

K13: Grundlagen: Polynome und endliche Körper

Stichworte: Def. Polynom, Ableitung, Produkt / Kettenregel
 Nullstelle + Ordnung, irreduzibles Polynom,
 eindeutig Zerlegung in irred. Polynom (Gauß) $\hat{=}$ PTZ in \mathbb{Z}
 Eukl. Algo geht im Polynomring $k[x]$ $\hat{=}$ Eukl. Algo in \mathbb{Z}
 Restklassenring $\underbrace{k[x]/(f)}_{\text{Körper, wenn } f \text{ irreduzibel}}$ $\hat{=}$ $\underbrace{\mathbb{Z}/m\mathbb{Z}}_{\text{Körper, wenn } m \text{ prim}} \sim \mathbb{F}_p$

(neu) endliche Körper \mathbb{F}_{p^r} + Rechnen darin, algebraischer Abschluss

Grundlagen aus der Algebra — Polynome

Sei k ein (beliebiger) Körper.

13.1. Def.: Ein Polynom über k in den n Variablen x_1, \dots, x_n ist ein Ausdruck der Form $f(x_1, \dots, x_n) = \sum_{\substack{v_1, \dots, v_n \\ \geq 0}} \alpha_{v_1, \dots, v_n} x_1^{v_1} \cdots x_n^{v_n}$,

mit Koeffizienten $\alpha_{v_1, \dots, v_n} \in k$, von denen nur endlich viele $\neq 0$ sind.
 Hat man es mit mehreren Variablen ($n \geq 2$) zu tun, kann man auch kurz $f(\underline{x}) = \sum_{\underline{v} \in \mathbb{N}_0^n} \alpha_{\underline{v}} x_1^{v_1} \cdots x_n^{v_n}$ schreiben,

wenn man die Tupel Schreibweise $\underline{v} \in \mathbb{N}_0^n$ bzw. $\underline{x} = (x_1, \dots, x_n)$ einführt, wobei man für das Monom $x_1^{v_1} \cdots x_n^{v_n}$ auch kurz $x^{\underline{v}}$ schreiben kann, wenn klar ist, dass $n \geq 2$ viele Variablen vorliegen.

Die Menge aller Polynome über k in n Variablen wird kurz mit $k[x_1, \dots, x_n]$ oder noch kürzer mit $k[x]$ bezeichnet, schreiben dann auch kurz $f \in k[x]$ wenn $f(x)$ ein Polynom ist.

13.2. Bem.:

Durch Komponentenweise Addition $\sum_{\underline{v}} \alpha_{\underline{v}} x^{\underline{v}} + \sum_{\underline{v}} \beta_{\underline{v}} x^{\underline{v}} := \sum_{\underline{v}} (\alpha_{\underline{v}} + \beta_{\underline{v}}) x^{\underline{v}}$
und der Multiplikation $(\sum_{\underline{v}} \alpha_{\underline{v}} x^{\underline{v}}) (\sum_{\underline{m}} \beta_{\underline{m}} x^{\underline{m}}) := \sum_{\underline{v}, \underline{m}} \alpha_{\underline{v}} \beta_{\underline{m}} x^{\underline{v} + \underline{m}}$

wird $k[x] = k[x_1, \dots, x_n]$ zu einem kommutativen Ring mit 1;

das Nullpolynom $0 := \sum_{\underline{v}} 0 \cdot x^{\underline{v}}$ ist dabei das Nullelement,

das Polynom $1 := 1 \cdot x^{\underline{0}} + \sum_{\underline{v} \neq \underline{0}} 0 \cdot x^{\underline{v}}$ ist das Einselement. ("Einspolynom")

Der Ring

$(k[x], +, \cdot)$ heißt Polynomring über k .

13.3. Def.: Für $f \in k[x]$ mit $f(x) = \sum_{\underline{v}} \alpha_{\underline{v}} x^{\underline{v}}$ und $1 \leq j \leq n$

heißt $\frac{\partial f}{\partial x_j} \in k[x]$ mit $\frac{\partial f}{\partial x_j}(x) := \sum_{\substack{\underline{v} \\ v_j > 0}} \alpha_{\underline{v}} v_j x_1^{v_1} \cdots x_j^{v_j-1} \cdots x_n^{v_n}$

die (formale) Ableitung von f nach x_j .

13.4. Bem.: Ist $k = \mathbb{R}$, stimmt diese Def. mit der üblichen Def. der Analysis überein. Hier sind "Ableitungen" wieder Polynome.

