① (i) Let $G = \mathbb{Z}$, $A = \{1, 2, 2^2, \dots, 2^{N-2}\}$

(ii) Note that $A+A = \underbrace{\{2a : a \in A\}}_{A_1} \cup \underbrace{\{a_1 + a_2 : a_1 \neq a_2, a_1, a_2 \in A\}}_{A_2}$.

Note that $|A_1| = |A|$, $|A_2| \leq \frac{|A|(|A|-1)}{2}$

We have that $|A+A| \leq |A_1| + |A_2| \leq \frac{|A|(|A|+1)}{2}$.

We have equality iff $A_1 \cap A_2 = \phi$, $|A_2| = \frac{|A|(|A|-1)}{2}$,

is iff A is Sidon set.

(iii) $\{(a, b, c, d) \in A^4 : a+b = c+d\} =: S$

$\cup|$

$\left(\underbrace{\{(a,a,a,a) : a \in A\}}_{A_1} \cup \overbrace{\{(a,b,a,b) : a, b \in A, a \neq b\}}^{A_2} \cup \underbrace{\{(a,b,b,a) : a, b \in A, a \neq b\}}_{A_3}. \right)$

Note that $|A_1| = |A|$, $|A_2| = |A_3| = |A|^2 - |A|$.

Since $A_1 \cap A_2 = A_2 \cap A_3 = A_3 \cap A_1 = \phi$,

Clearly $|S| \geq 2|A|^2 - |A|$.

$E(A, B)$.

We have equality iff A is Sidon set.

(iv) Let $A' \subset A$ a Sidon set.

Then $A'+A' \subset A+A$.

But $|A'+A'| = \frac{|A'|(|A'|+1)}{2} \leq \sigma(A)|A|$.

So $|A'|^2 < 2\sigma(A)|A|$.

② (i) Suppose $(t_1+t_2, t_1^2+t_2^2) = (t_3+t_4, t_3^2+t_4^2) = (u,v)$

So $t_1 t_2 = t_3 t_4 = \frac{u^2-v}{2}$. (assume $p>2$).

But now $\{t_1, t_1, t_3, t_4\}$ are solutions to

$$X^2 - uX + \frac{u^2-v}{2} \in \mathbb{F}_p[X].$$

This has at most 2 solutions in $\mathbb{F}_p$.

(ii) Consider the embedding

$$\phi : (\mathbb{Z}/p\mathbb{Z})^2 \longrightarrow \mathbb{Z}$$
$$(a,b) \longmapsto a+pb.$$

(consider unique representation with $a, b \in \left[-\frac{p}{2}, \frac{p}{2}\right]$).

Note that $\phi(\underline{x}+\underline{y}) = \phi(\underline{z}+\underline{w}) \Rightarrow \underline{x}+\underline{y} = \underline{z}+\underline{w}$.

This implies that if $A \subset (\mathbb{Z}/p\mathbb{Z})^2$ is a Sidon set, then $\phi(A) \subset \left[-\frac{p^2}{2}, \frac{p^2}{2}\right]$ is a Sidon set.

Using (i) and translating the set $\phi(A)$, this shows that any interval of length p^2 in $\mathbb{Z}$ contains a Sidon set of size p.

Conclusion follows from the fact that if N large enough, there exists a prime p with $\frac{\sqrt{N}}{2} \le p \le \sqrt{N}$.

(iii) We construct such a set using greedy algorithm (inductively).

Suppose we have a Sidon set $A_n = \{a_1, \dots, a_n\}$.
We choose a_{n+1} such that $A_{n+1} = A_n \cup \{a_{n+1}\}$ is also Sidon.

Choose $a_{n+1} = \min(\mathbb{Z} \setminus (A+A-A))$.

Then $a_{n+1} + k = l + m$ has no solution $(k, l, m) \in A^3$, hence A_{n+1} is Sidon set.

