Endliche Körper und der Satz von Chevalley

Wie versprochen, enthält diese Vorlesung mehr Information zu endlichen Körpern als üblicherweise in der ELEMENTAREN ZAHLLENTHEORIE angeboten wird. Gewöhnlich werden diese im Rahmen der allgemeinen Körpertheorie in der ALGEBRA behandelt. Da dafür in dieser Vorlesung nicht Zeit ist, habe ich die Beweise so gefaßt, dass sie mit den wenigen Methoden aus der Algebra, die in dieser Vorlesung verwendet werden, zu verstehen sind. Einerseits weicht die Darstellung dadurch von anderen Büchern ab, andererseits aber erspart das dem Leser das Studium der Algebra, die in Büchern über endliche Körper wie Lidl, Niederreiter,*Finite Fields*, Encyclopedia of Mathematics and its applications, Vol. 20, 1983 berichtet oder vorausgesetzt wird.
Vielleicht wird das aber den einen oder anderen Hörer zu einem vertieften Studium der ALGEBRA anregen. Allerdings wird der Satz von Chevalley gewöhnlich in Algebra-Vorlesungen nicht behandelt.

Erst einmal soll kurz rekapituliert werden, was wir über endliche Körper schon wissen: Für jeder Primzahl p haben wird den Restklassen-Körper $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ mit p Elementen, in dem wir mittels eines Vertretersystems Versys_p rechnen. Weiter ist $R = \mathbb{F}_p[X]$ euklidisch, also nach dem EuFa-Satz faktoriell. Hat man ein irreduzibles Polynom (Primpolynom) g in R vom Grad n, so ist $\mathbb{F}_q := R/gR$ ein Körper mit $q := p^n$ Elementen. Wir wissen auch, dass $\mathbb{F}_q$ wie jeder endliche Körper L ein primitives Element enthält, dessen Potenzen die multiplikative Gruppe $L^\times = L \setminus \{0\}$ von L bilden. Weiter enthält $\mathbb{F}_q$ den Körper $\mathbb{F}_p$, wenn man die Elemente von $\mathbb{F}_p$ als konstante Polynome $\bmod g$ betrachtet.
Was uns noch fehlt, ist die Einsicht, dass es zu jedem n ein Primpolynom in $\mathbb{F}_p[X]$ vom Grad n gibt und dass man so im Wesentlichen alle endlichen Körper erhält. Diese Einsichten werden durch eine Reihe von Hilfssätzen gewonnen.

Hilfssatz 1 Ist L ein endlicher Körper, so gibt es eine Primzahl $p \in \mathbb{P}$, so dass L (bis auf Isomorphie) den Körper $\mathbb{F}_p$ enthält. L ist dann ein Vektorraum über $\mathbb{F}_p$ und hat $q = p^n$ Elemente ($n = \dim(L)$ als Vektorraum).

Beweis: Ist p die Ordnung von $1 = 1_L$ in der additiven Gruppe von L, so ist p prim. Denn eine Zerlegung $p = uv$ mit $1 < u < p$ ergibt $0 = (u \cdot 1)(v \cdot 1)$ und daher $u \cdot 1 = 0$ oder $v \cdot 1 = 0$ im Widerpruch zur Minimaleigenschaft in der Definition der Elementordnung.
Nun ist leicht zu sehen, dass $\mathbb{F}_p$ als Teilköper betrachtet werden kann, indem man $\overline{z} \in \mathbb{F}_p$, $z \in \text{Versys}_p$ mit $z \cdot 1 = 1 + \ldots + 1$ (z Summanden) identifiziert. Ebensoleicht prüft man nach, dass die Vektorraumaxiome gelten, wenn man als skalares Produkt für $\overline{z}$, $z \in \text{Versys}_p$ und $\alpha \in L$ definiert

$$\overline{z}\alpha = z \cdot \alpha = \alpha + \ldots + \alpha,$$

(z Summanden). Durch Wahl einer Vektorraumbasis stellt man in der LINEAREN ALGEBRA dann eine Vektorraumismorphismus $L \cong \mathbb{F}_p^n$ her. Daher ist $\#L = \#\mathbb{F}_p^n = p^n$. **q.e.d.**