Durch einfaches Nachrechnen kann man bestätigen:

13.5. Satz: Für alle $f, g \in k[x]$ und $\gamma \in k$ gelten die Ableitungsregeln

$$\frac{\partial(\gamma f)}{\partial x_j} = \gamma \frac{\partial f}{\partial x_j} \quad \text{und} \quad \frac{\partial(f+g)}{\partial x_j} = \frac{\partial f}{\partial x_j} + \frac{\partial g}{\partial x_j},$$

$$\frac{\partial(f \cdot g)}{\partial x_j} = f \frac{\partial g}{\partial x_j} + g \frac{\partial f}{\partial x_j} \quad (\text{Produktregel}),$$

und für $f \in k[x_1, \dots, x_m]$, $g_1, \dots, g_m \in k[x_1, \dots, x_m]$

die Kettenregel $\frac{\partial f(g_1, \dots, g_m)}{\partial x_j}$

$$= \frac{\partial f}{\partial x_1}(g_1, \dots, g_m) \frac{\partial g_1}{\partial x_j} + \dots + \frac{\partial f}{\partial x_m}(g_1, \dots, g_m) \frac{\partial g_m}{\partial x_j}$$

Polynome in einer Variablen $f \in k[x]$ der Form $f(x) = \sum_{v \geq 0} \alpha_v x^v$ sind aus den Grundvorlesungen bekannt.

13.6. Ist $f \neq 0$, so heißt $\text{deg}(f)$:= $\max \{j \in \mathbb{N}_0; \alpha_j \neq 0\}$ der Grad von f .

Für $f \in k[x]$ in n Variablen ist $\text{deg}(f)$:= $\max \{v_1 + \dots + v_n; \alpha_{v_1, \dots, v_n} \neq 0\}$ der Grad von f .

Nun ist bei uns, dass wir uns hier vor allem mit $n=2$ oder $n=3$

Variablen beschäftigen werden, wo wir dann auch $f(x, y)$ oder $f(x, y, z)$

schreiben möchten, z.B. $f(x, y) = \alpha_{(2,0)} x^2 + \alpha_{(1,1)} xy + \alpha_{(0,1)} y$,

wir werden dann für die Koeffizienten einfachere Notationen wählen.

13.7. Bleiben wir zunächst beim Polynomring $k[x]$ in einer Variablen x , sei $f \in k[x]$. Wie im Ring \mathbb{Z} können wir Teilbarkeit in $k[x]$ studieren und Divisionen mit Rest durchführen ("Polynomdivisionen") (daher kann man wie in \mathbb{Z} z.B. den ggT von Polynomen mit dem Euklidischen Algorithmus ausrechnen).

Dies ist aus den Grundvorlesungen bekannt, wir erinnern hier nur an folgendes:

13.8. Def.: Geg. sei die "Einsetz" Abbildung $k \rightarrow k, c \mapsto f(c) := \sum_{i \geq 0} \alpha_i c^i$.
Ein El. $c \in k$ heißt Nullstelle von f , falls $f(c) = 0$ in k ist.

13.9 Bem.: $c \in k$ ist genau dann Nst., wenn $(x-c)$ ein Teiler von f im Polynomring $k[x]$ ist, d.h. falls ex. $g \in k[x]$ mit $(x-c) \cdot g = f$.

13.10. Def.: Ist c eine Nullstelle von $f \neq 0$, so gibt es ein maximales $e \geq 1$, so dass $(x-c)^e$ ein Teiler von f ist. Die Zahl e heißt Ordnung der Nullstelle c . Ist $f(c) \neq 0$, def. man diese "Nullstellen" Ordnung als 0.

13.11. Def.: Ein Polynom $f \in k[x]$ vom Grad ≥ 1 heißt irreduzibel (oder prim), falls gilt: $\forall m, v \in k[x]: f = m \cdot v \Rightarrow \deg m = 0$ oder $\deg v = 0$, d.h. f kann nicht als Produkt zweier Polynome vom Grad ≥ 1 geschrieben werden. (\leadsto vgl. Begriff "Primzahl" bei \mathbb{Z} ; der Satz von der eindeutigen Zerlegung in irreduzible Polynome heißt der "Satz von Gauß".)

