

# 4 Endliche Körper und der Satz von Chevalley

Schon bekannt:

- (1)  $\forall p \in \mathbb{P}$  gibt es den Körper  $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$  mit  $\#\mathbb{F}_p = p$
- (2) Hat man ein irred. Polynom (Primpolynom)  $g$  in  $R = \mathbb{F}_p[X]$  mit Grad  $g = n$ , so ist  $\bar{R} = R/gR$  ein Körper mit  $q = p^n$  Elementen, der  $\mathbb{F}_p$  als Teilkörper enthält.
- (3) Jeder endl. Körper  $L$  enthält primitives  $\zeta$ ,  $L^\times = L \setminus 0 = \{1, \zeta, \dots\}$ .

## 4.1 Untersuchung eines endl. Körpers $L$ mit $\#L = q$

$\text{ord}(1) = p = \min\{n \in \mathbb{N}_+ \mid n \cdot 1_L = 0\}$  (Ordnung in  $(L, +)$ , neutr. Element ist 0, statt  $x^n$  steht  $nx$ )

Beh.:  $p \in \mathbb{P}$

Ann.:  $p = uv$  zerlegbar,  $1 \leq u < p$ ,  $1 \leq v < p$ ,  $uv \cdot 1 = (u \cdot 1)(v \cdot 1) = 0$

$\Rightarrow u \cdot 1 = 0$  oder  $v \cdot 1 = 0$ , Widerspruch.  $\Rightarrow L$  enthält  $\mathbb{F}_p$ , wenn man  $\mathbb{F}_p \cong \text{Versys}_p = \{0, \dots, p-1\} \ni z$  nimmt und  $z \cdot 1$  mit  $\bar{z}$  identifiziert (inj. Ringhomomorphismus  $\mathbb{F}_p \rightarrow L$ ,  $\bar{z} \mapsto z \cdot 1$ )

Außerdem ist  $L$  ein  $\mathbb{F}$ -Vektorraum, wenn die Skalarmultiplikation so erklärt wird:

$\alpha \in L, \bar{z} \in \mathbb{F}_p : \bar{z}\alpha = (z \cdot 1) \cdot \alpha$  (VR-Axiome leicht nachprüfbar!)

$\#L = q < \infty \Rightarrow n := \dim L < \infty$ .

LA I: Basiswechsel liefert einen VR-Isomorphismus  $L \rightarrow \mathbb{F}_p^n$

$\Rightarrow q = \#L = \#\mathbb{F}_p^n = p^n$

- (1) Gesucht zu  $n \in \mathbb{N}_+, p \in \mathbb{P}$  ein Körper mit  $q = p^n$  Elementen.
- (2) Wie eindeutig ist  $L$ . (Wunsch: Je zwei solche  $L$ 's sind isomorph)

Idee: "Kleiner Fermat" gilt in  $L$ , d.h.  $\forall \alpha \in L : \alpha^q = \alpha$

$\Rightarrow L$  besteht aus allen Nullstellen  $\alpha$  von  $X^q - X$

$\Rightarrow X^q - X = \prod_{\alpha \in L} (X - \alpha)$

Suche "große" Körper  $K \supset \mathbb{F}_p$ , so dass  $X^q - X$  so zerfällt!

Hoffnung: Die Nullstellen  $\alpha$  von  $X^q - X$  bilden dann den gesuchten Körper.

Durchführung der Idee: Kette von Hilfssätzen

**Hilfssatz (1)**

Ist  $R$  ein Ring der  $\mathbb{F}_p$  als Teilring enthält, so gilt  $\forall \alpha, \beta \in R, n \in \mathbb{N}_+, a = p^n$

$$(\alpha \pm \beta)^a = \alpha^a \pm \beta^a$$

**Beweis**

In  $\mathbb{Z}$  gilt für  $1 \leq i \leq p$ :  $(1 \cdot 2 \cdot \dots \cdot i) \binom{p}{i} = p \cdot (p-1) \cdot \dots \cdot (p-i+1)$  In  $\mathbb{F}_p$  gilt für  $1 \leq i \leq p$ :  $\underbrace{(\overline{1} \cdot \overline{2} \cdot \dots \cdot \overline{i})}_{\in \mathbb{F}_p^x} \overline{\binom{p}{i}} = \overline{0} \dots = \overline{0}$

$$\Rightarrow \overline{\binom{p}{i}} = \overline{0}$$

$$\Rightarrow (\alpha + \beta)^p = \alpha^p + \beta^p + \sum_{i=1}^{p-1} \binom{p}{i} \alpha^i \beta^{p-i} = \alpha^p + \beta^p, \text{ ok für } n = 1 \text{ (- ähnlich)}$$