Nunmehr wollen wir einen endlichen Körper L mit $\mathbb{F}_p$ als Teilkörper und p^n Elementen konstruieren, ohne dass wir im Besitz eines Primpolynoms vom Grad n sind. Wenn wir L schon hätten, so gälte für $\alpha \in L$ der kleine Fermat, nämlich $\alpha^q = \alpha$ (Erinnerung: Nach dem Elementordnungssatz ist $\alpha^{q-1} = 1$ für $\alpha \in L^\times$). Das besagt genau, dass L aus den q Nullstellen des Polynoms $X^q - X$ besteht. Daraus folgt in $L[X]$ die Primzerlegung

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

Das legt nahe, erst einen Körper K zu konstruieren, der $\mathbb{F}_p$ enthält, so dass $X^q - X$ in $K[X]$ in ein Produkt von Linearfaktoren zerfällt und dann zu beweisen, dass die Nullstellen dieses Polynoms einen Körper mit q Elementen bilden.

Die erste Teilaufgabe ist gelöst im

Hilfssatz 2 Sei k ein Körper und $f \in k[X]$ ein normiertes Polynom des Grads $n > 0$. Dann existieren

(i) ein Körper k_1 , der k als Teilkkörper enthält und eine Nullstelle α von f ,

(ii) ein Körper K , der k als Teilkörper enthält und Elemente $\alpha_1, \ldots, \alpha_n \in K$ mit

$$f = \prod_{j=1}^{n} (X - \alpha_j).$$

Beweis: (i) Nach dem EuFa-Satz hat man von $f = gh$ mit einem Primteiler g von f in $R := k[X]$. Der Körper $k_1 := R/gR$ enthält k , wenn wir wie immer die Elemente von k mit konstanten Polynomen $\mod g$ identifizieren. $\alpha := \overline{X}$ ist die gesuchte Nullstelle wegen $g(\alpha) = g(\overline{X}) = \overline{g(X)} = \overline{0} = 0$, also auch $f(\alpha) = g(\alpha)h(\alpha) = 0$.

(ii) wird nun leicht durch Induktion nach $n = \mathrm{Grd}(f)$ gesehen. $n = 1$ besagt $f = X - \alpha$ und $\alpha \in k$, man kann dann $K = k$ nehmen. Für $n > 1$ haben wir k_1 und eine Nullstelle $\alpha_1 \in k_1$ gefunden. Aus $f(\alpha_1) = 0$ folgt in $k_1[X]$, dass $X - \alpha_1$ ein Teiler von f ist. Damit hat man ein Polynom $f_1 \in k_1[X]$ mit $f = (X - \alpha_1)f_1$. Die Anwendung der Induktionshypothese auf k_1, f_1 statt k, f ergibt dann die Behauptung. **q.e.d.**

Hilfssatz 3 Sei $p \in \mathbb{P}$, $q = p^n$ und R ein Ring, der $\mathbb{F}_p$ als Unterring enthält. Dann gelten für $\alpha, \beta \in R$.

$$(\alpha + \beta)^q = \alpha^q + \beta^q, \quad (\alpha - \beta)^q = \alpha^q - \beta^q.$$

Beweis: Für den Binomialkoeffizienten $\binom{p}{j}$ ist bekanntlich

$$1 \cdots j \cdot \binom{p}{j} = p(p-1) \cdots (p-j+1).$$

Liest man das $\mod p$, so wird für $1 \leq j \leq p-1$ in $\mathbb{F}_p$

$$\overline{\binom{p}{j}} = 0.$$

(links von $\overline{\binom{p}{j}}$ stehen Elemente $\neq 0 \in \mathbb{F}_p$). Demnach erhält man für die Binomialentwicklung, wenn man $z \cdot 1 = \overline{z} \cdot 1$ beachtet:

$$(\alpha+\beta)^p = \alpha^p + \sum_{j=1}^{p-1} \binom{p}{j} \cdot 1 \cdot \alpha^j \beta^{p-j} + \beta^p = \alpha^p + \beta^p.$$

