Stichworte:

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

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

---

§2 Elliptische Kurven (über beliebigen Grundkörper k)

§2.1 Grundlagen aus der Algebra

2.1.1 Polynome

Sei k ein (beliebiger) Körper.

1.) Def.: Ein Polynom über k in den n Variablen $x_1, \dots, x_n$ ist ein Ausdruck der Form $f(x_1, \dots, x_n) = \sum_{\nu_1, \dots, \nu_n \geq 0} \alpha_{\nu_1, \dots, \nu_n} x_1^{\nu_1} \cdots x_n^{\nu_n}$,

mit Koeffizienten $\alpha_{\nu_1, \dots, \nu_n} \in k$, von denen nur endlich viele $\neq 0$ sind.
Hat man es mit mehreren Variablen ($n \geq 2$) zu tun, kann man auch kurz $f(\underline{x}) = \sum_{\underline{\nu} \in \mathbb{N}_0^n} \alpha_{\underline{\nu}} x_1^{\nu_1} \cdots x_n^{\nu_n}$ schreiben,

wenn man die Tupelschreibweise $\underline{\nu} \in \mathbb{N}_0^n$ bzw. $\underline{x} = (x_1, \dots, x_n)$ einführt, wobei man für das Monom $x_1^{\nu_1} \cdots x_n^{\nu_n}$ auch kurz $\underline{x}^{\underline{\nu}}$ 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 $k[\underline{x}]$ bezeichnet,
schreiben dann auch kurz $f \in k[\underline{x}]$ wenn $f(\underline{x})$ ein Polynom ist.

2.) Bem.:
Durch Komponentenweise Addition $\sum_{\underline{\nu}} \alpha_{\underline{\nu}} \underline{x}^{\underline{\nu}} + \sum_{\underline{\nu}} \beta_{\underline{\nu}} \underline{x}^{\underline{\nu}} := \sum_{\underline{\nu}} (\alpha_{\underline{\nu}} + \beta_{\underline{\nu}}) \underline{x}^{\underline{\nu}}$
und der Multiplikation $\left(\sum_{\underline{\nu}} \alpha_{\underline{\nu}} \underline{x}^{\underline{\nu}}\right)\left(\sum_{\underline{\mu}} \beta_{\underline{\mu}} \underline{x}^{\underline{\mu}}\right) := \sum_{\underline{\nu}, \underline{\mu}} a_{\underline{\nu}} b_{\underline{\mu}} \underline{x}^{\underline{\nu}+\underline{\mu}}$

wird $k[\underline{x}] = k[x_1, \dots, x_n]$ zu einem Kommutativen Ring mit 1;
das Nullpolynom $0 := \sum_{\underline{\nu}} 0 \cdot \underline{x}^{\underline{\nu}}$ ist dabei das Nullelement,
das Polynom $1 := 1 \cdot \underline{x}^{\underline{0}} + \sum_{\underline{\nu} \neq \underline{0}} 0 \cdot \underline{x}^{\underline{\nu}}$ ist das Einselement. ("Einspolynom")
Der Ring
$(k[\underline{x}], +, \cdot)$ heißt Polynomring über k.

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

heißt $\frac{\partial f}{\partial x_j} \in k[\underline{x}]$ mit $\frac{\partial f}{\partial x_j}(\underline{x}) := \sum_{\underline{\nu},\, \nu_j > 0} \alpha_{\underline{\nu}}\, \nu_j\, x_1^{\nu_1} \cdots x_j^{\nu_j - 1} \cdots x_n^{\nu_n}$

die (formale) Ableitung von f nach x_j.

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:

4.) Satz: Für alle $f, g \in k[\underline{x}]$ 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 $f \in k[x_1, \dots, x_m]$, $g_1, \dots, g_m \in k[x_1, \dots, x_n]$

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 $f(x) = \sum_{\nu \geq 0} \alpha_\nu x^\nu$ sind aus den Grundvorlesungen bekannt.

5.) Ist $f \neq 0$, so heißt $\deg(f) := \max\{j \in \mathbb{N}_0 ; \alpha_j \neq 0\}$ der Grad von f.
Für $f \in k[\underline{x}]$ in n Variablen ist $\deg(f) := \max\{\nu_1 + \ldots + \nu_n ; \alpha_{\underline{\nu}} \neq 0\}$ der Grad von f.
Neu 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.

6.) 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:

7.) **Def.:** Geg. sei die "Einsetz"abbildung $k \to k$, $c \mapsto f(c) := \sum_{\nu \geq 0} \alpha_\nu c^\nu$.
Ein El. $c \in k$ heißt Nullstelle von f, falls $f(c) = 0$ in k ist.

8.) **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 $(x-c) \cdot g = f$.

9.) **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.

10.) **Def.:** Ein Polynom $f \in k[x]$ vom Grad ≥ 1 heißt irreduzibel (oder prim), falls gilt: $\forall u, v \in k[x] : f = u \cdot v \Rightarrow \deg u = 0$ oder $\deg v = 0$, d.h. f kann nicht als Produkt zweier Polynome vom Grad ≥ 1 geschrieben werden. ($\rightsquigarrow$ 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 "Modulorechnen" auf $k[x]$ übertragen, um neue Strukturen zu erhalten. Unsere Moduln sind dann Polynome:

11.) **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
$$a + f \cdot k[X] := \{ a + f \cdot g \, ; \, g \in k[X] \} \text{ mit } a \in k[X].$$
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. (aber doppelt unterstrichen!)
Die Menge der Restklassen modulo f bezeichnen wir mit
$$k[X]/(f) := \{ a + f \cdot k[X] \, ; \, a \in k[X] \} = \{ \underline{\underline{a}} \, ; \, a \in k[X] \}$$
und nennen diese den **Restklassenring modulo f**, weil diese bzgl. der Def. $\underline{\underline{a}} \pm \underline{\underline{b}} := \underline{\underline{a \pm b}}$ für Polynome $a, b \in k[X]$ wieder zu einem kommutativen Ring mit $\underline{\underline{1}}$ als Eins wird.