But also have that $a_{n+1} \le n^3$
$$\left(\text{since } |A+A-A| \le n^2 + \frac{n(n-1)}{2} \cdot n = \frac{n^3}{2} + \frac{n^2}{2}\right)$$

Conclusion follows by taking $A = \bigcup_{n \in \mathbb{N}} A_n$.

③ (i) Take $A = \{1, 2, \dots, N\}$, $B = \{N^2+N, N^2+2N, \dots, N^2+N\cdot N\}$

Then $\sigma(A), \sigma(B) \le 2$.

But $A+B = \{N^2 + aN + b : a, b \in [N]\}$,

So $|A+B| = N^2$.

But $A+B \subset (A\cup B) + (A\cup B)$.

So $\dfrac{|2(A\cup B)|}{|A\cup B|} \ge \dfrac{N^2}{2N} = \dfrac{N}{2}$.

(ii) From 2(iii), we can find a Sidon set S of size $\ge \dfrac{\sqrt{N}}{4}$ inside $\{1, 2, \dots, \frac{N}{2}\}$.

Let $A = S \cup \underbrace{\{N/2, \dots, N\}}_{A'}$.

$B = S \cup \underbrace{\{N, \dots, 3N/2\}}_{B'}$.

So $|A|, |B| \ge \dfrac{N}{2} + \dfrac{\sqrt{N}}{4}$.

Then $|2A| \le |2A'| + |2S| + |A'+S| \le 3N$.

Observe $A \cap B = S$, and $|2(A\cap B)| \ge \dfrac{N}{16}$.

Conclusion follows.

④ (i) Suppose $A \sim B$ and $B \sim C$.

Then $d(A, C) \le d(A, B) + d(B, C) = O(\log K)$

$\Rightarrow A \sim C$

(iii) If $A \sim B$, then $e(A, -B) \approx 1$.

By Sh 4, ex 1, this implies $|A| \simeq |B|$.

Since $d(A, A) \leq d(A, B) + d(B, A) = O(\lg K)$

By Sh 4, ex 4, this implies

$$|A+A| \approx |A-A| \approx |A|.$$

Finally, $d(A, -B) \leq d(A, B) + d(B, -B) = O(\lg K)$

$\Rightarrow A \sim -B$.

(iv) Suppose $A \sim B$, $\sigma(C) \approx 1$ and

$\exists x \in G$ s.t $|A \cap (x + C)| \approx |A| \approx |C|$.

Note that by replacing C with $x + C$,

we may assume that $x = 0$.

Hence $|A \cap C| \approx |A| \approx |C|$

Ruzsa triangle inequality $d(A, A\cap C) + d(A \cap C, C) \geq d(A, C)$

is equivalent to

$$|A - (A\cap C)|\,|(A \cap C) - C| \geq |A \cap C|\,|A - C|.$$

$$\begin{array}{cc} \shortparallel & \shortparallel \\ |A-A| & |C-C| \end{array}$$

But since $\sigma(A) \simeq \sigma(C) \approx 1$ and $|A| \approx |C|$,

we have that $|A \cap C|\,|A - C| \ll |A|^2$

But $|A \cap C| \simeq |A| \approx C$

$\Rightarrow |A - C| \ll |A| \Rightarrow A \sim C$.

(ii) Note that

$$d(2B,-2C) \le d(2B,B) + d(B,C) + d(C,-2C)$$

By Plünnecke, $|2B-B| \approx |B|$
$|2C-C| \approx |C|$

Since $B \sim C$, $|B-C| \approx |B| \approx |C|$.

Therefore $d(2B,-2C) = O(\lg K)$

Since we know $|B+C| \approx |B| \approx |C|$,

this implies $\sigma(B+C) \approx 1$.

We apply (iv). $A \sim B$, $\sigma(B+C) \approx 1$ and

for $x \in -B$, $|B \cap (x+B+C)| \approx |B| \approx |B+C|$.

Hence $A \sim B \sim B+C$.