Das ist der Fall $n = 1$ und für $n > 1$ ist der Induktionsschritt leicht getan:

$$(\alpha+\beta)^{p^n} = (\alpha+\beta)^{p^{n-1} \cdot p} = (\alpha^{p^{n-1}} + \beta^{p^{n-1}})^p = \alpha^{p^{n-1}p} + \beta^{p^{n-1}p} = \alpha^{p^n} + \beta^{p^n}.$$

Der Fall $\alpha - \beta$ ergibt sich nun aus $(-1)^q = -1$. Das stimmt auch für $p = 2$, weil in $\mathbb{F}_2$ die Gleichung $1 = -1$ richtig ist. **q.e.d.**

Hilfssatz 4 Sei K ein Körper, der $\mathbb{F}_p$ als Teilkörper enthält und $q = p^n$. Es gebe $\alpha_0, \ldots, \alpha_{q-1} \in K$, derart dass $X^q - X = \prod_{j=0}^{q-1}(X - \alpha_j)$.
Dann ist $L := \{\alpha_j \mid j = 1 \ldots q-1\}$ ein Köper mit q Elementen, der $\mathbb{F}_p$ als Teilkörper enthält.
Beweis: Für $\alpha \in K$ gilt offensichtlich: $\alpha \in L \Leftrightarrow \alpha^q = \alpha$. Ist $\alpha \in \mathbb{F}_p$, so ist (kleiner Fermat) $\alpha^p = \alpha$, woraus induktiv $\alpha^q = \alpha$. Hiernach ist $\mathbb{F}_p$ ein in L enthaltener Körper, erst recht ist L und $L^\times$ nichtleer. Für $\alpha, \beta \in L$, also $\alpha^q = \alpha$, $\beta^q = \beta$ sagt uns Hilfssatz 3: $(\alpha-\beta)^q = \alpha^q - \beta^q = \alpha - \beta$, demnach $\alpha - \beta \in L$. Noch einfacher ist der Fall $\alpha, \beta \in L^\times$, wo $\frac{\alpha}{\beta} \in L$ aus $(\frac{\alpha}{\beta})^q = \frac{\alpha^q}{\beta^q} = \frac{\alpha}{\beta}$ ersichtlich ist. Hiernach ist $(L, +)$ eine Untergruppe von $(K, +)$ und $L^\times$ eine Untergruppe von $K^\times$. Daher ist L ein Teilkörper von K.
Wir müssen uns noch überzeugen, dass L q Elemente hat, d.h. jede Nullstelle α von $X^q - X$ eine einfache Nullstelle ist. Dazu berechnen wir mit Hilfssatz 3, angewandt auf den Ring $K[X]$

$$(X-\alpha)((X-\alpha)^{q-1} - 1) = (X-\alpha)^q - (X-\alpha) = X^q - \alpha^q - X + \alpha = X^q - X.$$

Da offensichtlich α keine Nullstelle von $(X-\alpha)^{q-1} - 1$ ist, ist die Nullstelle α von $X^q - X$ einfach. **q.e.d.**
Ein letzter Hilfssatz befasst sich mit der Isomorphie solcher Körper:

Hilfssatz 5 Es sei $g \in R = \mathbb{F}_p[X]$ irreduzibel und M ein Körper mit p^n Elementen ($n \in \mathbb{N}_+$) und ξ eine Nullstelle von g in M. Ist dann entweder $\mathrm{Grd}(g) = n$ oder ξ ein primitives Element von M, so sind die Körper M und $\overline{R} = R/gR$ isomorph. Ist also das primitive Element ξ Nullstelle eines irreduziblen Polynoms g, so hat dieses Polynom den Grad n.
Beweis: Wir betrachten die Abbildung

