Week 2 : Groups, subgroups and homomorphisms

Exercise 1: Let G and H be groups and $f : G \to H$ a homomorphism.

1. Prove that $\ker(f)$ is a subgroup of G, and $Im(f)$ is a subgroup of H.
2. Show that f is injective if and only if $\ker(f) = \{1_G\}$.

Solution to Exercise 1 :

1. Since $1_G \in \ker(f)$, $\ker(f) \neq \emptyset$. Take any $a, b \in \ker(f)$. Then $f(b) = 1_H$, and so $f(b^{-1}) = f(b)^{-1} = 1_H$ and so $b^{-1} \in \ker(f)$. Hence, $f(ab) = f(a)f(b) = 1_H 1_H = 1_H$, and so $ab \in \ker(f)$. Thus $\ker(f) \leq G$ by HW 1.

   If $x, y \in Im(f)$, there exist $a, b \in G$ such that $f(a) = x$ and $f(b) = y$. Then $xy = f(a)f(b) = f(ab)$ and so $xy \in Im(f)$. Moreover, $x^{-1} = f(a)^{-1} = f(a^{-1})$ and so $x^{-1} \in Im(f)$. Thus $Im(f) \leq H$.
2. Since $1_G \in \ker(f)$, if f is injective, $\ker(f) = \{1_G\}$. Assume now that $\ker(f) = \{1_G\}$. Let $x, y \in G$ be such that $f(x) = f(y)$. Then $f(x)f(y)^{-1} = 1_H$. Using HW1, we obtain $f(x)f(y)^{-1} = f(x)f(y^{-1}) = f(xy^{-1}) = 1_H$. Hence, $xy^{-1} \in \ker(f)$, and so $xy^{-1} = 1_G$. Thus $x = y$ and f is injective.

Exercise 2: Decide whether the following statement is true or false : two finite groups of the same order are isomorphic.

Solution to Exercise 2 : False. The groups $\mathbb{Z}/6\mathbb{Z}$ and $\mathscr{S}_3$ have order 6 but are not isomorphic since $\mathbb{Z}/6\mathbb{Z}$ is abelian and $\mathscr{S}_3$ is not.

Exercise 3: Decompose the following permutations as products of cycles with disjoint supports and find their signatures :

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 6 & 1 & 3 & 10 & 9 & 8 & 4 & 2 & 5 & 7 \end{pmatrix},$$
$$\tau = (8\,2\,4)(1\,4\,7)(3\,5\,6)(6\,1\,8).$$

Can you compute τ^{2025} ?

Solution to Exercise 3 : We have :

$$\sigma = (1\,6\,8\,2)(4\,10\,7)(5\,9),$$
$$\tau = (1\,2\,4\,7)(3\,5\,6\,8).$$

Hence $\mathrm{sign}(\sigma) = \mathrm{sign}(\tau) = 1$, and :

$$\tau^{2025} = (1\,2\,4\,7)^{2025}(3\,5\,6\,8)^{2025} = (1\,2\,4\,7)(3\,5\,6\,8) = \tau.$$

Exercise 4: For $n \geq 2$, find the signature of the permutation :

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \dots & (n-1) & n \\ n & (n-1) & (n-2) & \dots & 2 & 1 \end{pmatrix}.$$

Solution to Exercise 4 : We have :

$$\sigma = (1\ n)(2\ (n-1))(3\ (n-2))\dots\left(\left[\frac{n-1}{2}\right]\ \left[\frac{n+3}{2}\right]\right).$$

Hence :

$$\mathrm{sign}(\sigma) = (-1)^{\left[\frac{n-1}{2}\right]}.$$

Exercise 5: Let G be a group and $A \subseteq G$. If $A = \emptyset$, show that $\langle A \rangle = \{1_G\}$. If $A \neq \emptyset$, show that $\langle A \rangle = \{g_1^{\epsilon_1} \dots g_n^{\epsilon_n} \mid n \in \mathbb{N}, \epsilon_i \in \{\pm 1\}, g_i \in A, 1 \leq i \leq n\}$.

Solution to Exercise 5 : If $A = \emptyset$, $A \subset \{1_G\}$, and clearly, $\{1_G\}$ is the smallest subgroup of G containing A. Hence, $\langle A \rangle = \{1_G\}$. Suppose that $A \neq \emptyset$. Let $H = \{g_1^{\epsilon_1} \dots g_n^{\epsilon_n} \mid n \in \mathbb{N}, \epsilon_i \in \{\pm 1\}, g_i \in A, 1 \leq i \leq n\}$. Then $H \neq \emptyset$. Clearly a product of any two elements of H is again in H, and so is the inverse of any element of H. Hence, $H \leq G$ and $A \subseteq H$. Since $\langle A \rangle$ is the smallest subgroup of G containing A, $\langle A \rangle \subseteq H$. But every subgroup of G containing A, contains every element of H, and so $H \subseteq \langle A \rangle$. Thus $H = \langle A \rangle$.

