WEEK 1 : REVISION

Exercise 1:

Recall that a group is a set G with a binary operation $\circ : G \times G \to G$ that satisfies the following properties :

(Associativity) for all $a, b, c \in G$, $(a \circ b) \circ c = a \circ (b \circ c)$,

(Identity) there exists $e \in G$ such that $a \circ e = e \circ a = a$ for all $a \in G$,

(Inverse) given $a \in G$, there exists $b \in G$ such that $a \circ b = b \circ a = e$.

1. Let G be a set with a binary operation $\circ : G \times G \to G$. Assume that the operation is associative. Assume further that there exists $e \in G$ such that for all $a \in G$, $e \circ a = a$. Finally, assume also that for every $a \in G$, there exists $b \in G$ such that $b \circ a = e$. Prove that $(G, \circ)$ is a group.
2. Let $(G, \circ)$ be a group. Prove that G has a unique identity element.
3. Let $(G, \circ)$ be a group. Prove that any $g \in G$ has a unique inverse.

Solution to Exercise 1 :

1. Take any $a \in G$, and let $b \in G$ be such that $b \circ a = e$. Then $b \circ (a \circ e) = (b \circ a) \circ e = e \circ e = e = b \circ a$. Let $c \in G$ be such that $c \circ b = e$. Multiplying both sides by c, we obtain $(c \circ b) \circ (a \circ e) = (c \circ b) \circ a$. Hence, $e \circ (a \circ e) = e \circ a$, i.e., $a \circ e = a$.

   Also, $b \circ (a \circ b) = (b \circ a) \circ b = e \circ b = b$. Multiplying both sides by c, we get $(c \circ b) \circ (a \circ b) = c \circ b$, and so $e \circ (a \circ b) = e$. Thus $a \circ b = e$. Since the operation is associative, we may conclude that $(G, \circ)$ is a group.
2. Let e and e' be two identities of $(G, \circ)$. Then $e = e \circ e' = e'$.
3. Let b and b' be two inverses of a. Then $b = e \circ b = (b' \circ a) \circ b = b' \circ (a \circ b) = b' \circ e = b'$.

Exercise 2: Recall that a group $(G, \circ)$ is abelian iff $a \circ b = b \circ a$ for all $a, b \in G$. Decide whether the following pairs are groups. In the case when $(G, \circ)$ is a group, decide whether it is abelian.

1. $(\mathbb{Z}, +)$
2. $(\mathbb{Z} \setminus \{0\}, \cdot)$
3. Fix $n \in \mathbb{Z}$ with $n \geq 1$. Recall that $\mathbb{Z}/n\mathbb{Z}$ is the set of equivalence classes of integers with respect to the equivalence relation : $x \sim y$ if n divides $x - y$, and it has representatives $[0], \ldots, [n-1]$. Recall further that one can define an operation $+$ on $\mathbb{Z}/n\mathbb{Z}$ so that $[a] + [b] = [a + b]$. Consider $(\mathbb{Z}/n\mathbb{Z}, +)$.
4. $GL(2, \mathbb{R}) = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{R}, ad - bc \neq 0\}$ with matrix multiplication.

5. The set G of functions $f : \mathbb{R} \to \mathbb{R}$ of the form $x \mapsto ax + b$ for some $a \in \mathbb{R}^\times$ and $b \in \mathbb{R}$, endowed with composition.
6. The set H of non-decreasing functions from $\mathbb{R}$ to $\mathbb{R}$ endowed with addition.
7. The set $K =]-1, 1[$ endowed with the operation $x \star y = \frac{x+y}{1+xy}$.

Solution to Exercise 2 :