$$\lambda : \overline{R} \to M,\ \overline{h} = h + gR \mapsto h(\xi).$$

Wir wollen zeigen: Unter obigen Voraussetzungen ist λ ein Isomorphismus. Dazu müssen wir nachprüfen:
(i) λ ist wohldefiniert,
(ii) $\lambda(\overline{h}_1 + \overline{h}_2) = \lambda(\overline{h}_1) + \lambda(\overline{h}_2)$,
$\lambda(\overline{h}_1\overline{h}_2) = \lambda(\overline{h}_1)\lambda(\overline{h}_2)$ (λ Ringhomomorphismus),
(iii) λ ist injektiv,
(iv) λ ist surjektiv.
Zu (i): $\overline{h}_1 = \overline{h}_2 \Rightarrow h_2 = h_1 + gu$ mit $u \in R$. Es folgt $h_2(\xi) = h_1(\xi) + g(\xi)u(\xi) = h_1(\xi)$ wegen $g(\xi) = 0$.
(ii) ist eine einfache Nachrechnung.
(iii) Wäre $0 \neq \alpha \in \ker(\lambda)$, so $1 = \lambda(1) = \lambda(\alpha^{-1}\alpha) = \lambda(\alpha^{-1})\lambda(\alpha) = 0$, Widerspruch! Aus $\ker(\lambda) = \{0\}$ folgt bekanntlich die Injektivität.
(iv) Ist $\mathrm{Grd}(g) = n$, so haben M und $\overline{R}$ p^n Elemente, die injektive Abbildung λ muss daher auch surjektiv sein. Ist ξ primitiv, so enthält das Bild alle $X^u(\xi) = \xi^u$ ($u \in \mathbb{N}$), muss also surjektiv sein. Auch in diesem Fall muss daher $\mathrm{Grd}(g) = n$ sein. **q.e.d.**

Fassen wir die in den Hilfssätzen enthaltenen Information zusammen, so sehen wir

Theorem: (Endliche-Körper-Satz)
(i) Ist K ein endlicher Körper, so ist $q = \#K$ eine Primzahlpotenz $q = p^n$, $n \in \mathbb{N}_+$, $p \in \mathbb{P}$. $\mathbb{F}_p$ ist ein Teilkörper von K.
(ii) Zu jeder Primzahlpotenz $q = p^n$ gibt es einen endlichen Körper L mit $\#L = q$.
(iii) Je zwei Körper mit q Elementen sind isomorph.

Beweis: (i) steht in Hilfssatz 1.
(ii) Laut Hilfssatz 2 haben wir einen Körper K, der $\mathbb{F}_p$ enthält, in dem $f = X^q - X$ in Linearfaktoren zerfällt. Hilfssatz 4 sagt uns, dass die Menge der Nullstellen von f in K einen Körper L mit q Elementen bilden.
(iii) Es seien L und M Körper mit $q = p^n$ Elementen. Die Primzerlegung von $X^q - X$ in $R := \mathbb{F}_p[X]$ laute

$$f := X^q - X = \prod_{j=1}^{t} g_j^{n_j},\ n_j \in \mathbb{N}_+$$

mit verschiedenen normierten Primpolynomen g_j und $n_j \in \mathbb{N}_+$ (die n_j müssen übrigens alle $= 1$ sein). Wir betrachten ein primitives Element von M (existiert laut Primitivwurzelsatz). Wegen $0 = f(\xi) = \prod_{j=1}^{t} g_j(\xi)^{n_j}$ existiert ein j mit $g_j(\xi) = 0$. Nach Hilfssatz 5 hat man dann für $g = g_j$ einen Isomorphismus $\lambda : M \to R/gR$ und es ist $Grd(g) = n$.
In $L[X]$ hat f die Primzerlegung

$$f = \prod_{\alpha \in L} (X - \alpha).$$

Die Primzerlegung in $\mathbb{F}_p[X]$ ist auch ein Produkt in $L[X]$. Demnach muss jedes g_j, also auch g ein Produkt gewisser $(X - \alpha)$ sein (EuFa-Satz für $L[X]$). Demach

existiert ein $\alpha \in L$ mit $X - \alpha \,|\, g$, also $g(\alpha) = 0$. Wegen $\mathrm{Grd}(g) = n$ liefert uns Hilfssatz 5 (mit α statt ξ) nun eine Isomorphismus $L \cong R/gR$, und da wir schon wissen $M \cong R/gR$ sind L und M isomorph. **q.e.d.**
Die Isomorphie besagt, dass es bei geeigneter Bezeichnung der Elemente nur einen Körper mit q Elementen gibt, was die Bezeichnung $\mathbb{F}_q$ für ebendiesen rechtfertigt. Übrigens zeigt dieser Beweis noch