Exercise 6: Let G be a group, and $g \in G$ an element of finite order n. Prove that $\langle g \rangle = \{1, g, \dots, g^{n-1}\}$ and $|\langle g \rangle| = o(g)$.

Solution to Exercise 6 : If $g = 1$, then $\langle g \rangle = \{1_G\}$ and so $o(g) = |\langle g \rangle|$.

Suppose that $g \neq 1$. Then $1_G, g, \dots, g^{n-1}$ are distinct, for if $g^i = g^j$ for some $1 \leq i < j \leq n$, $0 < j - i < n$ and $g^{j-i} = 1_G$, a contradiction. Let $A := \{1, g, \dots, g^{n-1}\} \neq \emptyset$. Clearly, $A \subseteq \langle g \rangle$. Take any g^i and g^j in A. Then $g^i g^j = g^{i+j} = g^{qn+r}$ for some $q, r \in \mathbb{N}$ with $0 \leq r < n$. But $g^{qn+r} = (g^n)^q g^r = g^r \in A$. Moreover, for each $g^i \in A$, $g^{n-i} \in A$ and $g^{n-i} g^i = g^n = 1_G$, i.e., $g^{n-i} = g^{-1} \in A$. Hence, $A \leq G$, and so $A = \langle g \rangle$. In particular, $o(g) = |\langle g \rangle|$.

Exercise 7:

1. Is a cyclic group abelian?
2. Prove that any two infinite cyclic groups are isomorphic.
3. If G and H are two cyclic groups and $|G| = |H| = n$, $n \in \mathbb{N}^*$, then $G \cong H$.

Solution to Exercise 7 :

1. Yes. Let G be a cyclic group. By definition, there exists $g \in G$ such that $G = \{g^k \mid k \in \mathbb{Z}\}$. Hence, for any $x, y \in G$, $x = g^m$ and $y = g^n$ for some $m, n \in \mathbb{Z}$, and so $xy = g^m g^n = g^{m+n} = g^n g^m = yx$.

2. If G and H are infinite cyclic groups, there exist $g \in G$ and $h \in H$ such that $G = \{g^k \mid k \in \mathbb{Z}\}$ and $H = \{h^k \mid k \in \mathbb{Z}\}$. Observe that if $m, n \in \mathbb{Z}$ and $m > n$, then $g^m \neq g^n$, for otherwise, $m-n > 0$ and $g^{m-n} = 1_G$, and so $o(g) \leq m-n$, a contradiction. Similarly, $h^m \neq h^n$. Consider a map $f : G \to H$ with $f(g^k) = h^k$ for $k \in \mathbb{Z}$. Clearly, f is a bijection. Take any $x, y \in G$. Then $x = g^m$ and $y = g^n$ for some $m, n \in \mathbb{Z}$, and so $f(xy) = f(g^m g^n) = f(g^{m+n}) = h^{m+n} = h^m h^n = f(x)f(y)$. Thus f is an isomorphism and so $G \cong H$.
3. Let G and H be finite cyclic groups with $|G| = |H| = n$. Let g be a generator of G and h a generator of H. Then the order of g is finite and $o(g) = n$. Similarly, $o(h) = n$. Hence, $G = \{g, g^2, \ldots, g^{n-1}, g^n = 1\}$ and $H = \{h, \ldots, h^{n-1}, h^n = 1\}$. Consider a map $f : G \to H$ with $f(g^i) = h^i$ for $1 \leq i \leq n$. Clearly, this is a bijection. Take any $g^i, g^j \in G$. Then $f(g^i g^j) = f(g^{i+j})$. If $i + j \leq n$, $f(g^{i+j}) = h^{i+j} = h^i h^j = f(g^i)f(g^j)$. If $i + j > n$, there exist $q, r \in \mathbb{N}$ such that $i + j = qn + r$ with $0 \leq r \leq n-1$. Then $f(g^i g^j) = f((g^n)^q g^r) = f(g^r) = h^r$ while $f(g^i)f(g^j) = h^i h^j = h^{i+j} = h^{qn+r} = (h^n)^q h^r = h^r$, and so f is a homomorphism. It follows that $G \cong H$.

Exercise 8: Let p be a prime and G a group of order p. Then G is cyclic.

