Theorem. *Given $0 < \delta < 1$, there is $\delta' > \delta$ such that if $S \subset \mathbb{F}_p$ (p-prime) satisfies $|A| = p^\delta$, then*

$$|S + S| + |S.S| > p^{\delta'}$$

(we assume p large).

We basically follow the Edgar-Miller approach, see [E-M].

(1). Lemma. *Let $A \subset \mathbb{F}_p$, $|A| \geq p^\delta$ (p large prime, $\delta > 0$ fixed). Then there are $\xi_1, \ldots, \xi_k \in \mathbb{F}_p^*, k \leq k(\delta) \sim \frac{1}{\delta}$, such that*

$$\mathbb{F}_p = A\xi_1 + \cdots + A\xi_k \tag{1.1}$$

Proof. Using the Cauchy-Davenport inequality in $\mathbb{F}_p$

$$|\mathcal{A} + \mathcal{B}| \geq \min(|\mathcal{A}| + |\mathcal{B}| - 1, p),$$

it clearly suffices to obtain $\xi_1, \ldots, \xi_k$ s.t.

$$|A\xi_1 + \cdots + A\xi_k| \geq \frac{p}{100}. \tag{1.2}$$

This may be achieved exploiting the fact that given $\mathcal{A}, \mathcal{B} \subset \mathbb{F}_p$ with $|\mathcal{A}|.|\mathcal{B}| < \frac{p}{10}$ there is $\xi \in \mathbb{F}_p$ for which

$$|\mathcal{A} + \mathcal{B}\xi| > \frac{1}{2}|\mathcal{A}|.|\mathcal{B}|. \tag{1.3}$$

Use randomization in ξ according to the normalized counting measure $d\xi$ on $\mathbb{F}_p^*$. Thus

$$|\mathcal{A} + \mathcal{B}\xi| = |\bigcup_{a \in \mathcal{A}} (a + \mathcal{B}\xi)| \geq \sum_{a \in \mathcal{A}} |a + \mathcal{B}\xi| - \sum_{\substack{a, a' \in \mathcal{A} \\ a \neq a'}} |(a + \mathcal{B}\xi) \cap (a' + \mathcal{B}\xi)|$$

and

$$\int_{\mathbb{F}_p^*} |\mathcal{A} + \mathcal{B}\xi| d\xi \geq |\mathcal{A}|.|\mathcal{B}| - \sum_{\substack{a, a' \in \mathcal{A} \\ a \neq a'}} \int |(a + \mathcal{B}\xi) \cap (a' + \mathcal{B}\xi)| d\xi$$

$$\geq |\mathcal{A}|.|\mathcal{B}| - |\mathcal{A}|^2 \frac{|\mathcal{B}|^2}{p - 1} > \frac{1}{2}|\mathcal{A}|\ |\mathcal{B}| \tag{1.4}$$

complying (1.3).

This proves the Lemma.

(2). Denote $R = \mathbb{F}_p$ and let $\xi_1, \ldots, \xi_k$ be as in the Lemma. Thus $A^k \to R : (a_1, \ldots, a_k) \mapsto \sum_{j \leq k} a_j \xi_j$ is onto. Assume $k > 1$. Our map cannot be one-to-one, since otherwise

$$|A|^k = p \Rightarrow p^{1/k} \in \mathbb{Z} \text{ (contradicting primarily of } p).$$

Thus there are $(b_1, \dots, b_k) \neq (b'_1, \dots b'_k) \in A^k$ with

$$(b_1 - b'_1)\xi_1 + \cdots + (b_k - b'_k)\xi_k = 0. \tag{2.1}$$

Let $b_k \neq b'_k$. By (1.1) and since R is a field, also

$$R = A\xi_1(b_k - b'_k) + \cdots + A\xi_k(b_k - b'_k)$$

and substituting $(b_k - b'_k)\xi_k$ from (2.1)

$$\begin{aligned} R &= A\xi_1(b_k - b'_k) + \cdots + A\xi_{k-1}(b_k - b'_k) - A(b_1 - b'_1)\xi_1 - \cdots - A(b_{k-1} - b'_{k-1})\xi_{k-1} \\ &\subset A_1\xi_1 + \cdots + A_1\xi_{k-1} \end{aligned} \tag{2.2}$$

where

$$A_1 = A(A - A) + A(A - A) \supset A(b_k - b'_k) - \bigcup_{1 \leq j < k} A(b_j - b'_j). \tag{2.3}$$

Thus we reduced k to $k - 1$, subject to replacement of A by A_1.

After $k - 1$ steps, we get clearly

$$R = A_{k-1} \cdot \xi \ (\xi \in \{\xi_1, \dots, \xi_k\} \subset \mathbb{F}_p^*)$$

hence

$$R = A_{k-1}$$

where

$$A_{k-1} = \ell_k A^{2^{k-1}} - \ell_k A^{2^{k-1}} \tag{2.4}$$

($\ell_k \in \mathbb{Z}_+$ depending on k) and denoting

$$\ell A = \underbrace{A + \cdots + A}_{\ell}$$

$$A^m = \underbrace{A \cdots A}_{m}.$$