Exercise sheet 4

1. Let G be a group and H a subgroup of G. Let $x \in G$, and define $I = H \cap x^{-1}Hx$; this is a subgroup of H.

   (a) For h_1 and $h_2 \in H$, show that

   $$Hxh_1 \cap Hxh_2 = \varnothing$$

   unless $h_1h_2^{-1} \in I$.

   (b) If $h_1h_2^{-1} \in I$, then show that

   $$Hxh_1 = Hxh_2.$$

   (c) Deduce that the product set HxH (known as a *double coset* of H) is the disjoint union of Hxy for y running over a set of representatives of the cosets hI of I in H. In particular, if H is finite, deduce that

   $$|HxH| = [H : I]\ |H|.$$

Solution.

(a) Suppose there exists $h, \tilde{h}$ such that

$$hxh_1 = \tilde{h}xh_2 \Leftrightarrow h_1{h_2}^{-1} = x^{-1}h^{-1}\tilde{h}x,$$

therefore $h_1h_2^{-1} \in I$.
On the hand, if $h_1h_2^{-1} = x^{-1}hx \Rightarrow exh_1 = hxh_2$.

(b) Let $hxh_1 \in Hxh_1$ and write $h_1h_2^{-1} = x^{-1}\tilde{h}x$. Then

$$hxh_1 = hxx^{-1}\tilde{h}xh_2 = h\tilde{h}xh_2.$$

The other direction follows similarly.

(c) From the previous item we have

$$HxH = \bigcup_{\substack{h_i \in H \\ h_ih_j^{-1} \notin I}} Hxh_i,$$

a diskoint union. Therefore, $|HxH| = |H||H : I|$.

2. Let p be a prime number and let

$$U = \left\{ \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix} \mid t \in \mathbf{F}_p \right\}, \qquad B = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \mid a, b, d \in \mathbf{F}_p,\ ad = 1 \right\}.$$

Set $U^* = U \setminus \{1\}$.

(a) Show that U and B are subgroups of $\mathrm{SL}_2(\mathbf{F}_p)$ with $|U| = p$ and $|B| = p(p-1)$.

(b) Let $x \in \mathrm{SL}_2(\mathbf{F}_p) \setminus B$. Show that the map

$$\begin{cases} U^* \times U^* \times U^* & \to \quad \mathrm{SL}_2(\mathbf{F}_p) \\ (u, v, w) & \mapsto \quad uxvx^{-1}w \end{cases}$$

is injective.

(c) Let A be a symmetric subset of $\mathrm{SL}_2(\mathbf{F}_p)$. Show that either $A \subset B$ or

$$|U^* \cap A|^3 \leqslant |A^{(5)}|.$$

(This is a very special case of what are called *Larsen–Pink non-concentration inequalities.*)

(d) Let $x \in \mathrm{SL}_2(\mathbf{F}_p) \setminus B$. Let $A = U \cup \{x, x^{-1}\}$. Show that there exists $c > 0$ and $\delta > 0$, independent of p and x, such that

$$|A^{(3)}| \geqslant c|A|^{1+\delta}.$$

How large can you get δ to be?

Solution.

(a) Let $T_t = \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}$ and observe that

$$\begin{aligned} T_0 &= I \\ T_{t_1} \cdot T_{t+2} &= T_{t_1+t_2} \\ (T_t)^{-1} &= T_{-t}, \end{aligned}$$

so U is a subgroup and $|U| = |\mathbf{F}_p| = p$

To show that B is a subgroup, observe that taking $b = 0, a = 1, d = 1$ we have the identity, and

$$\begin{pmatrix} a_1 & b_1 \\ 0 & d_1 \end{pmatrix} \cdot \begin{pmatrix} a_2 & b_2 \\ 0 & d_2 \end{pmatrix} = \begin{pmatrix} a_1a_2 & a_1b_2 + b_1d_2 \\ 0 & d_1d_2 \end{pmatrix} \in B,$$

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}^{-1} = \begin{pmatrix} d & -b \\ 0 & a \end{pmatrix} \in B,$$

so B is a subgroup. Since $a \neq 0$ it holds that $|B| = p(p-1)$.

(b) Since $x \in \mathrm{SL}_2(\mathbf{F}_p) \smallsetminus B$ it holds that

$$x = \begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

where $c \neq 0$. We observe that

$$\begin{aligned} uxvx^{-1}w = \tilde{u}x\tilde{v}x^{-1}\tilde{w} \Leftrightarrow \\ (\tilde{u}^{-1}u)xvx^{-1}(w\tilde{w}^{-1}) = x\tilde{v}x^{-1}. \end{aligned}$$

Using that

$$x \begin{pmatrix} 1 & v \\ 0 & 1 \end{pmatrix} x^{-1} = \begin{pmatrix} ad - cav - c & -ab + a^2v + a \\ -cv^2 & -bc + acv + a \end{pmatrix}$$

and

$$\begin{aligned} \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix} &= \begin{pmatrix} a_1 & a_1t + b_1 \\ c_1 & c_1t + d_1 \end{pmatrix} \\ \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} &= \begin{pmatrix} a_1 + tc_1 & b_1 + td_1 \\ c_1 & d_1, \end{pmatrix} \end{aligned}$$

and the fact that $c \neq 0$, we conclude that the map must be injective by comparing all the entries after multiplying the matrices.