Solution to Exercise 8 : Take any $g \in G \setminus \{1\}$. By the corollary to the Lagrange's Theorem, $o(g)$ divides $|G| = p$. Since p is a prime, $o(g) \in \{1, p\}$. As $g \neq 1_G$, $o(g) = p$. By the previous exercise, $|\langle g \rangle| = p$, and as $\langle g \rangle \subseteq G$, $G = \langle g \rangle$ is cyclic.

Exercise 9: Prove that the following sets generate the symmetric group S_n :

1. the set of all transpositions;
2. the set $\{(1\,2), (2\,3), \ldots, ((n-1)\; n)\}$.
3. the transposition $(1\,2)$ and the cycle $(1\,2\,\ldots\,n)$.

Solution to Exercise 9 :

1. We proceed by induction on n. If $n = 1$, the statement is obvious. Otherwise, take any element $\sigma \in \mathscr{S}_n$. Define $\tau := \sigma$ if $\sigma(n) = n$ and $\tau := (n\;\sigma(n))\sigma$ otherwise. Since $\tau(n) = n$, we can consider the restriction $\tau|_{\{1,\ldots,n-1\}}^{\{1,\ldots,n-1\}} \in \mathscr{S}_{n-1}$. By the inductive assumption, $\tau|_{\{1,\ldots,n-1\}}^{\{1,\ldots,n-1\}}$ is a product of transpositions in $\mathscr{S}_{n-1}$. We deduce that both τ and σ are products of transpositions in $\mathscr{S}_n$, as wished.
2. Fix two elements $a < b$ in $\{1, \ldots, n\}$. Then :

$$
\begin{aligned}
(a\;b) = (a\;(a+1))((a+1)\;(a+2))\ldots((b-2)\;(b-1))((b-1)\;b)((b-2)\;(b-1)) \\
\ldots((a+1)\;(a+2))(a\;(a+1)).
\end{aligned}
$$

Hence question (1) implies that $\mathscr{S}_n$ is generated by

$$\{(1\,2), (2\,3), \ldots, ((n-1)\; n)\}.$$

3. By the previous question, it is enough to observe that, for each $c \in \{1, ..., n-1\}$:

$$(c\ (c+1)) = (1\ 2\ ...\ n)^{c-1}(1\ 2)(1\ 2\ ...\ n)^{1-c}.$$

Exercise 10: ⋆ Let $n \in \mathbb{N}^*$ and consider the symmetric group S_n. Recall that $A_n = \{\sigma \in \mathscr{S}_n \mid \sigma \text{ is even}\}$. Show that A_n is a subgroup of S_n. Prove that the alternating group $\mathscr{A}_n$ is generated by the set of 3-cycles.

Solution to Exercise 10 : As $1 \in A_n$, $A_n \neq \emptyset$. Take any $a, b \in A_n$. Then $a = t_1...t_n$ and $b = s_1...s_m$ for some even $n, m \in \mathbb{N}$ where $t_1, ..., t_n, s_1, ..., s_m$ are involutions. Then $ab = t_1...t_n s_1...s_n \in A_n$ as $n+m$ is even, and $a^{-1} = t_n...t_1 \in A_n$. Hence, $A_n \leq S_n$.

Any element of A_n is a product of an even number of transpositions. The group A_n is therefore generated by products of two transpositions. But if a, b, c, d are pairwise distinct elements of $\{1, ..., n\}$, we have :

$$(a\ b)(a\ c) = (a\ c\ b), \quad (a\ b)(c\ d) = (a\ c\ b)(a\ c\ d).$$

Hence A_n is generated by 3-cycles.

Exercise 11: Let X and Y be two sets with $|X| = |Y|$. Prove that $\mathrm{Sym}(X) \cong \mathrm{Sym}(Y)$. (Recall that $\mathrm{Sym}(X)$ is a group of all permutations of X under composition of maps.)

Solution to Exercise 11 : Let $\phi : X \to Y$ be a bijection (it exists as $|X| = |Y|$). Then there exists a bijection $\phi^{-1} : Y \to X$. Take any $f \in \mathrm{Sym}(X)$ and consider $\phi \circ f \circ \phi^{-1} : Y \to Y$. This is a bijection as a composition of bijections. Hence, $\phi \circ f \circ \phi^{-1} \in \mathrm{Sym}(Y)$. Hence, we obtained a map $\Phi : \mathrm{Sym}(X) \to \mathrm{Sym}(Y)$ with $\Phi(f) = \phi \circ f \circ \phi^{-1}$. This is a homomorphism as $\Phi(f \circ g) = \phi \circ f g \circ \phi^{-1} = \phi \circ f \phi^{-1} \circ \phi \circ g \phi^{-1} = \Phi(f)\Phi(g)$. Let $f \in \ker(\Phi)$. Then $\phi \circ f \circ \phi^{-1} = id_Y$, and so $f = id_X$. Thus $\ker(f) = \{id_X\}$ and so f is injective by Q1. Take any $g \in \mathrm{Sym}(Y)$. Then $\phi^{-1} \circ g \circ \phi \in \mathrm{Sym}(X)$ and $\Phi(\phi^{-1} \circ g \circ \phi) = g$. Thus Φ is an isomorphism.