Rest Induktion, sei  $j > 1$

$$(\alpha + \beta)^{p^j} = (\alpha + \beta)^{p^{j-1} \cdot p} = (\alpha^{p^{j-1}} + \beta^{p^{j-1}})^p = \alpha^{p^{j-1} \cdot p} + \beta^{p^{j-1} \cdot p} = \alpha^{p^j} + \beta^{p^j} \quad \blacksquare$$

**Hilfssatz (2)**

Sei  $K$  ein Körper, der  $\mathbb{F}_p$  als Teilkörper enthält, so dass  $(q = p^n, n \in \mathbb{N}_+)$

$$X^q - X = \prod_{j=0}^{q-1} (X - \alpha_j) \text{ mit } \alpha_0, \dots, \alpha_{q-1} \in K$$

Dann ist  $L := \{\alpha_0, \dots, \alpha_{q-1}\}$  ein Körper mit  $q$  Elementen.

**Beweis**

$$K \ni \alpha \text{ Nullstelle von } X^q - X \Leftrightarrow \alpha^q - \alpha = 0 \Leftrightarrow \alpha^q = \alpha$$

$$\alpha \in L \Leftrightarrow \alpha^q = \alpha$$

Prüfe nach:  $(L, +)$  ist Untergruppe von  $(K, +)$ ,  $(L^x = L \setminus \{0\}, \cdot)$  ist Untergruppe von  $(K^x, \cdot) \Leftrightarrow$  Teilkörper,  $\mathbb{F}_p \subseteq L$  wegen  $\alpha^p = \alpha = \alpha^q$  für  $\alpha \in \mathbb{F}_p$

$$0 \in L \neq \emptyset$$

$$\alpha, \beta \in L \Rightarrow \alpha^q = \alpha, \beta^q = \beta \Rightarrow (\alpha - \beta)^q = \alpha^q - \beta^q \text{ (HS1)} = \alpha - \beta \Rightarrow \alpha - \beta \in L \text{ also } L \text{ Untergruppe von } K.$$

$$\text{Analog } L^x \alpha, \beta \in L^x \Rightarrow \alpha^q = \alpha, \beta^q = \beta \Rightarrow \alpha^q (\beta^q)^{-1} = \alpha \beta^{-1} \Rightarrow \alpha \beta^{-1} \in L^x, \text{ also } L^x \text{ Untergruppe von } K^x.$$

Wieso  $\#L = q$ ? Wieso hat  $X^q - X$  in  $K$  nur einfache Nullstellen?

$$\alpha \in L, \text{ Wende HS1 an auf } K[X]$$

$$X^q - X = (X - \alpha)^q = X^q - \alpha^q - (X - \alpha) \Rightarrow 0 = (X - \alpha)^q - (X - \alpha) = (X - \alpha) ((X - \alpha)^{q-1} - 1),$$

$$\alpha \text{ ist nicht Nullstelle von } (X - \alpha)^{q-1} - 1$$

$$\text{Die NST ist einfach, Hinweis: } L = \{\zeta - \alpha | \zeta \in L\} \quad \blacksquare$$

Existenz von  $L$ : Suche  $K \supseteq \mathbb{F}_p$  (Körper), so dass  $K$   $q$  NST von  $X^q - X$  enthält.