1 Folgerung: Zu jedem $p \in \mathbb{P}$ und $n \in \mathbb{N}_+$ gibt es ein irreduzibles Primpolynom g in $\mathbb{F}_p[X]$. Alle solchen Primpolynome sind Teiler von $X^q - X$.

Abschließend wollen wir noch herausfinden, welche Teilkörper $\mathbb{F}_q$ hat.

Satz: (Teilkörpersatz)
Sei $L = \mathbb{F}_q$ ein Körper mit $q = p^n$ Elementen.
(i) Ist K ein Teilkörper von L so gibt es einen Teiler d von n mit $\#K = p^d$
(ii) Zu jedem $d \in \mathbb{N}$ mit $d \,|\, n$ gibt es genau einen Teilkörper K von L mit $\#K = p^d$.

Beweis: (i) Ist K ein Teilkörper von L, so ist L ein K-Vektorraum, wenn man als skalare Multiplikation die in L vorliegende nimmt. Ist d' die Dimension diese Vektorraums L und $\#K = p^d$, so ist $p^n = \#L = \#K^{d'} = p^{dd'}$, woraus $n = dd'$ und $d \,|\, n$ ersichtlich sind.
(ii) ist klar, weil K aus den Nullstellen von $X^{p^d} - X$ in L bestehen muss. **q.e.d.**
Hiernach läuft die Bestimmung aller Teilkörper von L auf die Bestimmung aller Teiler von n hinaus.

Der Satz von Chevalley

Im Folgenden ist stets K ein Körper mit $q = p^n$ Elementen, wo $p \in \mathbb{P}$, $n \in \mathbb{N}_+$ ist. Wir suchen nach möglichst einfachen Bedingungen, die garantieren, dass ein Polynom $f \in K[X_1, \ldots, X_n]$ in n Unbestimmten (Variablen) eine Nullstelle $x = (\xi_1, \ldots, \xi_n) \in K^n$, $x \neq 0$ besitzt.

Wir benutzen dabei folgende Notation

$$f = \sum_{\underline{m} \in \mathbb{N}^n} \alpha_{\underline{m}} X^{\underline{m}},$$

wobei

- $\underline{m} = (m_1, \ldots, m_n)$, $\underline{0} = (0, \ldots, 0)$
- $\alpha_{\underline{m}} \in K$, nur endliche viele $\neq 0$,
- $|\underline{m}| := m_1 + \cdots m_n$

Definition: Man erklärt $\mathrm{Grd}(0) = -\infty$ und für $0 \neq f$ setzt man

$$\mathrm{Grd}(f) := \max\{|\underline{m}| \mid \alpha_{\underline{m}} \neq 0\}.$$

$\mathrm{Grd}(f)$ heißt *Gesamtgrad* von f.
Wie üblich kann man in ein Polynom f statt X_i Elemente $\xi_i \in K$ einsetzen und findet so $f(x) \in K$ für $x = (\xi_1, \ldots, \xi_n)$. Man arbeitet weitgehend so, wie man es aus der Analysis für $\mathbb{R}$ statt K gewöhnt ist. Z.B. gilt: $f(\underline{0}) = \alpha_{\underline{0}}$, speziell $f(\underline{0}) = 0 \Leftrightarrow \alpha_{\underline{0}} = 0$.
Definition: Die Nullstellenmannigfaltigkeit von $f \in K[X_1, \ldots, X_n]$ ist

$$\mathcal{V}_f(K) := \{x \in K^n \mid f(x) = 0\}.$$

Analog für l Polynome $f_1, \ldots, f_l$

$$\mathcal{V}_{f_1,\ldots,f_l}(K) := \{x \in K^n \mid f_1(x) = \ldots f_l(x) = 0\} = \bigcap_{j=1}^{l} \mathcal{V}_{f_j}(K).$$

