① (i) Since $B_G = \{ d_\pi^{1/2} \Phi_{v_i, v_j, \pi} : \pi \in \mathrm{Irr}(G),\ v_i, v_j \in B_\pi \}$ is an ONB for $\mathcal{F}(G, \mathbb{C})$, we have that

$$\forall f \in \mathcal{F}(G, \mathbb{C}), \quad f = \sum_{\pi \in \mathrm{Irr}(G)} \sum_{1 \le i,j \le d_\pi} d_\pi \langle f, \Phi_{\pi, v_i, v_j} \rangle \Phi_{\pi, v_i, v_j} \quad (*)$$

and
$$\sum_{g \in G} |f(g)|^2 = |G| \langle f, f \rangle$$

$$= |G| \sum_{\pi \in \mathrm{Irr}(G)} d_\pi \sum_{i,j \le d_\pi} |\langle f, \Phi_{\pi, v_i, v_j} \rangle|^2$$
(by expanding $\langle f, f \rangle$)

$$= |G| \sum_{\pi} d_\pi \sum_{i,j \le d_\pi} \left| \frac{1}{|G|} \sum_{g \in G} f(g) \Phi_{\pi, v_i, v_j}(g) \right|^2$$
(by def of inner product $\langle f, \Phi_{\pi, v_i, v_j} \rangle$)

$$= \frac{1}{|G|} \sum_{\pi} d_\pi \sum_{i,j \le d_\pi} \left| \sum_{g \in G} f(g) \langle \pi(g) v_i, v_j \rangle \right|^2$$
(by def of matrix coeff Φ_{π, v_i, v_j})

$$= \frac{1}{|G|} \sum_{\pi} d_\pi \sum_{i,j \le d_\pi} | \langle \pi(f) v_i, v_j \rangle |^2$$
(by def of $\pi(f)$)

$$= \frac{1}{|G|} \sum_{\pi} d_\pi \sum_{i \le d_\pi} \| \pi(f) v_i \|^2$$
(since $\{v_1, \dots, v_{d_\pi}\}$ ONB for V_π)

$$= \frac{1}{|G|} \sum_{\pi} d_\pi \|\pi(f)\|_{HS}^2$$

(by def of HS norm).

(ii) From (*): $f(g) = \sum_{\pi} \sum_{i,j \le d_\pi} d_\pi \langle f, \Phi_{v_i, v_j, \pi} \rangle \langle \pi(g) v_i, v_j \rangle$

$$= \sum_{\pi} \sum_{i,j \le d_\pi} d_\pi \langle \pi(g) v_i, v_j \rangle \sum_{g' \in G} \frac{1}{|G|} f(g') \langle \pi(g') v_i, v_j \rangle$$

$$= \frac{1}{|G|} \sum_{\pi} d_\pi \sum_{i,j} \langle \pi(g) v_i, v_j \rangle \langle \pi(f) v_i, v_j \rangle$$

$$= \frac{1}{|G|} \sum_{\pi} d_\pi \langle \pi(f), \pi(g) \rangle_{HS}.$$

(iii) Note that

$$\pi(f_1 * f_2)(v) = \sum_{g \in G} (f_1 * f_2)(g) \pi(g) v$$

$$= \sum_{g \in G} \Big(\sum_{g_1 g_2 = g} f_1(g_1) f_2(g_2) \Big) \pi(g_1 g_2) v$$

$$= \sum_{g_1, g_2 \in G} f_1(g_1) f_2(g_2) \pi(g_1 g_2)(v)$$

$$= \sum_{g_1, g_2} f_1(g_1) f_2(g_2) \pi(g_1)(\pi(g_2)(v))$$

$$= \sum_{g_1 \in G} f_1(g_1)\pi(g_1)\left(\sum_{g_2 \in G} f_2(g_2)\pi(g_2(v))\right)$$

$$= \pi(f_2)\circ\pi(f_2)(v).$$

Then $\|\pi(f_1 * f_2)\|_{HS} = \|\pi(f_2)\circ\pi(f_2)\|$

$$\le \|\pi(f_1)\|_{HS}\,\|\pi(f_2)\|_{HS},$$

where the inequality follows from standard linear algebra (norm of composition of operators acting on Hilbert spaces).

---

(2) a) Let $x = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{F}_p) \setminus B$.

Hence $c \neq 0$.

Suppose $uxvx^{-1}w = u'xv'x^{-1}w'$,

for some $, v, w, u', v', w' \in N^*$.

$\Rightarrow (u'^{-1}u)\,xvx^{-1}\,(ww'^{-1}) = xv'x^{-1}$.

Note that $x\begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}x^{-1} = \begin{pmatrix} ad - cat - c & -ab + a^2t + a \\ -ct^2 & -bc + act + a \end{pmatrix}$

Write $u'^{-1}u = \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}$, $ww'^{-1} = \begin{pmatrix} 1 & \beta \\ 0 & 1 \end{pmatrix}$,

$$v = \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}, \quad v' = \begin{pmatrix} 1 & t' \\ 0 & 1 \end{pmatrix}$$

Then we have
$$\begin{pmatrix} ad - cat - c - \alpha ct^2 & * \\ -ct^2 & -bc + act + a - \beta ct^2 \end{pmatrix}$$
$$\parallel$$
$$\begin{pmatrix} ad - cat' - c & * \\ -ct'^2 & -bc + act' + a \end{pmatrix}$$

Hence
$$(t')^2 = t^2$$
$$cat + \alpha ct^2 = cat'$$
$$cat - \beta ct^2 = cat'$$

It follows $t = t'$, $\alpha = \beta = 0$.

ii) Suppose $A \not\subset B$, so there exists $x \in A \setminus B$.