**Hilfssatz (3)**

Ist  $K$  ein Körper,  $f \in K[X]$ , Grad  $f > 0$ ,  $K \supseteq \mathbb{F}_p$  (als Teilkörper), so gibt es einen endl. Körper  $\tilde{K}$ , der  $K$  (und damit  $\mathbb{F}_p$ ) als Teilkörper enthält und ein  $\alpha \in \tilde{K}$  mit  $f(\alpha) = 0$

**Beweis**

Primzerlegung von  $f$ , sei  $f = g_1^{m_1} \cdot \dots \cdot g_t^{m_t}$ ,  $g_j$  irred. in  $K[X]$  (EuFa-Satz)

$$f(\alpha) = 0 \Rightarrow 0 = g_1(\alpha)^{m_1} \cdot \dots \cdot g_t(\alpha)^{m_t} \Rightarrow \exists j : g_j(\alpha) = 0$$

So ein  $\alpha$  ist gesucht! (und  $\tilde{K}$ )

$\tilde{K} := K[X]/g_j K[X]$  ist ein Körper, der  $K$  als Teilkörper enthält.

$$\alpha = \overline{X} \text{ ist NST von } g_j, \text{ also } f! \ g_j(\overline{X}) = \overline{g_j(X)} = \overline{0} = 0 \quad \blacksquare$$

**Hilfssatz (4)**

Es gibt einen endl. Körper  $K$ , in dem  $f \in \mathbb{F}_p[X]$  (Grad  $f > 0$ ,  $f$  normiert) in Linearfaktoren zerfällt, d.h.

$$f = \prod_{j=1}^m (X - \alpha_j) \quad (\alpha_1, \dots, \alpha_m \in K)$$

**Beweis**

Induktion nach  $m = \text{Grad } f$ ,  $m = 1$ ,  $f = X - \alpha$ ,  $\alpha \in \mathbb{F}_p$

$m > 1$   $\tilde{\mathbb{F}}_p$  nach HS3 mit  $\alpha \in \tilde{\mathbb{F}}_p$ ,  $f(\alpha) = 0$   
 $\Rightarrow X - \alpha \mid f$  in  $\tilde{\mathbb{F}}_p[X]$   
 $\Rightarrow f = (X - \alpha)\tilde{f}$ ,  $\text{Grad } \tilde{f} = \text{Grad } f - 1$   
 IH für  $\tilde{f} \Rightarrow \text{Beh.}$  ■

**Hilfssatz (5)**

Sei  $M$  ein Körper mit  $p^n$  Elementen,  $R = \mathbb{F}_p[X]$ ,  $\xi \in M$ ,  $g \in R$  mit  $g(\xi) = 0$  und  $g$  irreduzibel.

Ist dann entweder  $\text{grad } g = n$  oder  $\xi$  ein primitives Element von  $M$ , so sind die Körper  $M$  und  $R/gR = \bar{R}$  isomorph. Ein irreduzibles Polynom, das  $\xi$  als Nullstelle hat, hat den Grad  $n$ .

**Beweis**

$\psi : \bar{R} \rightarrow M, \bar{h} \mapsto h(\xi) = \psi(\bar{h})$  ist der gesuchte Isomorphismus.

(1)  $\psi$  ist wohldefiniert:

$$\begin{aligned} \bar{h}_1 = \bar{h}_2 &\iff h_1 \equiv h_2 \pmod{g} \\ &\iff \exists u \in R : h_2 = h_1 + ug \\ &\implies h_2(\xi) = h_1(\xi) + u(\xi) \cdot g(\xi) = h_1(\xi) \end{aligned}$$

(2)  $\psi$  ist ein Ringisomorphismus, also  $\psi(\bar{h}_1 + \bar{h}_2) = \psi(\bar{h}_1) + \psi(\bar{h}_2)$ :

Klar wegen  $(h_1 \pm h_2)(\xi) = h_1(\xi) \pm h_2(\xi)$

(3)  $\psi$  ist injektiv:

Es genügt zu zeigen:  $\text{Kern } \psi = \{0\}$ .

Ann:  $\alpha \in \text{Kern } \psi$ ,  $\alpha \neq 0$ .  $1 = \psi(1) = \psi(\alpha^{-1}\alpha) = \psi(\alpha^{-1})\psi(\alpha) = 0$ , Wid!