Wenn wir \mathbb{Z} als Vorbild für den Polynomring $k[x]$ nehmen, möchten wir auch das "Modulrechnen" auf $k[x]$ übertragen, um neue Strukturen zu erhalten. Unsere Module sind dann Polynome:

13.12. Def.: Sei $f \in k[x]$. Dann heißen $a \in k[x]$ und $b \in k[x]$ Kongruent modulo f , wenn $f \mid (b-a)$, d.h. falls $g \in k[x]$ ex. mit $b = a + fg$.
(Das Kongruenzzeichen \equiv möchten wir für \mathbb{Z} vorbehalten.)

Die Restklassen modulo f sind Teilmengen von $k[x]$ der Gestalt
 $a + f \cdot k[x] := \{a + f \cdot g; g \in k[x]\}$ mit $a \in k[x]$.

Das Polynom $a \in k[x]$ heißt ein Repräsentant der Restklasse.

Ist der Modul $f \in k[x]$ klar, möchten wir dafür auch kurz wieder \underline{a} schreiben.

Die Menge der Restklassen modulo f bezeichnen wir mit $k[x]/(f) := \{a + f \cdot k[x]; a \in k[x]\} = \{\underline{a}; a \in k[x]\}$ (aber doppelt unterstreichen!)

und nennen diese den Restklassenring modulo f , weil diese bzgl.

der Def. $\underline{a} + \underline{b} := \underline{a+b}$ für Polynome $a, b \in k[x]$

wieder zu einem kommutativen Ring mit $\underline{1}$ als Eins wird.

13.13. Bem.: Doch die einfache Frage, wieviele Elemente der Restklassenring hat, hängt u.a. vom Körper k ab. Im Fall $k = \mathbb{F}_p$ beantworten wir diese, klar ist wegen der Teilbarkeit mit Rest im Ring $k[x]$

"Polynom-
division") d.h. sind $b, f \in k[x]$ und $f \neq 0$, so ex. eindeutige $g, r \in k[x]$ mit $r = 0$ oder $\deg r < \deg f$ so dass $b = f \cdot g + r$ gilt):

13.14. Bem.: Für jede Restklasse $\underline{a} = a + f \cdot k[x] \in k[x]/(f)$ gibt es genau einen Vertreter $b \in \underline{a} = a + f \cdot k[x]$, d.h. $\underline{b} = \underline{a}$ bzw. $b + f \cdot k[x] = a + f \cdot k[x]$, mit $b = 0$ oder $\deg b < \deg f$.

Grundlagen aus der Algebra — Endliche Körper

Sei nun $k = \mathbb{F}_p$ mit p prim.

13.15. Satz: Sei $f \in \mathbb{F}_p[x]$ irreduzibel mit $r := \deg f$.

Dann ist $\mathbb{F}_p[x]/(f)$ ein Körper mit p^r Elementen.

Bew.: Körper: \checkmark [Inverse findet man mit erweitertem Euklidischen Algorithmus

für Polynome], p^r El.: jede Restklasse hat genau einen Vertreter $b = \alpha_0 + \dots + \alpha_{r-1} X^{r-1}$.

\uparrow
 p Möglichkeiten
für jedes α_i

□

- 13.16. Bem.: Für jedes $n \in \mathbb{N}$ gibt es ^(mind.) ein irreduzibles Polynom $f \in \mathbb{F}_p[x]$ mit $\deg f = n$.
- 13.17. Bem.: Es gibt im wesentlichen (d.h. bis auf Isomorphie) genau einen endlichen Körper mit p^n Elementen, d.h. welches irreduzible f mit $\deg f = n$ wir als Modul nehmen, ist für seine Konstruktion (bis auf Isomorphie!) egal. Wir bezeichnen diesen Körper mit \mathbb{F}_{p^n} .
- 13.18. Bem.: Jeder Körper mit endlich vielen Elementen ist einer dieser Körper \mathbb{F}_{p^n} mit p prim und $n \geq 1$. [Beweis s. Vorl. Algebra, A21.5]

13.19. Wegen Bem. 14 ist nach Wahl eines irreduziblen Polynoms $f \in \mathbb{F}_p[x]$, $\deg f = n$, also $\mathbb{F}_{p^n} = \{(\alpha_{r-n}x^{r-n} + \dots + \alpha_n x + \alpha_0) + f \cdot \mathbb{F}_p[x]; \alpha_i \in \mathbb{F}_p\}$,

die Restklassenvertreter $\alpha_{r-n}x^{r-n} + \dots + \alpha_n x + \alpha_0$ lassen sich auch durch Koeffizienten- n -Tupel $(\alpha_{r-n}, \alpha_{r-2}, \dots, \alpha_n, \alpha_0) \in \mathbb{F}_p^n$ darstellen. Will man mit ihnen stellvertretend für die Polynomrestklassen in \mathbb{F}_{p^n} rechnen, muss man also erst mit den zugehörigen Polynomen über \mathbb{F}_p rechnen und modulo f reduzieren.