Man möchte möglichst viel Information über $\mathcal{V}_f(K)$ gewinnen. Hierzu werden in der ALGEBRA und ANALYSIS (Differentialgeometrie) vor allem für $K = \mathbb{C}$ tiefliegende Sätze mit komplizierten und schwierigen Methoden bewiesen (algebraische bzw. analytische Geometrie). In der ELEMENTAREN ZAHLENTHEORIE konzentriert man sich auf endliche K, am meisten ist $K = \mathbb{F}_p$ von Interesse, aber die Beschränkung auf $\mathbb{F}_p$ vereinfacht die Beweise kaum. Die im Folgenden bewiesenen Sätze von Warning und Chevalley sind die bedeutendsten auf diesem Gebiet. Die Beweise beruhen auf einigen Grundideen, die hier isoliert werden sollen:

Idee 1 Das Kroneckersche δ auf K ist als Polynom darstellbar:
Lemma: Für $\alpha \in K$ sei

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

Dann gilt

$$\delta(\alpha) = 1 - \alpha^{q-1} = (1 - X^{q-1})(\alpha).$$

Das ist klar, denn nach dem Elementordnungssatz ist $\alpha^{q-1} = 1$, wenn $\alpha \neq 0$ ist.

Damit ist es leicht, den folgenden interessanten Satz zu beweisen, den wir aber nicht benötigen und der daher als Übungsaufgabe empfohlen wird:

Satz: Alle Funktionen $f : \mathbb{F}_q \to \mathbb{F}_q$ sind durch Polynome darstellbar.

Idee 2 Aus $f \in K[X_1, \ldots, X_n]$ kann man ein Polynom F basteln, das die Nullstellen von f zählen hilft:
Lemma: Für $F = 1 - f^{q-1}$ gilt

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

Damit erhalten wir die Formel

$$\sum_{\underline{x}\in K^n} F(x) = \#\mathcal{V}_f(K)\cdot 1_K \qquad (*)$$

Idee 3 Man will die linke Seite dieser Formel berechnen. Das ist manchmal möglich. Wir beginnen mit $n=1$ und X^k statt F. Um Ausnahmen zu vermeiden, setzen wir noch

$$X^0(0) = 0^0 := 1.$$

Das passt zu der Formel $\sum_{\alpha\in K^1}\gamma X^0(\alpha) = q\gamma = 0$.

Hilfssatz 1 Sei $k\in\mathbb{N}$. Dann gilt

$$\sum_{\alpha\in K^1} X^k(\alpha) = \sum_{\alpha\in K}\alpha^k = \begin{cases} 0 & \text{falls } k=0 \text{ oder } q-1\not| k \\ -1_K & \text{sonst}\end{cases}$$

Beweis: a) $k=0$ ist klar wegen $q\cdot 1_K = 0$.
b) Für $k>0$ ist $0^k=0$ und für $\alpha\neq 0$ ist wegen $\mathrm{ord}(\alpha)\,|\,q-1\,|\,k$ dann $\alpha^k=1$. Demnach ist die Summe $(q-1)1_K = -1_K$.
c) Im Fall $k>0$ und $q-1\not| k$ benutzen wir ein primitives Element ξ von K, also $K^\times = \{1,\xi,\xi^2,\ldots,\xi^{q-1}\}$ (existiert laut Primitivwurzelsatz). Entscheidend ist nun $\xi^k\neq 1$ laut Elementordnungssatz, denn $\mathrm{ord}(\xi) = q-1\not| k$. Damit berechnet man mi Hilfe der geometrischen Reihe

$$\sum_{\alpha\in K}\alpha^k = \sum_{j=1}^{q-2}\xi^{jk} = \sum_{j=1}^{q-2}(\xi^k)^j = \frac{\xi^{k(q-1)}-1}{\xi^k-1} = 0,$$