(4)  $\psi$  ist surjektiv:

a)  $\text{grad } g = n \implies \#\bar{R} = p^n$ ,  $\psi : M \rightarrow \bar{R}$  injektiv. Da  $\#M = p^n \implies \psi$  surjektiv.

b)  $\xi$  primitiv  $\iff M = \{0, \xi, \xi^2, \dots, \xi^{q-2}\}$ .  $\psi(\bar{R}) \ni h(\xi)$  für z.B.  $h = X^n$  ( $n \in \mathbb{N}$ )  
 $\implies \psi(\bar{R}) \ni X^n(\xi) = \xi^n \implies \psi(\bar{R}) \supseteq M \implies \psi$  surjektiv. ■

**Satz 4.1 (Endliche-Körper-Raum)**

- (1) Ist  $L$  ein endlicher Körper,  $\#L = q$ , dann  $\exists p \in \mathbb{P}$ ,  $n \in \mathbb{N}_+$  mit  $q = p^n$ . (Genauer: Dann ist  $\mathbb{F}_p$  ein Teilkörper von  $L$  und  $L$  ein  $\mathbb{F}_p$ -Vektorraum der Dimension  $n$ ).
- (2) Zu jedem  $n \in \mathbb{N}_+$ ,  $p \in \mathbb{P}$ , existiert ein Körper mit  $q = p^n$  Elementen. Zusätzlich gilt: Es gibt ein irreduzibles Polynom  $g \in \mathbb{F}_p[X]$  mit  $\text{grad } g = n$ . Es ist  $g \mid X^q - X$ .
- (3) Je zwei Körper mit  $q$  Elementen sind isomorph.

Also ist es gerechtfertigt, von dem Körper  $\mathbb{F}_q$  oder  $GF(q)$  zu sprechen.

### Beweis

- (1) Wurde bereits geleistet. (Aber wo?)
- (2) Erinnerung: Es gibt einen Körper  $K$ , der  $\mathbb{F}_p$  enthält, so dass  $X^q - X = \prod_{j=0}^{q-1} (X - \alpha_j)$ , ( $\alpha_j \in K$ ),  $L = \{\alpha_j \mid j = 0, \dots, q-1\}$  ist Körper mit  $q$  Elementen.
- (3)  $M, L$  seien Körper mit  $q = p^n$  Elementen.  $\xi$  sei ein primitives Element von  $M$  (Existenz: Satz vom primitiven Element).  $X^q - X = \prod_{\alpha \in L} (X - \alpha)$ . Betrachte die Primzerlegung  $X^q - X = \prod_{j=1}^t p_j^{n_j}$  in  $\mathbb{F}_p[X]$ ,  $p_j$  irreduzibel in  $R$ , die es nach dem EuFa-Satz gibt.

Wegen  $(X^q - X)(\xi) = 0 = \prod_{j=1}^t p_j(\xi)^{n_j}$  existiert ein  $j \in \{1, \dots, t\}$ ,  $p_j(\xi) = 0$ ,  $p_j = g$  irreduzibel in  $\mathbb{F}_p[X]$ . Hilfssatz 5 liefert:  $M \cong R/gR$  und  $\text{grad } g = n$  (wo  $\#M = p^n$ ). Wir folgern also: Jedes  $p_j$  (also auch  $g$ ) ist Produkt gewisser  $(X - \alpha)$  (EuFa-Satz für  $L[X]$ )  $\implies \exists \alpha \in L : X - \alpha \mid g \implies g(\alpha) = 0$ . Wir benutzen nun den Hilfssatz für  $L$  statt  $M$  und erhalten:  $\overline{R} = R/gR \cong L$ . Damit erhalten wir:  $L \cong M$ . ■

#### Satz 4.2 (Teilkörpersatz)

- (1) Sei  $K$  ein Teilkörper von  $\mathbb{F}_q$  mit  $q = p^n$  wie oben. Dann existiert ein  $d \in \mathbb{N}$  mit  $d \mid n$  und  $K \cong \mathbb{F}_{p^d}$ .
- (2) Ist  $d \mid n$ , so gibt es genau einen Teilkörper von  $\mathbb{F}_q$  mit  $\#K = p^d$

Fazit: Teilkörper entsprechen bijektiv den Teilern  $d$  von  $n$ .

### Beweis

**Bemerkung:** Ist  $K$  ein Teilkörper von  $L$ , so ist  $L$  ein  $K$ -Vektorraum (Skalare Multiplikation ist die von  $L$ ).