1. This is an abelian group (one has to check).
2. Not a group : for example, 2 has no inverse.
3. This is an abelian group (see the notes for MAA201).
4. This is a non-abelian group (see notes for MAA201).
5. For $a \in \mathbb{R}^\times$ and $b \in \mathbb{R}$, denote by $\varphi_{a,b}$ the map $\mathbb{R} \to \mathbb{R}$ that sends $x \in \mathbb{R}$ to $ax + b$. One can then check that, for $a, c, e \in \mathbb{R}^\times$ and $b, d, f \in \mathbb{R}$:

$$\varphi_{a,b} \circ \varphi_{c,d} = \varphi_{ac,ad+b} \in G, \tag{1}$$

$$\begin{aligned}(\varphi_{a,b} \circ \varphi_{c,d}) \circ \varphi_{e,f} = \varphi_{ac,ad+b} \circ \varphi_{e,f} = \varphi_{ace,acf+ad+b} \\ = \varphi_{a,b} \circ \varphi_{ce,cf+d} = \varphi_{a,b} \circ (\varphi_{c,d} \circ \varphi_{e,f}),\end{aligned} \tag{2}$$

$$\varphi_{a,b} \circ \varphi_{1,0} = \varphi_{1,0} \circ \varphi_{a,b} = \varphi_{a,b}, \tag{3}$$

$$\varphi_{a,b} \circ \varphi_{a^{-1},-ba^{-1}} = \varphi_{a^{-1},-ba^{-1}} \circ \varphi_{a,b} = \varphi_{1,0}. \tag{4}$$

Equality (1) shows that G is closed under composition. Moreover, equality (2) shows that composition is associative, equality (3) shows that $\varphi_{1,0}$ is the identity, and equality (3) shows that each element of G has an inverse. Hence G is a group. It is not abelian since :

$$\varphi_{1,1} \circ \varphi_{2,0} = \varphi_{2,1} \neq \varphi_{2,2} = \varphi_{2,0} \circ \varphi_{1,1}.$$

6. The identity element here is the zero function. But the identity function has no inverse because the function $x \mapsto -x$ is not in H. Hence H is not a group.
7. First observe that, for $x, y \in (-1, 1)$, we have :

$$1 + xy \pm (x + y) = (1 \pm x)(1 \pm y) > 0.$$

Hence $x \star y \in K$, and $\star$ is a binary operation on K. Now, for $x, y, z \in K$:

$$\begin{aligned}(x \star y) \star z = \frac{x+y}{1+xy} \star z = \frac{\frac{x+y}{1+xy} + z}{1 + \frac{x+y}{1+xy} z} \\ = \frac{x+y+z+xyz}{1+xy+xz+yz} = \frac{x + \frac{y+z}{1+yz}}{1 + x\frac{y+z}{1+yz}} \\ = x \star \frac{y+z}{1+yz} = x \star (y \star z),\end{aligned}$$

$$x \star 0 = 0 \star x = x,$$
$$x \star (-x) = (-x) \star x = 0.$$

Hence K is a group.

Exercise 3:

1. Let G be a group such that $g^2 = 1$ for all $g \in G$. Prove that G is abelian.
2. Let p be an odd prime number. Consider the set U of upper triangular matrices in $GL_3(\mathbb{Z}/p\mathbb{Z})$ that have ones on the diagonal. We endow U with the matrix multiplication. Prove that U is a non-abelian group such that $u^p = 1$ for all $u \in U$.

Solution to Exercise 3 :

1. We have $g = g^{-1}$ for every $g \in G$. Hence :

$$\forall (g,h) \in G^2,\ gh = (gh)^{-1} = h^{-1}g^{-1} = hg.$$

The group G is therefore abelian.

2. One has to check that U is a group as in the previous exercise. Now any element $u \in U$ can be written as $u = I_3 + v$ for some upper triangular matrix v having zeroes on the diagonal. By direct calculation we can see that $v^3 = 0$ and hence, by the binomial formula, we have :

$$u^p = I_3 + pv + \frac{p(p-1)}{2}v^2 = I_3.$$

The group U is not abelian because the matrices :

$$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

are both in U but do not commute.

Exercise 4: Let $(G, \circ)$ and $(H, *)$ be two groups and $f : G \to H$ a homomorphism. (Recall, that a map $f : G \to H$ is a homomorphism if for all $g_1, g_2 \in G$, $f(g_1 \circ g_2) = f(g_1) * f(g_2)$. Also, recall that a bijective homomorphism is called an isomorphism and two groups are isomorphic if there exists an isomorphism between them.)