Exercise 12: ⋆⋆ Let $n \geq 3$ be an integer. Prove that S_n is not generated by $n-2$ transpositions.

Solution to Exercise 12 : Let m be a positive integer and let $\tau_1, ..., \tau_m$ be m transpositions that generate $\mathscr{S}_n$. Fix an integer $s \in \{1, ..., m\}$. For $i, j \in \{1, ..., n\}$, say that $i \sim_s j$ if one can find a finite sequence $a_1, ..., a_r$ in $\{1, ..., n\}$ such that $a_1 = i$, $a_r = j$ and $(a_k\ a_{k+1}) \in \{\tau_1, ..., \tau_s\}$. One easily checks that $\sim_s$ is an equivalence relation. Moreover, $|\{1, ..., n\}/\sim_1| = n-1$, and for $s \geq 2$:

$$|\{1, ..., n\}/\sim_s| = \begin{cases} |\{1, ..., n\}/\sim_{s-1}| \text{ if } a \sim_{s-1} b \\ |\{1, ..., n\}/\sim_{s-1}| + 1 \text{ if } a \nsim_{s-1} b \end{cases}$$

where $\tau_s = (a\ b)$. By an easy induction, we deduce that $|\{1,\ldots,n\}/\sim_s| \leq n-s$ for each $s \in \{1,\ldots,m\}$. In particular, $|\{1,\ldots,n\}/\sim_m| \leq n-m$. But for any equivalence class $C \in \{1,\ldots,n\}/\sim_m$, we have :

$$\mathscr{S}_n = \langle \tau_1,\ldots,\tau_m\rangle \subseteq \{\sigma \in \mathscr{S}_n | \sigma(C) = C\}.$$

Hence there is only one equivalence class in $\{1,\ldots,n\}/\sim_m$, and $n-m \geq 1$.

Exercise 13: ⋆ Consider the following complex matrices :

$$A = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Let Q_8 be the subgroup of $GL_2(\mathbb{C})$ generated by A and B. It is called the *quaternion group.*

1. Check that :
$$A^4 = I_2, \quad A^2 = B^2, \quad BA = A^3B.$$
2. Deduce that Q_8 has order 8.

Solution to Exercise 13 :

1. Explicit computation.
2. Consider the set $X = \{A^rB^s \,|\, 0 \leq r \leq 3, 0 \leq s \leq 1\}$. Observe that, by the equality $BA = A^3B$, we have, for $r, r' \in \{0,1,2,3\}$ and $s, s' \in \{0,1\}$:
$$A^rB^sA^{r'}B^{s'} = A^rB^{s-1}A^{3r'}B^{s'+1} = A^rB^{s-2}A^{9r'}B^{s'+2} = \ldots = A^{r+3^sr'}B^{s'+s}.$$
By using the equalities $A^4 = I_2$ and $A^2 = B^2$, if we let k be the integer in $\{0,1,2,3\}$ such that $k \equiv r+3^sr' \mod 4$ and l be the integer in $\{0,1,2,3\}$ such that $l \equiv r+3^sr'+2 \mod 4$, we get :
$$A^rB^sA^{r'}B^{s'} = \begin{cases} A^kB^{s+s'} & \text{if } s+s' < 2 \\ A^l & \text{otherwise.} \end{cases} \tag{$\star$}$$
Hence $A^rB^sA^{r'}B^{s'} \in X$, and we conclude that the product of two elements of X always lies in X.
Moreover, for $r \in \{0,1,2,3\}$, the inverse of A^r is A^m where m is the integer in $\{0,1,2,3\}$ such that $r+m \equiv 0 \mod 4$, and according to the equality ($\star$), the inverse of A^rB is A^mB where m is the integer in $\{0,1,2,3\}$ such that $r+3^sm+2 \equiv 0 \mod 4$. In particular, the inverse of an element of X always lies in X. We deduce that X is a subgroup of $GL_2(\mathbb{C})$, and hence $X = \langle A, B\rangle = Q_8$. One can then easily check that the A^rB^s for $r \in \{0,1,2,3\}$ and $s \in \{0,1\}$ are pairwise distinct. Hence Q_8 has order 8.