Consider the map
$$(N^* \cap A)^3 \longrightarrow SL_2(\mathbb{F}_p)$$
$$(u, v, w) \longmapsto u x v x^{-1} w.$$

This map is injective, and the image is contained in $A^{(5)}$. (since $x^{-1} \in A$ from symmetry of A).

Hence $|N^* \cap A|^3 \leq |A^{(5)}|$.

(iii) Note that the map
$$N^* \times N^* \longrightarrow SL_2(\mathbb{F}_p)$$
(for $x \in SL_2(\mathbb{F}_p) \setminus B$)
$$(u, v) \longmapsto u x v x^{-1}$$

is injective (similar to part (i)).

But if $A = N \cup \{x, x^{-2}\}$, image is contained in $A^{(3)} x^{-2}$

$|A| = p+2$.

This shows $(p-1)^2 = (|A|-3)^2 \leq |A^{(3)}|$.

So $|A^{(3)}| \geq C\,|A|^2$, for some suitable C.

3 (i) Follows easily since $x^2 \in K$ and K is a subgroup.

(ii) Let $H = x^{-1} K x \cap K$, which is a subgroup of K. From basic group theory,
$$|KxK| = [K:H]\,|K| = C\,X.$$

(since KxK is the disjoint union of Kxy, where y runs over cosets of H in K).

Conclusion follows.

(iii) Note that $x^2 = -I$, and since $p \equiv 1\,(4)$, then -1 is a square modulo p.

First note $|K| = \frac{p(p-1)}{2}$.

Note that $\begin{pmatrix} -1 & -2 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}\begin{pmatrix} 1 & 2 \\ -1 & -1 \end{pmatrix} = \begin{pmatrix} -a+b+2d & -2a+b+2d \\ a-b-d & 2a-b-d \end{pmatrix}$

If this belongs to K, then $a-b-d=0$.

In this case, $\begin{pmatrix} -1 & -2 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}\begin{pmatrix} 1 & 2 \\ -1 & -1 \end{pmatrix} = \begin{pmatrix} d & -a+d \\ 0 & a \end{pmatrix}$

If a is square mod p, and $ad=1$, then also d is square mod p.

Hence $|K \cap x^{-1}Kx| = p-1$.

(iii) From previous two points,

$$|A^{(3)}| \leq (2+p)\frac{p(p-1)}{2} < \frac{p(p^2-1)}{2} = |SL_2(\mathbb{F}_p)|$$

Also $|A| = \frac{p(p-1)}{2} + 2$, so $|A^{(3)}| \leq C'|A|^{3/2}$.

(4) We prove Theorem 6.1 assuming Theorems 6.2 & 6.3.

Let A a generating for $SL_2(\mathbb{F}_p)$ such that $|A^{(3)}| \leq |A|^{1+\delta}$ (for some δ sufficiently small).

Assume WLOG $A = A \cup A^{-1} \cup \{e\}$ (consider $B = A \cup A^{-1} \cup \{e\}$ otherwise).

(Note that $|A^{(3)}| \le |A|^{1+\delta}$ can be rewritten as

$$d(A^{(2)}, A^{-1}) = \log\left(\frac{|A^{(3)}|}{\sqrt{|A^{(2)}||A|}}\right) \le \delta \log A.$$

Using Ruzsa Δ-ineq, one can show for example

$$d(A^{(2)}, A) \le d(A^{(2)}, A^{-1}) + d(A^{-1}, A) \le 2\delta \log A,$$

which implies $|A^{(2)} \cdot A^{-1}| \le |A|^{2\delta}$.

We have $B^{(3)} = \bigcup_{\varepsilon_i \in \{0, \pm 1\}} A^{\varepsilon_1} A^{\varepsilon_2} A^{\varepsilon_3}$, where $A^0 := \{e\}$.

Can bound each of them, also using

$$|A| \le |A^{(2)}| \le |A^{(3)}| \le |A|^{1+\delta} \quad \ldots$$

So one has $|B| \le 8|A|^{1+2\delta} \le 8|B|^{1+2\delta}$,

WLOG assumption is OK).

Since $|A^{(3)}| \le A^{1+\delta}$, using Theorem 3.5 from notes, it follows that $A^{(3)}$ is a K-approx subgroup, with $K \le 2|A|^{5\delta}$.

But now, from 6.2, we know that either

$|A^{(3)}| \le (2|A|^{5\delta})^C$

or $|A^{(3)}| \ge |SL_2(\mathbb{F}_p)| / (2|A|^{5\delta})^C$, for some absolute C.

In the first case, since $|A| \le |A^{(3)}| \le 2^c |A|^{50c}$,

this can only hold for $|A|$ of some finite size, and then can choose δ accordingly.

In the second case, by Theorem 6.3, it follows that $A^{(9)} = SL_2(\mathbb{F}_p)$. $\square$.

5 Proof is very similar to 6.9. Consider instead $N_A = N \cap A$ and the map

$$N_A \times N_A \times N_A \longrightarrow A$$
$$(u, v, w) \longmapsto u x v x^{-1} w,$$

for some $g \in A \setminus B$.

As in Exercise 2, this map will be (almost) injective.