wegen $\xi^{q-1}=1$ und $\xi^k-1\neq 0$. **q.e.d.**

Hilfssatz 2 Sei $g\in K[X_1,\ldots,X_n]$, $\mathrm{Grd}(g) < n(q-1)$. Dann gilt

$$\sum_{\underline{x}\in K^n} g(x) = 0.$$

Beweis: Es genügt der Beweis für alle $g = X^{\underline{m}}$ mit $|m| < n(q-1)$, denn g ist eine Linearkombination von solchen $X^{\underline{m}}$, und eine Linearkombination von Nullen ist 0. Die Gradbedingung liefert $|m| = m_1+\cdots+m_n < n(q-1)$. Daher gilt für mindestens ein $j\in\{1,\ldots,n\}$ die Ungleichung $m_j < q-1$, also $m_j = 0$ oder $q-1\not| m_j$. Hilfssatz 1 liefert nun für dieses j

$$\sum_{\alpha\in K^1} X_j^{m_j}(\alpha) = \sum_{\alpha\in K}\alpha^{m_j} = 0.$$

Andererseits sieht man durch Ausmultiplizieren des Produkts (für ein festes $\underline{m}$)

$$\prod_{j=1}^{n}\Big(\sum_{\alpha_j\in K}\alpha_j^{m_j}\Big) = \sum_{\underline{x}=(\alpha_1,\ldots,\alpha_n)\in K^n}\alpha_1^{m_1}\cdots\alpha_n^{m_n} = \sum_{\underline{x}\in K^n} X^{\underline{m}}(\underline{x}).$$

(Wer das nicht sieht, kann einen Induktionsbeweis nach n machen). Wie wir sahen, ist aber einer der Faktoren, also das Produkt $= 0$, was wir zeigen wollten. **q.e.d.**
Nun wenden wir Hilfssatz 2 an auf $g = F = 1 - f^{q-1}$. Die Voraussetzung $\mathrm{Grad}(g) < n(q-1)$ ist wegen $\mathrm{Grd}(F) = (q-1)\mathrm{Grd}(f)$ äquivalent mit $\mathrm{Grd}(f) < n$. In diesem Fall haben wir die linke Seite der Formel $(*)$ als 0 berechnet und erhalten somit

$$0 = \#\mathcal{V}_f(K) \cdot 1_K.$$

Da p die Ordnung von 1_K in der additiven Gruppe von K ist, folgt daraus

$$\#\mathcal{V}_f(K) \equiv 0 \bmod p.$$

Damit habne wir bewiesen

Theorem: (Satz von Warning)
Sei $K = \mathbb{F}_{p^n}$ ein endlicher Körper, $f \in K[X_1, \ldots, X_n]$ ein Polynom mit n Unbestimmten und Koeffizienten in K. Falls dann $\mathrm{Grd}(f) < n$ ist, so ist die Anzahl der Nullstellen in K^n von f durch p teilbar.

Selbstverständlich kann diese Anzahl 0 sein. Das trifft aber nicht zu, wenn $f(\underline{0}) = \alpha_{\underline{0}} = 0$ (konstanter Koeffizient) ist: Dann gibt es nach dem Satz von Warning mindestens p Nullstellen. Es folgt der (schon vor Warnings Satz bewiesene)
Satz: (Satz von Chevalley)
Sei $K = \mathbb{F}_{p^n}$ ein endlicher Körper, $f \in K[X_1, \ldots, X_n]$ ein Polynom mit n Unbestimmten und Koeffizienten in K, dessen konstanter Koeffizient 0 ist. Dann hat f eine nichttriviale (d.h. von $\underline{0}$ verschiedene) Nullstelle in K^n.