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 $k[X]$
"Polynomdivision" (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):

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

2.1.2 Endliche Körper

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

13.) **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: ✓ [Inverse findet man mit erweitertem Euklidischen Algorithmus für Polynome], p^r El.: jede Restklasse hat genau einen Vertreter $b = \alpha_0 + \ldots + \alpha_{r-1} X^{r-1}$. □
p Möglichkeiten für jedes α_j

14) **Bem.:** Für jedes $r \in \mathbb{N}$ gibt es (mind.) ein irreduzibles Polynom $f \in \mathbb{F}_p[x]$ mit $\deg f = r$.

15) **Bem.:** Es gibt im wesentlichen (d.h. bis auf Isomorphie) <u>genau einen</u> endlichen Körper mit p^r Elementen, d.h. welches irreduzible f mit $\deg f = r$ wir als Modul nehmen, ist für seine Konstruktion (bis auf Isomorphie!) egal. Wir bezeichnen diesen Körper mit $\boxed{\mathbb{F}_{p^r}}$.

16) **Bem.:** Jeder Körper mit endlich vielen Elementen ist einer dieser Körper $\mathbb{F}_{p^r}$ mit p prim und $r \geq 1$. [Ohne Beweis, vgl. "Algebra"-Vorl.]

17.) Wegen Bem. 12.) ist nach Wahl eines irreduziblen Polynoms $f \in \mathbb{F}_p[x]$, $\deg f = r$, also $\mathbb{F}_{p^r} = \{(\alpha_{r-1}x^{r-1} + \ldots + \alpha_1 x + \alpha_0) + f \cdot \mathbb{F}_p[x] \; ; \; \alpha_i \in \mathbb{F}_p\}$,

die Restklassenvertreter $\alpha_{r-1}x^{r-1} + \ldots + \alpha_1 x + \alpha_0$ lassen sich auch durch Koeffizienten-r-Tupel $(\alpha_{r-1}, \alpha_{r-2}, \ldots, \alpha_1, \alpha_0) \in \mathbb{F}_p^r$ darstellen. Will man mit ihnen stellvertretend für die Polynomrestklassen in $\mathbb{F}_{p^r}$ rechnen, muss man also erst mit den zugehörigen Polynomen über $\mathbb{F}_p$ rechnen und modulo f reduzieren.

18) **Bsp.:** Sei $p = 2$, $r = 3$, 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 $(0 \cdot x^2 + 1 \cdot x + 0) \cdot (x^2 + x + 1) = x^3 + x^2 + x \underset{\substack{\uparrow \\ \text{Div. mit Rest} \\ \text{durch } f}}{=} 1 \cdot (x^3 + x + 1) + \underbrace{(x^2 + 1)}$ in $\mathbb{F}_2[x]$ gilt

- Bei Wahl des irreduziblen Polynoms $f(x) = x^3 + x^2 + 1$ ergeben sich zwar andere Rechenregeln für die Vektorenmultiplikation, man erhält aber dieselbe "Struktur" bei $+, \cdot$ 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. $\underline{\underline{(1,0,1)}} = \underline{\underline{x^2+1}}$ für die Elemente von $\mathbb{F}_8$ schreiben, um die Reduktion mod f zu verdeutlichen.

19.) **Bsp.:** Rechnen in $\mathbb{F}_{5^3} = \mathbb{F}_{125}$: Haben wir diesen Körper mit dem irreduziblen Polynom $f = x^3 + x + \underline{1} \in \mathbb{F}_5[x]$ 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. $(\underline{1}, \underline{2}, \underline{4}) \cdot (\underline{-1}, \underline{3}, \underline{0})$

$$= (x^2 + \underline{2}x - \underline{1})(-x^2 + \underline{3}x) = -x^4 + \underline{3}x^3 - \underline{2}x^3 + \underline{6}x + x^2 - \underline{3}x$$

$$= -x^4 + x^3 + x^2 + \underline{3}x = \underbrace{(x^3 + x + \underline{1}) \cdot (-x + \underline{1})}_{\text{Polydiv. durch } f} + \underline{2}x^2 + \underline{3}x + \underline{1}$$

$$= (\underline{2}, \underline{3}, \underline{1}) \bmod f,$$

"eigentlich" ja: $\underline{\underline{(1, 2, -1)}} \cdot \underline{\underline{(-1, 3, 0)}} = \underline{\underline{(2, 3, 1)}}$.

20.) **Bem.:** $\operatorname{char}(\mathbb{F}_{p^r}) = p$, denn es gilt $\underline{1} + \underline{1} + \ldots + \underline{1} = \overbrace{\underline{1 + \ldots + 1}}^{p \text{ mal}} = \underline{p \cdot 1} = \underline{0}$,
und p minimal so da p prim.

21.) **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 $f(x) = d(x - c_1) \cdots (x - c_m)$, die $c_i, d \in k$, gilt.

22.) **Bem.:** Man kann jeden Körper k in einen algebraisch abgeschlossenen Körper einbetten. Ein bzgl. "$\subseteq$" 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].