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

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
   $$\begin{cases} U^* \times U^* \times U^* & \to & \mathrm{SL}_2(\mathbf{F}_p) \\ (u, v, w) & \mapsto & uxvx^{-1}w \end{cases}$$
   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 $x \in \mathrm{SL}_2(\mathbf{F}_p) \smallsetminus B$. 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 $\delta$ to be?

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 $1/2$.