Dieser sehr allgemeine Satz ist auch für die ELEMENTARE ZAHLENTHEORIE von Bedeutung: Für $K = \mathbb{F}_p$ kann man die Gleichungen als Kongruenzen schreiben. Zum Beispiel heißt ein f mit $f(\underline{0}) = 0$ und $\mathrm{Grd}(f) = 2$ (also $f = \sum \alpha_{ij} X_i X_j$)) *quadratische Form* über K, und eine quadratische Form wird *indefinit* genannt, wenn sie eine nichttriviale Nullstelle besitzt. Der Satz von Chevalley liefert dann sofort:

Satz: Jede quadratische Form über einem endlichen Körper mit 3 oder mehr Variablen ist indefinit.

Eine ähnliche Anwendung sieht so aus:
Satz: Es seinen $\alpha_1, \ldots, \alpha_{n+1} \in \mathbb{Z}$, p eine Primzahl, $d \in \mathbb{N}_+$ mit $d \leq n$. Dann hat die Kongruenz

$$\alpha_1 x_1^d + \cdots \alpha_{n+1} X_{n+1}^d \equiv 0 \bmod p$$

stets eine nichttriviale Lösung $\underline{x} = (x_1, \ldots, x_{n+1}) \in \mathbb{Z}^{n+1}$. Nichtrivial heißt hier: Mindestens ein x_j ist nicht durch p teilbar.
Beweis: Das in Frage stehende Polynom in $\mathbb{F}_p[X_1, \ldots, X_{n+1}]$ hat den Grad d und $n+1$ Variablen. Wegen $d < n+1$ ist die Voraussetzung zum Satz von Chevalley erfüllt. **q.e.d.**

Die Schranke $Grd(f) < n$ in den Sätzen von Warning und Chevalley ist übrigens scharf; schon bei $d = n$ kann man Gegenbeispiele finden. Z.B. hat die Kongruenz $x_1^2 + x_2^2 \equiv 0 \bmod 3$ nur Lösungen mit $3 \,|\, x_1$ und $3 \,|\, x_2$.
Abschließend sollen noch einige Sätze in diesem Zusammenhang mitgeteilt werden. Indem man im Beweis $1 - f^{q-1}$ durch $\prod_{i=1}^{l}(1 - f_i^{q-1})$ ersetzt, erhält man den

Satz: Sei $K = \mathbb{F}_{p^n}$ ein endlicher Körper, $f_1, \ldots, f_l \in K[X_1, \ldots, X_n]$ Polynome mit n Unbestimmten und Koeffizienten in K. Falls dann $d = \sum_{i=1}^{l} \mathrm{Grd}(f_i) < n$ ist, so ist die Anzahl der gemeinsamen Nullstellen der f_i in K^n durch p teilbar.

Die Beweise der zwei folgenden Sätze über Abschätzungen der Nullstellenanzahlen sind kaum schwieriger als der Beweis des Satzes von Warning. Da dies aber keine Vorlesung über endliche Körper ist, wird hier auf Beweise verzichtet.

Satz I Mit den Bezeichnungen und Voraussetzungen des vorigen Satzes gilt, falls $\mathcal{V}_{f_1,\ldots,f_l} \neq \emptyset$ ist, die Abschätzung

$$\#\mathcal{V}_{f_1,\ldots,f_l}(\mathbb{F}_q) \geq q^{n-d}.$$

Auch eine Abschätzung nach oben ist bekannt:

Satz II Sei $f \in K[X_1, \ldots, X_n]$ und $d = \mathrm{Grd}(f)$. Dann gilt

$$\#\mathcal{V}_f(\mathbb{F}_q) \leq d(q^{n-1}).$$

Ganz anders liegen die Dinge beim folgenden Satz, der zu den tiefliegendsten und am schwierigsten zu beweisenden Sätzen der modernen Mathematik zählt:

Satz III Sei $0 \neq f \in \mathbb{Z}[X_1, \ldots, X_n]$ Dann gibt es eine nur von f, nicht $p \in \mathbb{P}$ abhängige Konstante $C = C_f$, so dass gilt

$$|\#\mathcal{V}_f(\mathbb{F}_p) - p^{n-1}| \leq C \cdot \frac{p^{n-1}}{\sqrt{p}}.$$

Nunmehr werden endliche Körper in der Vorles ung nur mehr sporadisch vorkommen.