# 13. Vorlesung - Wiederholung.

## Alons kombinatorischer Nullstellensatz.

Es sei $K$ ein Körper und $P \in K[X_1, \dots, X_n]$ ein Polynom vom Grad $t_1 + \dots + t_n$, in dem das Monom $X_1^{t_1} \cdot \dots \cdot X_n^{t_n}$ vorkommt. Sind $S_1, \dots, S_n \subseteq K$ Mengen mit $|S_i| > t_i$ für alle $i \in [n]$, so gibt's $(s_1, \dots, s_n) \in S_1 \times \dots \times S_n$ mit $P(s_1, \dots, s_n) \neq 0$.

## Satz von Cauchy & Davenport. $A, B \subseteq \mathbb{F}_p \Rightarrow |A+B| \geq \min\{|A|+|B|-1, p\}$.

## Folgerung Zahl = □ + □ + □ + □ (Lagrange)

## Satz. $A \subseteq \mathbb{F}_p$ & $|A| \geq 2 \Rightarrow |A \dot{+} A| \geq \min\{2|A|-3, p\}$,

wobei $A \dot{+} A = \{a + a' : a, a' \in A \ \& \ a \neq a'\}$.

**Dfn 9.7.** Die **Davenport-Konstante** $D(G)$ einer endl. abelschen Gruppe $G$ ist die kleinste Zahl $k$ mit: Für alle $x_1, \dots, x_k \in G$ gibt's $I \subseteq [k]$ mit

$$\sum_{i \in I} x_i = 0, \quad I \neq \emptyset.$$

**Fakt 9.8.** Es gilt stets $D(G) \leq |G|$, d.h. insbesondere existiert $D(G)$.

**Beweis.** Seien $x_1, \dots, x_{|G|} \in G$ beliebig. Setze $s_i = x_1 + \dots + x_i$ für alle $i \in [|G|]$. Wenn $0 \in \{s_1, \dots, s_{|G|}\}$ ist man fertig. Andernfalls gibt's nach Schubfachprinzip $i < j$ mit $s_i = s_j$. Nun tut's $I = [i+1, j]$. □

**Fakt 9.9.** $D(\mathbb{Z}/n\mathbb{Z}) = n$.

**Beweis.** Die Folge $\underbrace{1, \dots, 1}_{n-1}$ zeigt $D(\mathbb{Z}/n\mathbb{Z}) \geq n$. □

**Satz 9.10.** (Olson) $D(\mathbb{F}_p^n) = n(p-1) + 1$.

**Beweis.** Seien $e_1, \dots, e_n$ die Einheitsvektoren. Die Folge

$$\underbrace{e_1, \dots, e_1}_{p-1}, \dots, \underbrace{e_n, \dots, e_n}_{p-1}$$

zeigt $D(\mathbb{F}_p^n) > n(p-1)$.

Nun seien $x_1, \dots, x_{n(p-1)+1} \in \mathbb{F}_p^n$ beliebig. Schreibe $x_j = (a_{j1}, \dots, a_{jn})$ für alle $j \in [n(p-1)+1]$. Betrachte das Polynom

$$P(z_1, \dots, z_{n(p-1)+1}) = \prod_{j=1}^{n(p-1)+1} (1 - z_j) - \prod_{i=1}^{n} \left[ 1 - \left( \sum_{j=1}^{n(p-1)+1} a_{ji} z_j \right)^{p-1} \right].$$

Es hat Grad $n(p-1)+1$ und das Monom $z_1 \cdot \dots \cdot z_{n(p-1)+1}$ kommt vor.

Nach komb. Nullstellensatz gibt's $z_1, \dots, z_{n(p-1)+1} \in \{0, 1\}$ mit

$$P(z_1, \dots, z_{n(p-1)+1}) \neq 0.$$

Setze $I = \{j : z_j = 1\}$. Da $P(0, \dots, 0) = 1 - 1 = 0$ ist $I \neq \emptyset$.

Also $\left( \sum_{j=1}^{n(p-1)+1} a_{ji} z_j \right)^{p-1} \neq 0 \; !$ für alle $i \in [n]$.

Nach kleinem Satz von Fermat ist also

$$\sum_{j \in I} a_{ji} = \sum_{j=1}^{n(p-1)+1} a_{ji} z_j = 0 \qquad \text{für alle } i \in [n].$$

Daher $\sum_{j \in I} x_j = 0$. □

**Satz 9.11 (Erdős, Ginzburg, Ziv)** Für $n \in \mathbb{N}$ besitzt jede Menge $A \subseteq \mathbb{Z}$ mit $|A| = 2n-1$ eine Teilmenge $B \subseteq A$ mit $|B| = n$ und $n \mid \sum_{b \in B} b$.