(c) If A is not contained in B, let $x \in A \backslash B$. Since A is symmetric, $x^{-1} \in A$ and we conclude that $A^{(5)}$ is in the image of the map

$$\begin{cases} U^* \cap A\backslash\{x, x^{-1}\} \times U^* \cap A\backslash\{x, x^{-1}\} \times U^* \cap A\backslash\{x, x^{-1}\} & \to \quad \mathrm{SL}_2(\mathbf{F}_p) \\ (u, v, w) & \mapsto \quad uxvx^{-1}w. \end{cases}$$

Since the map is injective, it holds that

$$|U^* \cap A|^3 \leqslant |A^{(5)}|.$$

(d) We define the map

$$\begin{aligned} A\backslash\{0\} \times A\backslash\{0\} &\to A^{(3)}x^{-1} \\ (u, v) &\mapsto uxvx^{-1}. \end{aligned}$$

Following the strategy from the second item, we conclude that the map is injective, thus $|A^{(3)}| \geqslant c|A|^2$.

3. Let p be an odd prime number. With the same notation as in the previous exercise, consider

$$x = \begin{pmatrix} 1 & 2 \\ -1 & -1 \end{pmatrix} \in \mathrm{SL}_2(\mathbf{F}_p).$$

Let K be a subgroup of B such that $x^2 \in K$. Let $A = K \cup \{x, x^{-1}\}$.

(a) Show that
$$A^{(3)} = K \cup KxK \cup x^{-1}Kx.$$

(b) Deduce that
$$|A^{(3)}| \leqslant (2+c)|K|,$$
where c is the index of $K \cap x^{-1}Kx$ in K. (Hint: use the first exercise.)

(c) Assume that -1 is a square modulo p (which means that p is congruent to 1 modulo 4). Let K be the subgroup of B of the form
$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$$
where a is a square modulo p. Show that $x^2 \in K$ and that
$$[K : K \cap x^{-1}Kx] = p.$$

(d) Under the same assumption, show that $A^{(3)} \neq \mathrm{SL}_2(\mathbf{F}_p)$, and
$$|A^{(3)}| \leqslant c'|A|^{3/2}$$
for some constant $c' \geqslant 0$. (You may use without proof the fact that
$$|\,\mathrm{SL}_2(\mathbf{F}_p)| = p(p^2-1)$$
for all p odd.)
Note: one can show that A is a generating set of $\mathrm{SL}_2(\mathbf{F}_p)$, so this example shows that the best exponent in Helfgott's Theorem (Theorem 2.6.7 in the notes) cannot be larger than 1/2.

Solutions.

(a) Since $x^2 \in K$, we can show that any combination of product of 3 elements of A lie in $K \cup KxK \cup x^{-1}Kx$. Indeed, observe that
$$Kx^{-1}K = KxK,$$
since any k_1xK_2 can be written as $(k_1x^2)x^{-1}k_2$, and the other direction follows analogosly, since K is a subgroup so $x^{-1} \in K$. By a similar argument, we can show that $x^{-1}Kx = xKx^{-1}$. All the other possibilities follow trivially from the fact that K is a subgroup.

(b) From 1c it holds that
$$|A^{(3)}| \leqslant |K| + |x^{-1}Kx| + |KxK| \leqslant 2|K| + c|K|,$$
where c is the index of $K \cap x^{-1}Kx$ in K.

(c) First we observe that $x^2 = -I$, and since -1 is a square modulo p it follows that $x^2 \in K$. To prove that $[K : K \cap x^{-1}Kx] = p$ we use Lagrange's Theorem. First observe that $|K| = p\frac{p-1}{2}$ and

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

We must have $a - b - d = 0$ so that the product belogs to K. In this case

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

and since a is a square modulo p and $ad = 1$ it holds that d is also a square modulo p and we can conclude that $|K \cap x^{-1}Kx| = \frac{p-1}{2}$. Thus, from Lagrange's Theorem it holds that $|K : K \cap x^{-1}Kx| = \frac{p \cdot \frac{p-1}{2}}{\frac{p-1}{2}}$.

(d) From item b) it follows that

$$|A^{(3)}| \leqslant (2+p)p\frac{p-1}{2} < p(p^2-1) = |\operatorname{SL}_2(\mathbf{F}_p)|, \tag{1}$$

so $|A^3| \neq \operatorname{SL}_2(\mathbf{F}_p)$. The inequality $|A^{(3)}| \leqslant c|A|^{3/2}$ follows directly from (1) and the fact that $|A| = p\frac{p-1}{2} + 2$.