1. Show that $f(e_G) = e_H$.

2. Show that for all $g \in G$, $f(g^{-1}) = f(g)^{-1}$.

Solution to Exercise 4 :

1. $f(e_G) = f(e_G \circ e_G) = f(e_G) * f(e_G)$. Since $f(e_G) \in H$, it has an inverse $f(e_G)^{-1}$. Multiplying both sides by $f(e_G)^{-1}$, we obtain $f(e_G) * f(e_G)^{-1} = f(e_G) * f(e_G) * f(e_G)^{-1}$, and so $e_H = f(e_G) * (f(e_G) * f(e_G)^{-1}) = f(e_G) * e_H = f(e_G)$.

2. Take any $g \in G$. Then $f(e_G) = f(g \circ g^{-1}) = f(g) * f(g^{-1})$. As $f(g) \in H$, it has the inverse $f(g)^{-1}$. Multiplying both sides by $f(g)^{-1}$ on the left, we obtain $f(g)^{-1} * f(e_G) = f(g)^{-1} * f(g) * f(g^{-1})$. Since $f(e_G) = e_H$, $f(g)^{-1} * e_H = (f(g)^{-1} * f(g)) * f(g^{-1}) = e_H * f(g^{-1})$, and so $f(g)^{-1} = f(g^{-1})$.

Exercise 5: Prove that the groups $(\mathbb{R}, +)$ and $(\mathbb{R}_{>0}, \times)$ are isomorphic. Are $(\mathbb{Q}, +)$ and $(\mathbb{Q}_{>0}, \times)$ isomorphic?

Solution to Exercise 5 : Consider the exponential map $\exp : \mathbb{R} \to \mathbb{R}_{>0}$. This is a bijection such that

$$\forall (x, y) \in \mathbb{R}^2, \exp(x + y) = \exp(x) \exp(y).$$

This is therefore an isomorphism between $(\mathbb{R}, +)$ and $(\mathbb{R}_{>0}, \times)$.

Now let $f : \mathbb{Q} \to \mathbb{Q}_{>0}$ be a group homomorphism. Let $a \in \mathbb{Q}$. For each $n \geq 1$, we have $f(a) = f(a/n)^n$, hence :

$$f(a) \in \{x \in \mathbb{Q}_{>0} | \forall n \geq 1, \exists y \in \mathbb{Q}_{>0}, x = y^n\} = \{1\}.$$

The homomorphism f is therefore trivial and $(\mathbb{Q}, +)$ and $(\mathbb{Q}_{>0}, \times)$ are not isomorphic.

Exercise 6: Find all group homomorphisms :

1. from $(\mathbb{Q}, +)$ to $(\mathbb{Z}, +)$.

2. from $(\mathbb{Z}/100\mathbb{Z}, +)$ to $(\mathbb{Z}, +)$.

Solution to Exercise 6 :

1. Let $f : \mathbb{Q} \to \mathbb{Z}$ be a non-trivial homomorphism, and take an element $a \in \mathbb{Q}$ such that $f(a) \neq 0$. Then $f(a) + f(-a) = f(a + (-a)) = f(0) = 0$, and without loss of generality we may assume that $f(a) > 0$. Then adding $f\left(\frac{a}{2f(a)}\right)$ to itself $2f(a)$ times we obtain that

$$2f(a) f\left(\frac{a}{2f(a)}\right) = f(a),$$

and hence $f\left(\frac{a}{2f(a)}\right) = \frac{1}{2} \notin \mathbb{Z}$, a contradiction. Hence the only homomorphism from $(\mathbb{Q}, +)$ to $(\mathbb{Z}, +)$ is the trivial homomorphism.

2. Let $f : \mathbb{Z}/100\mathbb{Z} \to \mathbb{Z}$ be a homomorphism. For any $a \in \mathbb{Z}/100\mathbb{Z}$, we have $100a = 0$, and hence, $100f(a) = f(100a) = f(0) = 0$. We deduce that $f(a) = 0$. This being true for every $a \in \mathbb{Z}/100\mathbb{Z}$, we get that f is the trivial homomorphism.

Exercise 7: Let G be a group. Prove that the map $f : x \mapsto x^{-1}$ is a homomorphism if, and only if, G is abelian.

