§ 9. Algebraisches.

In diesem Kapitel ist p immer eine Primzahl und $\mathbb{F}_p$ der Körper $\mathbb{Z}/p\mathbb{Z}$.

Satz 9.1 (Cauchy - Davenport). Für je zwei additive Mengen $A, B \subseteq \mathbb{F}_p$ gilt

$$|A+B| \geq \min(|A|+|B|-1, p).$$

Beweis. Sei zunächst $|A|+|B| \geq p+1$. Für alle $x \in \mathbb{F}_p$ ist $|A|+|x-B| > p$, also $A \cap (x-B) \neq \emptyset$. Somit gibt's $a \in A$ mit $a \in x-B$, d.h. $x = a+b$ für ein $b \in B$. Dies zeigt $A+B = \mathbb{F}_p$.

Durch Induktion nach $a \in [p]$ zeigen wir: Wenn $|A| = a$ und $|B| \leq p-a$, dann $|A+B| \geq a+|B|-1$.

$a=1$: Klar.

Schritt: Idee: $(A \cap B) + (A \cup B) \overset{\subseteq}{\neq} A+B$, $|A \cap B| + |A \cup B| = |A|+|B|$.

Nun $a \geq 2$. OBdA $0 \in A$ (sonst verschiebe A). Es kann nicht $A+B = B$ sein, da dann $\mathbb{F}_p = pA \subseteq pA+B = B$ wäre.

Es gibt also $b \in B$ mit $A + b \notin B$. Setze $B' = B - b$.
Nun $0 \in A \cap B'$ und $A \notin B'$. Also sind $A \cap B'$, $A \cup B'$ additive Mengen mit $|A \cap B'| < |A|$. Nach Ind. Ann. ist also

$$|(A \cap B') + (A \cup B')| \geq |A \cap B'| + |A \cup B'| - 1$$
$$= |A| + |B| - 1.$$

Folglich $$|A + B| = |A + B'| \geq |A| + |B| - 1.$$ □

Beispiel 9.2. Wenn p ungerade ist, hat

$$Q = \{ x^2 : x \in \mathbb{F}_p \}$$

die Mächtigkeit $\frac{p+1}{2}$, denn:

$$Q = \{ 0, 1^2, 2^2, \dots, \left(\tfrac{p-1}{2}\right)^2 \}$$

und für ganze Zahlen x, y mit $0 \leq x < y \leq \frac{p-1}{2}$ sind $y+x$, $y-x$ nicht durch p teilbar, d.h. $y^2 - x^2 = (y+x)(y-x)$ ist auch nicht durch p teilbar.

Nach Satz 9.1 folgt

$$|Q+Q| \geq \min(2|Q|-1, p) = p,$$

d.h. $Q+Q = \mathbb{F}_p$. Insbesondere $-1 \in Q+Q$, d.h. es gibt $x_p, y_p \in \mathbb{Z}$ mit

$$p \mid 1 + x_p^2 + y_p^2.$$

Dies stimmt auch für $p=2$ (nimm z.B. $x_2 = 1$, $y_2 = 0$).

Betrachte nun eine quadratfreie nat. Zahl n. Es sei $n = p_1 \cdot \ldots \cdot p_r$ die PFZ von n. Nach Chin. Restsatz gibt's $x_n, y_n \in \mathbb{Z}$ mit

$$x_n \equiv x_{p_i}, \quad y_n \equiv y_{p_i} \pmod{p_i} \text{ für alle } i \in [r].$$

Nun

$$n \mid 1 + x_n^2 + y_n^2.$$

Nach Übung gibt's also $a, b, c, d \in \mathbb{Z}$ mit $n = a^2 + b^2 + c^2 + d^2$.

Solche Zahlen gibt's also auch, wenn n nicht quadratfrei ist.

Damit ist der 4-Quadrate Satz von Lagrange bewiesen.

Problem Für $A \subseteq \mathbb{F}_p$ sei

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

Zeige $|A \dot{+} A| \geq \min(2|A| - 3, p)$ für $|A| \geq 2$.

Gleichheit gilt z.B. für $A = \{1, \ldots, n\}$.

. . . . . .

Für einen Körper K ist $K[X_1, \ldots, X_n]$ der Ring aller Polynome in $X_1, \ldots, X_n$ mit Koeff. in K. Jedes $P \in K[X_1, \ldots, X_n]$ ist (evtl. leere) Summe von Monomen $a X_1^{t_1} \cdot \ldots \cdot X_n^{t_n}$, wobei $a \in K$, $t_1, \ldots, t_n \in \mathbb{N}_0$. Für $i \in [n]$ sei $\deg_i(P)$ der Grad von P als Polynom in X_i (mit Koeff. in $K[X_1, \ldots, X_{i-1}, X_{i+1}, \ldots, X_n]$.

Außerdem setzen wir $\deg(a X_1^{t_1} \cdot \ldots \cdot X_n^{t_n}) = t_1 + \ldots + t_n$ (wenn $a \neq 0$) und für $P \in K[X_1, \ldots, X_n]$ sei $\deg(P)$ der höchste Grad eines in P vorkommenden Monoms. $\deg(0) = -\infty$.

Lemma 9.3. Es sei K ein Körper, $P \in K[X_1, \dots, X_n]$ und $S_1, \dots, S_n \subseteq K$ endliche Mengen. Für jedes $i \in [n]$ sei $\deg_i(P) < |S_i|$. Wenn $P(s_1, \dots, s_n) = 0$ für alle $(s_1, \dots, s_n) \in S_1 \times \dots \times S_n$, dann $P = 0$.

Beweis. Induktion nach n.

$n = 1$ klar.