**Beweis.** Spezialfall: $n = p$ ist Primzahl.

Wir zeigen folgende Version: Für alle $x_1, \dots, x_{2p-1} \in \mathbb{F}_p$ gibt's $I \subseteq [2p-1]$ mit $|I| = p$, $\sum_{i \in I} x_i = 0$. Betrachte $(x_1, 1), \dots, (x_{2p-1}, 1) \in \mathbb{F}_p^2$.

Wegen $D(\mathbb{F}_p^2) = 2(p-1)+1 = 2p-1$ gibt's $I \subseteq [2p-1]$ mit $I \neq \emptyset$ und $\sum_{i \in I} (x_i, 1) = (0,0)$. Nun $\sum_{i \in I} x_i = 0$, $p \mid |I|$.

Beachte, dass wegen $0 < |I| \leq 2p-1$ hieraus $|I| = p$ folgt.

**Produktargument.** Es sei $EGZ(n)$ die Aussage, dass der Satz für $n$ stimmt. Uns genügt nun

$$EGZ(m) \;\&\; EGZ(n) \Rightarrow EGZ(mn).$$

Betrachte $A \subseteq \mathbb{Z}$ mit $|A| = 2mn-1$. Wiederholte Anwendung von $EGZ(m)$ liefert

- $B_1 \subseteq A$ mit $|B_1| = m$, $m \mid \sum B_1$
- $B_2 \subseteq A \setminus B_1$ mit $|B_2| = m$, $m \mid \sum B_2$
- $\vdots$
- $B_{2n-1} \subseteq A \setminus (B_1 \dot\cup \dots \dot\cup B_{2n-2})$ mit $|B_{2n-1}| = m$, $m \mid \sum B_{2n-1}$

Dies klappt, da $|A \setminus (B_1 \dot\cup \dots \dot\cup B_{2n-2})| = 2mn-1-(2n-2)m$

$= 2m-1$.

Setze $b_i = \frac{\sum B_i}{m}$ für alle $i \in [2n-1]$. Nach $\star$ $EGZ(n)$

dürfen wir $n \mid b_1 + \dots + b_n$ annehmen. Setze $B = \dot{\bigcup}_{i \in [n]} B_i$.

Nun $|B| = m \cdot n$ und $\sum B = \sum B_1 + \dots + (\sum B_n)$

$= m(b_1 + \dots + b_n)$

ist durch $mn$ teilbar. □

Bemerkung. Im Satz von EGZ kann man $2n-1$ nicht durch $2n-2$ ersetzen.

Lemma 9.12. Für jeden endl. Körper $F$ der Charakteristik $p$ und alle $i \leq p-2$ gilt $\sum_{x \in F} x^i = 0$.

Beweis. Setze $S_j = \sum_{x \in F} x^j$ für $j \in \mathbb{N}_0$. Es sei $i \leq p-2$ die kleinste Zahl mit $S_i \neq 0$. Da $x \longmapsto x+1$ die Elemente von $F$ permutiert, ist

$$S_{i+1} = \sum_{x \in F} (x+1)^{i+1} = \sum_{x \in F} \sum_{k=0}^{i+1} \binom{i+1}{k} x^k = \sum_{k=0}^{i+1} \binom{i+1}{k} S_k$$

$= s_{i+1} + (i+1)\, s_i$ (nach Minimalität von $i$).

Also $(1+1)\, s_i = 0$. Aber $i+1 \neq 0$ (in $F$!), $s_i \neq 0$. Wid. □

Bem 9.13. Es sei $F$ ein endl. Körper mit $q$ Elementen. Dann gilt

$$x^{q-1} = \begin{cases} 1 & \text{wenn } x \neq 0 \\ 0 & \text{wenn } x = 0 \end{cases}.$$

denn: Die multiplikative Gruppe von $F$ hat Ordnung $q-1$.

Satz 9.14 (Chevalley & Warning) Es seien $F$ ein endl. Körper der Charakteristik $p$ und $P_1, \dots, P_m \in F[X_1, \dots, X_n]$ Polynome mit $\sum_{\mu=1}^{m} \deg(P_\mu) < n$. Dann ist die Anzahl der gem. Nullstellen von $P_1, \dots, P_m$ (in $F^n$) durch $p$ teilbar.