Solution to Exercise 7 : If f is a group homomorphism, then, for any $x, y \in G$, we have :

$$f(x)f(y) = f(xy).$$

Hence :

$$x^{-1}y^{-1} = (xy)^{-1} = y^{-1}x^{-1},$$

so that $xy = yx$. The group G is therefore abelian. Conversely, if G is abelian, then for any $x, y \in G$, we have $xy = yx$. Hence $x^{-1}y^{-1} = y^{-1}x^{-1} = (xy)^{-1}$, so that $f(x)f(y) = f(xy)$. Therefore f is a group homomorphism.

Exercise 8: Are the groups $(\mathbb{R}^\times, \cdot)$ and $(\mathbb{C}^\times, \cdot)$ isomorphic?

Solution to Exercise 8 : Let $f : \mathbb{C}^\times \to \mathbb{R}^\times$ be an isomorphism. Then, for each $z \in \{1, -1, i, -1\}$, we have :

$$f(z)^4 = f(z^4) = f(1) = 1.$$

Hence $f(z) \in \{1, -1\}$. This contradicts the injectivity of f. Hence $(\mathbb{R}^\times, \cdot)$ and $(\mathbb{C}^\times, \cdot)$ are not isomorphic.

Exercise 9: Let G be the following set of real matrices :

$$G = \{\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \mid a \in \mathbb{R}\}$$

We endow G with the matrix multiplication. Prove that G is isomorphic to $(\mathbb{R}, +)$.

Solution to Exercise 9 : One easily checks that G is a group (same method as in exercise 2). Consider now the map :

$$\begin{aligned} f : \mathbb{R} &\to G \\ a &\mapsto \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}. \end{aligned}$$

This map is of course bijective (check). Moreover, for any $a, b \in \mathbb{R}$:

$$f(a)f(b) = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a+b \\ 0 & 1 \end{pmatrix} = f(a+b).$$

Hence f is a group isomorphism.

Exercise 10: Let G be the set of functions $f : \mathbb{R} \to \mathbb{R}$ of the form $x \mapsto ax+b$ with $a \in \mathbb{R}^\times$ and $b \in \mathbb{R}$, endowed with composition. Let H be the set of invertible real matrices of the form :

$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}.$$

endowed with matrix multiplication. Prove that G and H are groups and that they are isomorphic.

Solution to Exercise 10 : In exercise 2 we saw that G is a group. One can check that H is a group (same method as in exercise 2). As in exercise 2, for $a \in \mathbb{R}^\times$ and $b \in \mathbb{R}$, denote by $\varphi_{a,b}$ the map $\mathbb{R} \to \mathbb{R}$ that sends $x \in \mathbb{R}$ to $ax+b$. Consider now the map :

$$\begin{aligned} f : G &\to H \\ \varphi_{a,b} &\mapsto \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}. \end{aligned}$$

This map is of course bijective. Moreover, for any $a, c \in \mathbb{R}^\times$ and $b, d \in \mathbb{R}$:

$$f(\varphi_{a,b}) f(\varphi_{c,d}) = \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} c & d \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} ac & ad+b \\ 0 & 1 \end{pmatrix} = f(\varphi_{ac,ad+b}) = f(\varphi_{a,b} \circ \varphi_{c,d}).$$

Hence f is an isomorphism.

Exercise 11: Let G be a group and let $\mathrm{Aut}(G) = \{f : G \to G \mid f \text{ is an isomorphism}\}$, the set of automorphisms of G.

1. Prove that, endowed with composition, $\mathrm{Aut}(G)$ is a group.
2. For $g \in G$, we consider the inner automorphism :

$$\begin{aligned} \gamma_g : G &\mapsto G \\ h &\mapsto ghg^{-1}. \end{aligned}$$

Prove that the map $\phi : G \to \mathrm{Aut}(G)$ that sends an element $g \in G$ to γ_g is a group homomorphism.

Solution to Exercise 11 :

1. This can easily be checked by the same method as in exercise 2.
2. For any $g, g, h \in G$, we have :

$$\gamma_g \circ \gamma_{g'}(h) = \gamma_g(g'hg'^{-1}) = gg'hg'^{-1}g^{-1} = (gg')h(gg')^{-1} = \gamma_{gg'}(h).$$

Hence $\gamma_g \circ \gamma_{g'} = \gamma_{gg'}$ and ϕ is indeed a group homomorphism.

Exercise 12: Let $(G,\circ)$ be a group. Recall that a subset H of G is called a subgroup of G if it forms a group under the same operation as that one of G (i.e., $(H,\circ)$ is a group).