13.20. Bsp.: Sei $p=2$, $n=3$, wir möchten \mathbb{F}_8 konstruieren.

Das Polynom $f(x) = x^3 + x + 1$ ist irreduzibel über $\mathbb{F}_2 = \{0, 1\}$,

also ist $\mathbb{F}_8 = \mathbb{F}_2[x]/(f) = \{(0,0,0), (0,0,1), (0,1,0), (0,1,1), (1,0,0), (1,0,1), (1,1,0), (1,1,1)\}$,

und man rechnet z.B. $(0,1,0) \cdot (1,1,1) = (1,0,1)$,

weil $(0 \cdot x^2 + 1 \cdot x + 0) \cdot (x^2 + x + 1) = x^3 + x^2 + x = 1 \cdot (x^3 + x + 1) + (x^2 + 1)$
Div. mit Rest durch f in $\mathbb{F}_2[x]$ gilt

- Bei Wahl des irreduziblen Polynoms $f(x) = x^3 + x + 1$ ergeben sich zwar andere Rechenregeln für die Vektormultiplikation, man erhält aber dieselbe "Struktur" bei $+$ mit entsprechenden Elementen. Stellen Sie als Übung mal die Multiplikations- und Additionstabellen auf, der Einfachheit halber auch erstmal von \mathbb{F}_4 .

- Streng genommen müsste man z.B. $\underline{(1, 0, 1)} = \underline{x^2 + 1}$ für die Elemente von \mathbb{F}_5 schreiben, um die Reduktion mod f zu verdeutlichen.

13.21. Bsp.: Rechnen in $\mathbb{F}_{5^3} = \mathbb{F}_{125}$: Haben wir diesen Körper mit dem irreduziblen Polynom $f = x^3 + x + 1 \in \mathbb{F}_5[x]$ vom Grad 3 konstruiert

(da es keine Nst. in \mathbb{F}_5 hat, muss es irreduzibel sein, da es Grad 3 hat!),

So rechnen wir in \mathbb{F}_{5^3} z.B. $\underline{(1, 2, 4)} \cdot \underline{(-1, 3, 0)}$

$$= (x^2 + 2x - 1)(-x^2 + 3x) = -x^4 + 3x^3 - 2x^3 + 6x + x^2 - 3x$$

$$= -x^4 + x^3 + x^2 + 3x = (x^3 + x + 1) \cdot (-x + 1) + 2x^2 + 3x + 1$$

$$\stackrel{\text{Polydiv. durch } f}{=} \underline{(2, 3, 1)} \text{ mod } f, \quad \text{"eigentlich" ja: } \underline{(1, 2, -1)} \cdot \underline{(-1, 3, 0)} = \underline{(2, 3, 1)}.$$

13.22. Bem.: $\text{char}(\mathbb{F}_p) = p$, denn es gilt $\underbrace{1 + 1 + \dots + 1}_{p \text{ mal}} = \underbrace{1 + \dots + 1}_{p \text{ mal}} = p \cdot 1 = 0$,
und p minimal so da p prim.

13.23. Def.: Ein Körper k ist algebraisch abgeschlossen, wenn sich jedes Polynom $f \in k[x]$, $\deg f > 0$, als Produkt von linearen Polynomen schreiben lässt, d.h. wenn $f(x) = d(x - c_1) \dots (x - c_m)$, die $c_i, d \in k$ gilt.

13.24. Bem.: Man kann jeden Körper k in einen algebraisch abgeschlossenen Körper einbetten. Ein bzgl. " \leq " minimaler heißt algebraischer Abschluss von k , dieser ist eindeutig und wird mit \bar{k} bezeichnet.

So ist etwa $\overline{\mathbb{R}} = \mathbb{C}$. Der algebraische Abschluss $\overline{\mathbb{F}_p}$ enthält jeden der Körper \mathbb{F}_{p^r} , $r \geq 1$, und umgekehrt ist jedes Element von $\overline{\mathbb{F}_p}$ schon in einem dieser Körper \mathbb{F}_{p^r} , $r \geq 1$, enthalten [ohne Beweis].