**Beweis.** Setze $q = |F|$ und betrachte das Polynom

$$Q(X_1, \ldots, X_n) = \prod_{\mu=1}^{m} \left[ 1 - P_\mu(X_1, \ldots, X_n)^{q-1} \right].$$

Offenbar

$$Q(x_1, \ldots, x_n) = \begin{cases} 1 & \text{wenn } (x_1, \ldots, x_n) \text{ gem. NS von } P_1, \ldots, P_m. \\ 0 & \text{sonst} \end{cases}$$

Für die Anzahl $\Omega$ der gem. Nullstellen von $P_1, \ldots, P_m$ gilt in $F$ also

$$\Omega = \sum_{(x_1, \ldots, x_n) \in F^n} Q(x_1, \ldots, x_n)$$

Dabei $\deg(Q) \leq (q-1) \sum_{\mu=1}^{m} \deg(P_\mu) < (q-1)n$.

Wenn daher das Monom $X_1^{\alpha_1} \cdot \ldots \cdot X_n^{\alpha_n}$ in $Q$ vorkommt, so gibt's $j \in [n]$ mit $\alpha_j \leq q-2$, weshalb

$$\sum_{(x_1, \ldots, x_n) \in F^n} x_1^{\alpha_1} \cdot \ldots \cdot x_n^{\alpha_n} = \prod_{i=1}^{n} \left( \sum_{x \in F} x^{\alpha_i} \right) = 0.$$

Also $\Omega = 0$ (in $F$), d.h. $p \mid \Omega$. □

Bem. Streng genommen braucht man hier folgende Verstärkung von Lemma 9.12: Es gilt $\sum_{x \in F} x^i = 0$ für alle $i \leq |F|-2$.

Dazu benutzt man, dass die mult. Gruppe von $F$ zyklisch ist.

Schreibt man $F = \{0\} \cup \{1, \xi, \xi^2, \dots, \xi^{|F|-2}\}$, so ist

$$\sum_{x \in F} x^i = \sum_{n=0}^{|F|-2} \xi^{ni} = \frac{1 - \xi^{n(|F|-1)}}{\underbrace{1 - \xi^n}_{\neq 0}} = 0.$$

Beispiel 9.15. Die Anzahl der Tripel $(x,y,z) \in \mathbb{F}_p^3$ mit

$$x^2 + y^2 + z^2 = 0$$

ist durch $p$ teilbar. Also gibt's ein solches Tripel $(x,y,z) \neq (0,0,0)$,

o.B.d.A. $x \neq 0$. Nun $1 + \left(\frac{y}{x}\right)^2 + \left(\frac{z}{x}\right)^2 = 0$.

Wie in Beispiel 9.2 fortfahrend erhält man den 4-Quadrate Satz.

**Satz 9.16.** Für alle Folgen $a_1, \dots, a_{2p-1} \in \mathbb{F}_p$ ist die Anzahl der $I \subseteq [2p-1]$ mit $|I| = p$ mit $\sum_{i \in I} a_i = 0$ kongruent zu 1 modulo $p$.

**Beweis.** Es sei $\Omega$ die Anzahl dieser Mengen $I$. Das Gleichungssystem

$$X_1^{p-1} + \dots + X_{2p-1}^{p-1} = 0 \qquad \dots\dots (1)$$

$$a_1 X_1^{p-1} + \dots + a_{2p-1} X_{2p-1}^{p-1} = 0 \qquad \dots\dots (2)$$

hat $1 + (p-1)^p \Omega$ Lösungen in $\mathbb{F}_p^{2p-1}$, denn:

Betrachte eine solche Lösung $(x_1, \dots, x_{2p-1})$ und setze $I = \{i \in [2p-1] : x_i \neq 0\}$.

Dann sind (1), (2) zu

$$p \mid |I| \qquad \dots\dots (1')$$

$$\sum_{i \in I} a_i = 0 \qquad (2')$$

äquivalent. Es gibt eine Lsg mit $I = \emptyset$ und $(p-1)^p \Omega$ Lsgen mit $|I| = p$.

Aus dem Satz von Chevalley & Warning folgt also

$$p \mid 1 + (p-1)^p \Omega .$$

Da $(p-1)^p \equiv -1 \pmod{p}$ folgt $\Omega \equiv 1 \pmod{p}$. □