$n-1 \to n$ Schreibe $P = Q_0 + Q_1 X_n + Q_2 X_n^2 + \dots + Q_{|S_n|-1} X_n^{|S_n|-1}$ mit $Q_0, \dots, Q_{|S_n|-1} \in K[X_1, \dots, X_{n-1}]$. Für beliebige $s_1 \in S_1, \dots, s_{n-1} \in S_{n-1}$ setze $q_j = Q_j(s_1, \dots, s_{n-1})$.

Nun ist

$$U = q_0 + q_1 X_n + q_2 X_n^2 + \dots + q_{|S_n|-1} X_n^{|S_n|-1}$$

ein Polynom in $K[X_n]$ mit $U(s_n) = 0$ für alle $s_n \in S_n$.

Also $U = 0$, d.h. $q_0 = \dots = q_{|S_n|-1} = 0$.

Da $s_1, \dots, s_{n-1}$ bel. waren, trifft die Ind. Ann. $Q_0 = \dots = Q_{|S_n|-1} = 0$.

Also $P = 0$. □

Folgerung 9.4. Es sei K ein Körper, $S_1, \dots, S_n \subseteq K$ endlich und $P \in K[X_1, \dots, X_n]$ ein Polynom mit $P(s_1, \dots, s_n) = 0$ für alle $(s_1, \dots, s_n) \in S_1 \times \dots \times S_n$.

Dann gibt's Polynome $Q_1, \dots, Q_n \in K[X_1, \dots, X_n]$ mit

$$P = \sum_{i=1}^{n} \prod_{s \in S_i} (X_i - s)\, Q_i$$

und $\deg(Q_i) \leq \deg(P) - |S_i|$ für alle $i \in [n]$.

Beweis. Wähle $Q_1, \dots, Q_n$ mit $\deg(Q_i) \leq \deg(P) - |S_i|$ so, dass für

$$R = P - \sum_{i=1}^{n} \prod_{s \in S_i} (X_i - s)\, Q_i$$

gilt, dass $\deg_i(R) < |S_i|$ für alle $i \in [n]$. Nach Lemma 9.3 ist $R = 0$. □

Satz 9.5 (Alons komb. 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 $S_1, \dots, S_n \subseteq K$ mit $|S_i| > t_i$ für alle $i \in [n]$, dann gibt's $s_1 \in S_1, \dots, s_n \in S_n$ mit $P(s_1, \dots, s_n) \neq 0$.

Beweis. Andernfalls gäbe es $Q_1, \dots, Q_n \in K[X_1, \dots, X_n]$ mit

$$P = \sum_{i=1}^{n} \prod_{s \in S_i} (X_i - s) \cdot Q_i$$

und $\deg(Q_i) \leq \deg(P) - |S_i|$. Aber $X_1^{t_1} \cdot \dots \cdot X_n^{t_n}$ kommt rechts nicht vor, Wid. □

Zweiter Beweis von Satz 9.1.

Angenommen es gäbe additive Mengen $A, B \subseteq \mathbb{F}_p$ mit $|A|+|B| \leq p$ und $|A+B| < |A|+|B|-1$. Wähle C mit $A+B \subseteq C \subseteq \mathbb{F}_p$ und $|C| = |A|+|B|-2$.

Das Polynom

$$P(X,Y) = \prod_{c \in C} (X+Y-c)$$

hat Grad $|C| = (|A|-1)+(|B|-1)$ und das Monom $x^{|A|-1} y^{|B|-1}$ hat in P den gleichen Koeffizienten wie in $(X+Y)^{|C|}$, d.h.

$$\binom{|A|+|B|-2}{|A|-1} \neq 0 \qquad (\text{in } \mathbb{F}_p !)$$

Nach Komb. Nullstellensatz gibt's $a \in A$, $b \in B$ mit $P(a,b) \neq 0$.

Doch $a+b \in A+B \subseteq C$. Wid.

□

Satz 9.6. Für alle $A \subseteq \mathbb{F}_p$ mit $|A| \geq 2$ gilt

$$|A \dot{+} A| \geq \min(2|A| - 3, p).$$

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

Beweis. Der Fall $p = 2$ ist trivial. Sei nun p ungerade.

Fall 1: $|A| \geq \frac{p+3}{2}$.

Wir zeigen $A \dot{+} A = \mathbb{F}_p$. Sei dazu $x \in A$ bel. Nun

$|A \cap (x - A)| \geq 2|A| - p \geq 3$, es gibt also $a \in A \cap (x - A)$

mit $2a \neq x$. Da $a, x - a \in A$, $a + (x - a) = x$, $a \neq x - a$

ist in der Tat $x \in A \dot{+} A$.

Fall 2: $|A| \leq \frac{p+1}{2}$.

Angenommen es gäbe B mit $A \dot{+} A \subseteq B \subseteq \mathbb{F}_p$, $|B| = 2|A| - 4$.

Das Polynom

$$P(X, Y) = \prod_{b \in B} (X + Y - b)(X - Y)$$

hat Grad $|B|+1 = 2|A|-3$ und das Monom $x^{|A|-1}y^{|A|-2}$ hat den gleichen Koeff. in P wie in $(X+Y)^{2|A|-4}(X-Y)$,

d.h.

$$\binom{2|A|-4}{|A|-2} - \binom{2|A|-4}{|A|-1} = \frac{(2|A|-4)!}{(|A|-2)!(|A|-1)!}\left[(|A|-1)-(|A|-2)\right]$$

$$= \frac{(2|A|-4)!}{(|A|-2)!\,(|A|-1)!} \neq 0 \quad (\text{in } \mathbb{F}_p)$$

Nach Komb. Nullstellensatz gibt's also $a, a' \in A$ mit

$P(a,a') \neq 0$. Nun $a \neq a'$ und $a+a' \notin B$, Wid. □