(v) Replacing B with $B+x$, can assume $x=0$.

Then $|A \cap B| \approx |A| \approx |B|$.

By Ruzsa inequality, $\underbrace{|A-(A\cap B)|}_{\le |A-A|}\,\underbrace{|(A\cap B)-B|}_{\le |B-B|} \ge |A\cap B||A-B|$

So $|A\cap B||A-B| \le |A-A||B-B|$.

$\sigma(A), \sigma(B) \approx 1$ and $|A| \approx |B| \Rightarrow |A-A| \approx |B-B| \approx |A|$

$\rightarrow |A-B| \approx |A| \Rightarrow A \sim B.$

5 (i) Let $a \neq b$, $a, b \in A$.

$$0 = \frac{a-a}{a-b} \in Q[A]$$

$$1 = \frac{a-b}{a-b} \in Q[A]$$

If $k = \frac{a-b}{c-d} \in Q[A] \Rightarrow -k = \frac{b-a}{c-d} \in Q[A]$

$$\Rightarrow Q[A] = -Q[A].$$

If $K = \frac{a-b}{c-d} \in Q[A]^\times \Rightarrow K^{-1} = \frac{c-d}{a-b} \in Q[A]^\times$

$$\Rightarrow Q[A]^\times = (Q[A]^\times)^{-1}$$

(ii) Easy check since for $x \in \mathbb{F}_p$, $\lambda \in \mathbb{F}_p^\times$,

$$\frac{(x+a)-(x+b)}{(x+c)-(x+d)} = \frac{\lambda a - \lambda b}{\lambda c - \lambda d} = \frac{a-b}{c-d}.$$

(iii) "$\Rightarrow$" Suppose $|A + x.A| = |A|^2$. Then $x \neq 0$.
(because $|A+0.A| = |A| \neq |A|^2$).

Then if $(a,b), (c,d) \in A^2$ with $(a,b) \neq (c,d)$

$$a + x.b \neq c + x.d$$

$$\Rightarrow a - c \neq x(d-b).$$

If $b-d=0 \rightarrow a-c=0$ (since $x \neq 0$).

But $(a,b) \neq (c,d)$, so not possible.

Therefore $x \notin Q[A]$.

"$\Leftarrow$" If $x \notin Q[A]$, then $x \neq 0$.

If $|A + x \cdot A| \neq |A|^2 \Rightarrow \exists\, (a,b) \neq (c,d) \in A^2$

s.t. $a + xb = c + xd$

$\Rightarrow x = \dfrac{a-c}{d-b}$, false.

(iv) Suppose $\exists\, x \in \mathbb{F}_p \setminus Q[A]$.

$\Rightarrow |A + x \cdot A| = |A|^2$.

But $A + x \cdot A \subset \mathbb{F}_p \Rightarrow |A|^2 < p$.

6 (i) Since $b \neq 0$,

$|A + bA| = |b^{-1}(A + bA)| = |b^{-1}A + A| \leq K|A|$

$\Rightarrow b^{-1} \in Alg_K(A)$

(ii) $b \in Alg_K(A) \Rightarrow A \sim -bA$

But this implies $A \sim bA$ (exercise 4)

$\Rightarrow -b \in Alg_{K^c}(A)$.

(iii) $A \sim bA,\ A \sim b'A \Rightarrow A \sim bA + b'A$. (ex 4, ii)

$\Rightarrow A \sim A + bA + b'A$

$\Rightarrow |A| \approx |A + bA + b'A|$

But $A + (b+b')A \subset A + bA + b'A$

$\Rightarrow |A + (b+b')A| \approx |A|$.

(iv) $d(A,(bb')A) \leq d(A,bA) + d(bA, bb'A)$

$d(A, b'A)$

$= O(\lg K)$

$\Rightarrow -bb' \in Alg_{K^c}(A)$

$\Rightarrow bb' \in Alg_{K^c}(A)$.