Also ist  $\mathbb{F}_q$  ein  $K$ -Vektorraum  $\implies$  (Basiswahl)  $\mathbb{F}_q \cong K^{d'}$ ;  $d'$  ist die Dimension des  $K$ -Vektorraums  $\mathbb{F}_q = q^n = q = \#K_q = (p^d)^{d'}$ , (da  $\#K = p^d$ )  $\implies n = dd' \implies d \mid n$ .

Ist  $\#K = p^d$ ,  $d \mid n$ ,  $K$  Teilkörper von  $\mathbb{F}_q$ , so muss  $K$  aus den Nullstellen von  $X^{p^d} - X$  in  $\mathbb{F}_p$  bestehen, also ist  $K$  eindeutig bestimmt. ( $K = \{\alpha^{p^{\frac{n}{d}}} \mid \alpha \in \mathbb{F}_p\}$ ). ■

## 4.2 Die Sätze von Chevalley und Warming

Es sei generell hier  $K = \mathbb{F}_q$ ,  $q = p^n$  wie oben, mit dem wichtigsten Fall  $n = 1$ ,  $K = \mathbb{F}_p$ .

Das Problem ist:  $f \in K[X_1, \dots, X_n]$  liege vor mit  $f(\underline{0}) = 0$ ,  $\underline{0} = (0, \dots, 0) \in K^n$ . Gesucht: Möglichst gute Bedingungen, so dass  $f$  eine nicht-triviale Nullstelle  $\underline{x} = (\alpha_1, \dots, \alpha_n) \in K^n$  besitzt. (nicht-trivial:  $\underline{x} \neq \underline{0}$ ).

Bezeichnungen:

- (1)  $f = \sum_{\underline{m} \in \mathbb{N}^n} \alpha_{\underline{m}} X^{\underline{m}}$ , wobei  $\underline{m} = (m_1, \dots, m_n)$ ,  $\underline{0} = (0, \dots, 0)$ ,  $\alpha_{\underline{m}} \in K$ , davon nur endlich viele  $\neq 0$ .
- (2)  $X^{\underline{m}} := X_1^{m_1} \dots X_n^{m_n}$

- (3) Setze  $|\underline{m}| = m_1 + \dots + m_n$ . Damit ist der Gesamtgrad  $\text{grad } f$  wie folgt definiert:  $\text{grad } 0 = -\infty$ ,  $f \neq 0$ :  $\text{grad } f = \max\{|\underline{m}| \mid \alpha_m \neq 0\}$ .

**Satz 4.3 (von Warming)**

Sei  $f \in \mathbb{F}_q[X_1, \dots, X_n]$ ,  $\text{grad } f < n$ . Dann ist die Anzahl der Nullstellen von  $f$  in  $\mathbb{F}_q^n$  durch  $p$  teilbar.

Dabei heißt  $\mathcal{V}_f(K) := \{\underline{x} \in K^n \mid f(\underline{x}) = 0\}$  die Nullstellenmannigfaltigkeit von  $f$  in  $K$ .

Allgemeiner:  $f_1, \dots, f_l \in K[X_1, \dots, X_n]$ :  $\mathcal{V}_{f_1, \dots, f_l}(K) = \{\underline{x} \in K^n \mid f_1(\underline{x}) = \dots = f_l(\underline{x}) = 0\} = \bigcap_{i=1}^l \mathcal{V}_{f_i}(K)$

Die Aussage des Satzen ist nun: Ist  $\text{grad } f < n$ , so gilt  $p \mid \#\mathcal{V}_f(K)$

**Satz 4.4 (Satz von Chevalley)**

Sei  $f \in K[X_1, \dots, X_n]$ ,  $f(\underline{0}) = 0$  und  $\text{grad } f < n$ . Dann hat  $f$  eine nichttriviale Nullstelle.

