Homework 4

1. List the left and right cosets of the subgroups in the following list.
   (a) The subgroup $\langle 5\rangle$, generated by 5 (mod 20), inside $(\mathbb{Z}_{20}, +)$.
   (b) The subgroup $4\mathbb{Z} = \{4k : k \in \mathbb{Z}\}$ inside the group $(\mathbb{Z}, +)$.
   (c) The subgroup A_3 inside the symmetric group S_3.
   (d) The subgroup $H = \{e, (12)(34), (13)(24), (14)(23)\}$ in the group A_4.
   (e) The subgroup $H = \{e, (123), (132)\}$ in the group A_4.

   For which of these examples does it happen that every right coset is a left coset, and every left coset is a right coset?

(a) $0+\langle 5\rangle$, $1+\langle 5\rangle$, $2+\langle 5\rangle$, $3+\langle 5\rangle$, $4+\langle 5\rangle$. $\mathbb{Z}_{20}$ abelian $\Rightarrow$ Left cosets = Right Cosets.

(b) $0+4\mathbb{Z}$, $1+4\mathbb{Z}$, $2+4\mathbb{Z}$, $3+4\mathbb{Z}$. again Left cosets = Right cosets.

(c) Left cosets:

A_3, $(12)A_3 = \{(12), (23), (31)\}$

Right cosets:

A_3, $A_3(12) = \{(12), (23), (31)\}$

In this case Right cosets = Left cosets.

(d) Right cosets:

H

$H(123) = \{(123), (243), (142), (134)\}$

$H(132) = \{(132), (234), (124), (143)\}$

Left cosets: same as right cosets

H

$(123)H = H(123)$

$(132)H = H(132)$

(e) Right cosets:

H

$H(12)(34) = \{(12)(34), (134), (234)\}$

$H(13)(24) = \{(13)(24), (243), (124)\}$

$H(14)(23) = \{(14)(23), (142), (143)\}$

Left cosets:

H

$(12)(34)H = \{(12)(34), (243), (143)\}$

$(13)(24)H = \{(13)(24), (142), (234)\}$

$(14)(23)H = \{(14)(23), (134), (124)\}$

In this last case the left cosets are <u>not</u> the same as the right cosets (only common coset is H).

2. Let G be a group and $H \subset G$ a subgroup with index 2, i.e. $[G : H] = 2$. Show that $aH = Ha$ for all $a \in G$.

$[G:H] = 2 = \#$ left cosets $= \#$ right cosets

Let $a \in G$. Then either $a \in H$ or $a \notin H$.

If $a \in H$, $aH = H = Ha$.

If $a \notin H$, $aH \neq H$ and $Ha \neq H$.

Left (resp. right) cosets partition G so we have

$$G = H \cup aH \quad \& \quad H \cap aH = \emptyset$$

$$G = H \cup Ha \quad \& \quad H \cap Ha = \emptyset$$

Thus $aH = Ha = G \setminus H$.

In conclusion, $aH = Ha$ for all $a \in G$.

3. Recall that $\mathrm{GL}_2(\mathbb{R})$ is the group of real 2×2 matrices with non-zero determinant, and $\mathrm{SL}_2(\mathbb{R})$ is the subgroup of those matrices with determinant 1. Describe the right cosets of $\mathrm{SL}_2(\mathbb{R})$ in $\mathrm{GL}_2(\mathbb{R})$, and find the index of this subgroup.

Let $A \in GL_2(\mathbb{R})$. Then

$$SL_2(\mathbb{R}) \cdot A = \{ B \cdot A : \det(B) = 1 \}$$

Note $\det(B \cdot A) = \det(B)\det(A) = \det(A)$

Any $C \in GL_2(\mathbb{R})$ with $\det(C) = \det(A)$ can be written as $B \cdot A$ as above: $C = (CA^{-1}) \cdot A$ (note $\det(CA^{-1}) = 1$)

Thus $SL_2(\mathbb{R}) \cdot A = \{ C \in GL_2(\mathbb{R}) : \det(C) = \det(A) \}$

Thus for each $r \in \mathbb{R}^\times$ we have a right coset

$$\{ C : \det(C) = r \}$$

and this gives all right cosets.