Exercise 14: ⋆

1. Prove that the group $SL_2(\mathbb{Z})$ is generated by the matrices :

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

2. Consider the matrix :

$$B := \begin{pmatrix} 72 & 313 \\ 23 & 100 \end{pmatrix} \in SL_2(\mathbb{Z}).$$

Write B as a product of powers of S and T.

Solution to Exercise 14 :

1. Set $G := \langle S, T\rangle \subseteq SL_2(\mathbb{Z})$ and proceed by contradiction. Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ be a matrix in $SL_2(\mathbb{Z}) \setminus G$ such that $|a| + |c|$ is minimal. Observe that, for $k \in \mathbb{Z}$:

$$SA = \begin{pmatrix} -c & -d \\ a & b \end{pmatrix}, \qquad T^k A = \begin{pmatrix} a+kc & b+kd \\ c & d \end{pmatrix}.$$

Up to replacing A by SA, we may and do assume that $|c| \leq |a|$. If $c \neq 0$, by writing the Euclidean division $a = qc + r$ of a by c, we get :

$$T^{-q} A = \begin{pmatrix} r & b-qd \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \setminus G.$$

This contradicts the minimality of $|a| + |c|$. Hence $c = 0$.

Since $\det(A) = 1$, we have $ad = 1$, so that $(a,d) \in \{(1,1),(-1,-1)\}$. Up to replacing A by $S^2 A = -A$, we can assume that $a = d = 1$. We then get $A = T^b$: contradiction! Hence $G = SL_2(\mathbb{Z})$.

2. The previous proof gives an algorithm to decompose any matrix in $SL_2(\mathbb{Z})$ as a product of powers of S and T. For B :

$$\begin{aligned}
B &= \begin{pmatrix} 72 & 313 \\ 23 & 100 \end{pmatrix} = T^3 \begin{pmatrix} 3 & 13 \\ 23 & 100 \end{pmatrix} \\
&= T^3 S^{-1} \begin{pmatrix} -23 & -100 \\ 3 & 13 \end{pmatrix} = T^3 S^{-1} T^{-8} \begin{pmatrix} 1 & 4 \\ 3 & 13 \end{pmatrix} \\
&= T^3 S^{-1} T^{-8} S^{-1} \begin{pmatrix} -3 & -13 \\ 1 & 4 \end{pmatrix} = T^3 S^{-1} T^{-8} S^{-1} T^{-3} \begin{pmatrix} 0 & -1 \\ 1 & 4 \end{pmatrix} \\
&= T^3 S^{-1} T^{-8} S^{-1} T^{-3} S^{-1} \begin{pmatrix} -1 & -4 \\ 0 & -1 \end{pmatrix} = T^3 S^{-1} T^{-8} S^{-1} T^{-3} S^{-1} S^2 T^4 \\
&= T^3 S^{-1} T^{-8} S^{-1} T^{-3} S T^4.
\end{aligned}$$

Exercise 15: $\star\star$ Let G be the subgroup of $GL_2(\mathbb{Q})$ generated by $A := \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}$ and $B := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Let H be the subgroup of G given by those matrices in G that have ones on the diagonal. Prove that H is not finitely generated.

Solution to Exercise 15 : By an easy induction, one checks that any matrix in G is of the form

$$\begin{pmatrix} x & \frac{a}{2^b} \\ 0 & 1 \end{pmatrix}$$

for some rational number x and some integers a, b. Moreover, for each pair $(a, b) \in (\mathbb{Z} \setminus \{0\})^2$:

$$\begin{pmatrix} 1 & \frac{a}{2^b} \\ 0 & 1 \end{pmatrix} = A^{-b} B^a A^b.$$

Hence :

$$H = \left\{ \begin{pmatrix} 1 & \frac{a}{2^b} \\ 0 & 1 \end{pmatrix} | (a, b) \in \mathbb{Z} \times (\mathbb{Z} \setminus \{0\}) \right\} \cong \left\{ \frac{a}{2^b} | (a, b) \in \mathbb{Z} \times (\mathbb{Z} \setminus \{0\}) \right\} \subseteq \mathbb{Q}.$$

If H was finitely generated, then so would be the group :

$$H' := \left\{ \frac{a}{2^b} | (a, b) \in (\mathbb{Z} \setminus \{0\})^2 \right\}.$$

But if $\frac{a_1}{2^{b_1}}, \dots, \frac{a_r}{2^{b_r}}$ were generators of H', then every element of H' would be of the form $\frac{a}{2^b}$ with $a \in \mathbb{Z}$ and $b \leq \max\{b_1, \dots, b_r\}$. Since this is not possible, H is not finitely generated.