1. If H is a subgroup of G, show that $e_H = e_G$.
2. Let H be a non-empty subset of G. Show that H is a subgroup of G if and only if for all $a,b \in H$, $a \circ b \in H$ and $a^{-1} \in H$.

Solution to Exercise 12 :

1. Let e_H be the identity of $(H,\circ)$. Then $e_H \circ e_H = e_H$. Since $e_H \in H \subseteq G$, $e_H \circ e_G = e_H$. Hence, $e_H \circ e_H = e_H \circ e_G$. As $e_H \in G$, it has the inverse e_H^{-1}. Hence, $e_H^{-1} \circ e_H \circ e_H = e_H^{-1} \circ e_H \circ e_G$, and so $e_H = e_G$.
2. Clearly, if H is a subgroup of G, from the definition of a group, one has that for all $a,b \in H$, $a \circ b \in H$ and $a^{-1} \in H$. Now suppose that for all $a,b \in H$, $a \circ b \in H$ and $a^{-1} \in H$. Since $H \neq \emptyset$, there exists $x \in H$. Then $x^{-1} \in H$ and $x \circ x^{-1} = x^{-1} \circ x = e_G \in H$. Now the identity axiom holds in H as H is closed under $\circ$. Finally associativity holds in H as it holds in G and H is a subset of G closed under $\circ$.

Exercise 13: Let G be a group and let H be a nonempty subset of G.

1. Assume that H is non-empty, finite and stable under the group law of G. Prove that H is a subgroup of G.
2. What happens if H is not assumed to be finite anymore?

Solution to Exercise 13 :

1. Take an element $h \in H \setminus \{e_G\}$. Observe that the set $\{h^n | n \geq 0\}$ is contained in H and hence is finite. We can therefore find $m > n \geq 0$ such that $h^m = h^n$. This implies that $h^{-1} = h^{m-n-1} \in H$. Hence, $e_G = hh^{-1} \in H$.
2. The conclusion does not hold anymore : for instance, take $G = \mathbb{Z}$ and $H = \mathbb{N}$.

Exercise 14: In each of the following cases, decide whether H is a subgroup of G.

1. $G = \mathbb{Z}$, $H = \{\text{odd integers}\}$.
2. $G = GL_n(\mathbb{R})$, $H = \{\text{invertible upper triangular matrices}\}$.
3. $G = \mathbb{R}^\times$, $H = \{a + b\sqrt{5} \,|\, (a,b) \in \mathbb{Q}^2 \setminus \{(0,0)\}\}$.

Solution to Exercise 14 :

1. No, because H is not stable under addition.
2. Yes, $I_n \in H$, a product of two invertible upper triangular matrices is an invertible upper triangular matrix and the inverse of an invertible upper triangular matrix is an invertible upper triangular matrix.

3. Yes, because if a,b,c,d are rational numbers with $(a,b) \neq (0,0)$ and $(c,d) \neq (0,0)$, then :

$$(a+b\sqrt{5})(c+d\sqrt{5}) = (ac+5bd)+(ad+bc)\sqrt{5} \in H,$$
$$(a+b\sqrt{5})^{-1} = \frac{a-b\sqrt{5}}{a^2-5b^2} \in H.$$

Exercise 15: Let G be a group and let H and K be two subgroups of G.

1. Prove that $H \cap K$ is a subgroup of G.

2. Prove that $H \cup K$ is a subgroup of G if, and only if, $H \subseteq K$ or $K \subseteq H$.

Solution to Exercise 15 :

1. Check.

2. Assume that $H \cup K$ is a subgroup of G. By contradiction, assume that H is not contained in K and that K is not contained in H. Then one can choose an element h in $H \setminus K$ and an element k in $K \setminus H$. Since $H \cup K$ is a sugbroup, we get that $hk \in H \cup K$. If hk is in H (resp. K), we deduce that $k \in H$ (resp. $h \in K$), a contradiction. Hence $H \subseteq K$ or $K \subseteq H$.

Conversely, if $H \subseteq K$, then $H \cup K = K$ is a subgroup of G, and if $K \subseteq H$, then $H \cup K = H$ is a subgroup of G.