Since $|\mathbb{R}^\times| = \infty$, $[GL_2(\mathbb{R}) : SL_2(\mathbb{R})] = \infty$.

4. Use Euler's Theorem or Fermat's Little Theorem to help compute the following.
   (a) $7^{26} \pmod{15}$
   (b) The last digit of 97^{123} (Hint: pass to integers mod 10)
   (c) $15^{83} \pmod{41}$

(a) $\mathbb{Z}_{15}^{\times} = \{1, 2, 4, 7, 8, 11, 13, 14\}$ $\quad \phi(15) = |\mathbb{Z}_{15}^{\times}| = 8$

Euler's Theorem: $7^{\phi(15)} \equiv 7^8 \equiv 1 \pmod{15}$

Thus $7^{26} \equiv 7^{3\cdot 8+2} \equiv 7^2 \equiv 49 \equiv 4 \pmod{15}$

(b) Last digit of a number = mod 10 reduction of number

$\mathbb{Z}_{10}^{\times} = \{1, 3, 7, 9\}$ $\quad \phi(10) = |\mathbb{Z}_{10}^{\times}| = 4$

Thus $97^{123} \equiv 97^{4\cdot 30+3} \equiv 97^3 \equiv 7^3 \equiv 7^2 \cdot 7$

$\equiv 49 \cdot 7 \equiv (-1)\cdot 7 \equiv -7 \equiv 3 \pmod{10}$

(c) 41 is prime

Fermat's Theorem: $15^{41-1} \equiv 1 \pmod{41}$

Thus $15^{83} \equiv 15^{40\cdot 2+3} \equiv 15^3 \equiv 15^2 \cdot 15 \equiv 225 \cdot 15$

$\equiv 20 \cdot 15 \equiv 300 \equiv 13 \pmod{41}$

5. Suppose G is a finite group, and $a \in G$. Suppose n is an integer greater than 1 that divides the order of G. Show that a^n cannot generate G, i.e. $\langle a^n \rangle \neq G$.

$$\begin{cases} a^n \text{ generates } G \iff \operatorname{ord}(a^n) = |G|. \\ a^{|G|} = e \quad \text{(consequence of Lagrange's Theorem)} \end{cases}$$

We have n divides $|G|$; write $|G| = nk$.

By assumption $n > 1$, so $k < |G|$.

Then $a^{|G|} = a^{nk} = (a^n)^k = e$.

So $\operatorname{ord}(a^n) \leq k < |G| \Rightarrow a^n$ doesn't generate G.

6. Let G be a finite group of order pq where p and q are distinct primes. Show that if $a, b \in G$ are non-identity elements of different orders, then the only subgroup in G containing a and b is the whole group G.

By Lagrange's Theorem, $\operatorname{ord}(a) = |\langle a \rangle|$ divides $|G| = pq$ and similarly for $\operatorname{ord}(b)$.

Since $a, b \neq e$, $\operatorname{ord}(a), \operatorname{ord}(b) \neq 1$.

Thus $\operatorname{ord}(a), \operatorname{ord}(b) \in \{p, q, pq\}$.

If $\operatorname{ord}(a) = pq$ then $\langle a \rangle = G$ and the claim is true; similarly if $\operatorname{ord}(b) = pq$.

So assume $\operatorname{ord}(a), \operatorname{ord}(b) \in \{p, q\}$.

Without loss of generality suppose $\operatorname{ord}(a) = p$ and $\operatorname{ord}(b) = q$ (recall $\operatorname{ord}(a) \neq \operatorname{ord}(b)$).

Then if H is a subgroup containing a and b, by Lagrange, p, q divide $|H|$ and $|H|$ divides $pq = |G| \Rightarrow |H| = pq$

$\Rightarrow H = G$, proving the claim.