Es ist klar: Satz von Warming impliziert den Satz von Chevalley, da:  $f(\underline{0}) = 0 \implies \underline{0} \in \mathcal{V}_f(K) \implies \#\mathcal{V}_f(K) > 0$ .  $p \mid \#\mathcal{V}_f(K) \implies \#\mathcal{V}_f(K) \geq p \geq 2$

Spezielles Beispiel:

**Satz 4.5**

Seien  $\alpha_1, \dots, \alpha_{n+1} \in \mathbb{Z}$ ,  $d \leq n$ ,  $d \in \mathbb{N}$ . Dann hat die Kongruenz  $\alpha_1 x_1^d + \dots + \alpha_{n+1} x_{n+1}^d \equiv 0 \pmod{p}$  stets eine nicht-triviale Lösung  $x = (x_1, \dots, x_n) \in \mathbb{Z}^{n+1}$

Noch spezieller:  $\alpha_1 x_1^2 + \alpha_2 x_2^2 + \alpha_3 x_3^2 \equiv 0 \pmod{p}$  hat stets nicht-triviale Lösung  $(x_1, x_2, x_3) \in \mathbb{Z}$ .

**Beweis**

$\text{grad } \alpha_1 x_1^d + \dots + \alpha_{n+1} x_{n+1}^d \leq d \leq n+1$  (Variablenzahl). Satz von Chevalley liefert die Behauptung. ■

Gegenbeispiel:  $x_1^2 + x_2^2 \equiv 0 \pmod{3}$ :  $x_j^2 \in \{0, 1\} \implies$  Jede Lösung hat  $3 \mid x_1$  und  $3 \mid x_2$

Weitere Sätze (siehe z.B. Lidl/Niederreiter, Finite Fields):

**Satz 4.6 (Satz I)**

Sei  $d = \text{grad } f_1 + \dots + \text{grad } f_l < n$  und  $f_j \in \mathbb{F}_q[X_1, \dots, X_n]$ . Falls  $\mathcal{V}_{f_1, \dots, f_l}(\mathbb{F}_q) \neq \emptyset$ , so gilt:  $\#\mathcal{V}_{f_1, \dots, f_l}(\mathbb{F}_q) \geq q^{n-d}$

**Satz 4.7 (Satz II)**

Falls  $f \in \mathbb{F}_1[X_1, \dots, X_n]$ ,  $0 < \text{grad } f = d$ , so gilt:  $\#\mathcal{V}_f(\mathbb{F}_q) \leq d \cdot 1^{n-1}$

**Satz 4.8**

Sei  $0 \neq f \in \mathbb{Z}[X_1, \dots, X_n]$ . Dann gibt es eine konstante  $c_f$  unabhängig von  $p$ , so dass

$$\forall p \in \mathbb{P} : |\#\mathcal{V}_f(\mathbb{F}_q) - p^{n-1}| \leq c_f \frac{p^{n-1}}{\sqrt{p}}$$

Der Beweis ist äußerst schwierig, bereits für  $n = 2$ .

**Beweis**

Der Beweis des Satzes von Warming ?? gliedert sich in mehrere Ideen, wie bringen sie hier schön isoliert. In vielen Büchern ist der Beweis ziemlich unübersichtlich.

Idee 1: Das Kronecker- $\delta$  ist als Polynom darstellbar.

**Lemma 4.9**

$\delta : K \rightarrow K$  sei definiert wie folgt:

$$\delta(\alpha) = \delta_0(\alpha) = \begin{cases} 1, & \alpha = 0 \\ 0, & \text{sonst} \end{cases}$$

Dann  $\delta(\alpha) = 1 - \alpha^{q-1} = (1 - X^{q-1})(\alpha)$ , weil  $\alpha^{q-1} = 1$ , wenn  $\alpha \in K^\times = \mathbb{F}_q^\times$  und  $\alpha^{q-1} = 0$ , wenn  $\alpha = 0$ .

**Satz 4.10**

Jede Funktion  $\mathbb{F}_1 \rightarrow \mathbb{F}_1$  ist als Polynom darstellbar.

**Beweis**

Übung. ■

Idee 2: Aus  $f$  kann man eine Funktion  $F$  konstruieren, so dass  $F$  die Nullstellen von  $f$  zählen hilft.

$F = A - f^{q-1}$ . Dann

$$F(x) = 1 - f(x)^{q-1} = \delta_{0, f(x)} = \begin{cases} 1, & x \in V_f(K) \\ 0, & \text{sonst} \end{cases}$$

Es folgt die Formel  $\sum_{x \in K^n} \delta_{0, f(x)} = \#\mathcal{V}_f(K) \cdot 1_K$ .

