q jedes der beiden Polynome teilt, teilt es also auch d.
Wir zeigen $d = p_2$ (dann folgt $q \mid d = p_2$):
Nach Konstruktion ist p_2 ein gemeinsamer Teiler von $p_1 p_2$ und $q p_2$, also ein Teiler von d, d.h. $d = s \cdot p_2$. Damit ist $s p_2 \mid p_1 p_2$ und $s p_2 \mid q p_2$, folglich $s \mid p_1$ und $s \mid q$, d.h. $s \mid ggT(p_1, q)$.
Nun ist $ggT(p_1, q) = 1$, da q irreduzibel und $q \nmid p_1$ ist.
⌜Sei $t := ggT(p_1, q)$ normiert. Da q irreduzibel und $t \mid q$ ist, folgt $t = 1 \vee t = \alpha q$, ack, o.E.
Im zweiten Fall wäre $q = \frac{1}{\alpha} \cdot t \mid p_1$, was nicht sein kann.⌟
Somit ist $s \mid 1$, also $s = 1$ und $d = p_2$. □

9.13. **Bem.:** • Das Lemma gilt auch über $\mathbb{Z}$ anstelle $K[T]$ (d.h. $a,b,p \in \mathbb{Z}$, p lat. prim $\Rightarrow$ p|a ∨ p|b).
Der Name "Lemma von Euklid" bezeichnet eher die $\mathbb{Z}$-Version.
Der Beweis dafür geht völlig analog/wortwörtlich wie oben in 9.12.
• Das Lemma von Euklid über $\mathbb{Z}$ schließt die Beweislücke in Beweis von L7.36 in LAI ($\mathbb{Z}/M\mathbb{Z}$ Körper $\Leftrightarrow$ M prim).

9.14. **Beweis der Eindeutigkeit der Zerlegung** ⊗ **mit dem Lemma von Euklid** (für Polynome): Angenommen, das Polynom p besitze zwei Zerlegungen in irreduzible Faktoren der verlangten Art:

$$p(T) = \prod_{j=1}^{m} q_j(T)^{\nu_j} = \prod_{\ell=1}^{n} r_\ell(T)^{\mu_\ell}.$$

Tritt für ein j und ein ℓ ein gleicher Faktor auf, d.h. $q_j = r_\ell$, so bleibt die rechte Gleichung erhalten, wenn wir diesen gemeinsamen Faktor herauskürzen. Dies iterieren wir solange, bis beide Seiten keinen gemeinsamen Faktor mehr enthalten.

⊙ Bleibt dann auf beiden Seiten nur das leere Produkt (=1) übrig, so waren die Zerlegungen (bis auf Reihenfolge) gleich.
⊙ Waren sie dagegen echt verschieden, so tritt etwa links ein Faktor q_j auf, der von allen rechts noch vorhandenen r_ℓ verschieden ist.

Damit teilt q_j das rechte Produkt und, da q_j irreduzibel ist, also auch einen Faktor im rechten Produkt (nach dem Lemma von Euklid 9.12).
Somit teilt q_j ein r_ℓ, und da r_ℓ irreduzibel ist,
muss $q_j = r_\ell$ sein, was nicht mehr möglich ist ↯.
Somit kann es keine wesentlich verschiedenen Darstellungen geben. □ Eind.✓

9.15. **Bem.:** Satz 9.10 kann ebenso komplett für $\mathbb{Z}$ statt $K[T]$ formuliert und genau analog bewiesen werden. In dieser Version heißt er dann "Satz von der eindeutigen Primfaktorzerlegung (über $\mathbb{Z}$)" oder auch "Fundamentalsatz der Arithmetik".
In Algebra studiert man Ringe, wo dies nicht mehr gilt; der Satz ist nicht selbstverständlich.

Mit Satz 9.10 können wir noch folgendes feststellen:

9.16. **Kor.:** In $\mathbb{C}[T]$ sind genau die linearen Polynome irreduzibel.
(Wie für jeden algebraisch abgeschlossenen Körper.)

9.17. **Bem.:** In $\mathbb{R}[T]$ ist dagegen etwa T^2+1 irreduzibel. Denn eine Zerlegung müsste lauten $T^2+1 = (T-\alpha)(T-\beta)$ mit $\alpha,\beta \in \mathbb{R}$, wobei dann T^2+1 die reellen Nullstellen α, β hätte, was falsch ist.
Polynome höheren Grades sind jedoch stets zerlegbar:

9.18. **Satz:** In $\mathbb{R}[T]$ gibt es nur irreduzible Polynome vom Grad 1 oder 2.

Bew.: Sei $p \in \mathbb{R}[T]$ mit $\deg(p) > 2$.

- Hat p eine reelle Nullstelle $\lambda \in \mathbb{R}$, so ist nach Lemma 9.2 dann $T-\lambda$ ein nichttrivialer Teiler von p, somit ist p zerlegbar (d.h. reduzibel).
- Bleibt der Fall, dass p keine reellen Nullstellen besitzt.
Nun lesen wir $p(T) = \alpha_n T^n + \alpha_{n-1} T^{n-1} + \dots + \alpha_0 \in \mathbb{R}[T]$ mit $\alpha_j \in \mathbb{R}$, $\alpha_n \neq 0$, als ein Polynom in $\mathbb{C}[T]$, d.h. als ein Polynom mit Komplexen Koeffizienten, deren Imaginärteile eben zufällig alle $=0$ sind, für die also $\alpha_j = \overline{\alpha_j}$ (konjugiert komplex) gilt. In $\mathbb{C}[T]$ besitzt p nun eine Nullstelle $\lambda = \alpha + i\beta$, und da p keine reelle Nullstelle hat, muss $\beta \neq 0$ sein. Nach den Regeln zum Komplex Konjugieren folgt nun

$$p(\overline{\lambda}) = \sum_{j=0}^{n} \alpha_j (\overline{\lambda})^j = \sum_{j=0}^{n} \overline{\alpha_j} (\overline{\lambda})^j = \overline{\sum_{j=0}^{n} \alpha_j \lambda^j} = \overline{p(\lambda)} = \overline{0} = 0,$$

also ist mit λ auch $\overline{\lambda}$ Nullstelle, und somit hat p die beiden verschiedenen Nullstellen $\lambda = \alpha+i\beta$ und $\overline{\lambda} = \alpha - i\beta$, hat also den Teiler

$$(T-\lambda)\cdot(T-\overline{\lambda}) = (T-\alpha-i\beta)\cdot(T-\alpha+i\beta) = T^2 - 2\alpha T + (\alpha^2+\beta^2) \in \mathbb{R}[T].$$

Da p den Grad ≥ 3 hatte, ist dies ein echter Teiler, also $p \in \mathbb{R}[T]$ reduzibel. □

9.19. **Satz:** In $\mathbb{Q}[T]$ gibt es für jedes $n = 1, 2, 3, \dots$ irreduzible Polynome vom Grad n.

Bew.: s. Algebra-Vorlesung; ein Bsp. ist etwa $T^n - 2$.