Idee 3: Versuche die linke Seite der Formel zu berechnen, nämlich  $\sum_{x \in K^n} g(x)$ ,  $g \in K[X_1, X_2, \dots, X_n]$ .  
 Beginne mit  $n = 1$ ,  $g = X^k$ .  $\sum_{\alpha \in K} \alpha^k = ?$ .

**Lemma 4.11**

Ist  $k \in \mathbb{N}$  und  $k = 0$  oder  $q - a \nmid k$ , so ist  $\sum_{\alpha \in K} \alpha^k = 0$  (Dabei muss  $0^0 = 1$  definiert werden).

**Beweis**

$k = 0$ :  $\sum_{\alpha \in K} \alpha^0 = \sum_{\alpha \in K} 1 = q \cdots 1_K = 0$  und  $1_K q = p^n$ .

$k > 0$ : Dann existiert ein primitives Element  $\xi \in K$ , das heißt,  $K^\times = K \setminus \{0\} = \{1, \xi, \xi^2, \dots, \xi^{q-2}\}$  und  $\text{ord } \xi = q - 1$ , daraus folgt  $\xi^k \neq 1$  (laut Elementarordnungssatz).

$$\sum_{\alpha \in K} \alpha^k = \sum_{\alpha \in K \setminus \{0\}} \alpha^k = \sum_{j=0}^{q-2} \xi^{j-k} = \sum_{j=0}^{q-2} (\xi^k)^j = \frac{\xi^{k(q-1)} - 1}{\xi^k - 1} \text{ (geometrische Reihe!)}$$

(wegen  $\xi^{q-1} = 1$ ). ■

**Lemma 4.12**

Sei  $g \in K[X_1, X_2, \dots, X_n]$ ,  $\text{grad } g < n(q - 1)$ , dann ist  $\sum_{x \in K^n} g(x) = 0$ .

**Beweis**

Ohne Beschränkung der Allgemeinheit ist  $g = x^m$  mit  $|m| < n(q - 1)$ ,  $m \in K^n$ , denn wenn  $g = \sum \beta_m X^m$ , dann  $\forall m$  mit  $\beta_m \neq 0$ :  $|m| < n(q - 1)$ , denn die Summe von Nullen ergibt null. Weiterhin gilt

$$\sum_{x \in K^n} X^m(x) = \sum_{(\alpha_1, \alpha_2, \dots, \alpha_n) \in K^n} \alpha_1^{m_1} \cdot \alpha_2^{m_2} \cdot \dots \cdot \alpha_n^{m_n}$$

(Durch Ausmultiplizieren erhält man

$$\prod_{j=1}^n \left( \sum_{\alpha_j \in K} \alpha_j^{m_j} \right) = \sum_{(\alpha_1, \alpha_2, \dots, \alpha_n) \in K^n} \alpha_1^{m_1} \cdot \alpha_2^{m_2} \cdot \dots \cdot \alpha_n^{m_n}.$$

(Kann man, wenn man Lust hat, mit Induktion beweisen))

Voraussetzung:  $m_1 + m_2 + \dots + m_n < n(q - 1) \implies \exists j \in \{1, 2, \dots, n\}$  mit  $m_j < q - 1 \implies m_j = 0$  oder  $q - 1 \mid m_j$ . Anwendung von Lemma 4.11 mit  $k = m_j$

$$\implies \sum_{\alpha_j \in K} \alpha_j^{m_j} = 0 \implies \prod \sum \alpha_j^{m_j} = 0 = \sum X^m(x). \quad \blacksquare$$

Wende das Lemma 4.12 an auf  $g = F = 1 - f^{q-1}$ .  $\text{grad } g = (q - 1) \underbrace{\text{grad } f}_{< n} \implies \text{grad } g < (q - 1)n$ , also kann letztes Lemma angewandt werden

$$\implies \sum_{x \in K^n} F(x) = 0 = \#V_f(K) \cdots 1_K \implies p = \text{ord } 1_K \mid \#V_f(K). \quad \blacksquare$$

