Sheet 3

Due 17.30 Tuesday 30th January

Hand in solutions to questions 1b, 1c, 3c, 3d, 4.

Please write your student ID number on your work and staple it together. Writing your name is optional. Hand in work in the MATH6301 mailbox in the 5th floor common room in the maths department.

1. For each of the following binary operations,

   - is the operation associative?
   - is there an identity element?
   - if there is an identity element then which elements have inverses?
   - is the set together with the operation a group?

   Justify your answers (i.e. give proofs).

   (a) The operation $\times$ on the set $\mathbb{Z}$.
   Solution. Associative, identity is 1, only ± 1 have inverses as $1/0$ does not exist and $1/n \notin \mathbb{Z}$ for $n \neq \pm 1$, not a group as there are elements without inverses

   **(b) The operation $-$ on the set $\mathbb{Z}$. (2 marks)
   Solution. Not associative, if x was identity then $x-1=1$ and $1-x=1$ which is impossible so no identity, no inverses because no identity, not a group as no identity

   **(c) On the set $\mathbb{Z}$, define the operation $\diamond$ by $x \diamond y = x + y - 2$. (2 marks)
   Solution. Associative, identity is 2, inverse of x is $4 - x$, is a group

   (d) The operation $\cup$ on the set $P(\mathbb{N})$.
   Solution. Associative, identity is $\varnothing$, only $\varnothing$ has an inverse, not a group due to lack of inverses

2. Let $n > 1$ be an integer and let G be the set $\{0, 1, \dots, n-1\}$. Define the binary operation $*$ on G by

$$a * b = \begin{cases} a + b & \text{if } a + b < n, \\ a + b - n & \text{otherwise.} \end{cases}$$

   Is this operation associative? Does it have an identity? Do all elements of G have inverses? Is $(G, *)$ a group?

   Solution. Observe that $a * b$ is the remainder when we divide $a + b$ by n, so $*$ is associative. The identity is 0, and the inverse of a is $n - a$ unless $a = 0$ in which case the inverse is 0. This is a group.

3. Which of the following pairs $(G, *)$ are groups? Justify your answer. In the cases where $(G, *)$ is a group, say what the identity element is.

(a) $G = \{x \in \mathbb{R} : x \geq 0\}$, $*$ is the addition of real numbers.

Solution. Not a group, since the positive numbers do not have inverses.

(b) $G = \mathbb{Z}$, $*$ is addition.

Solution. This is a group: addition is associative, the identity is 0 and the inverse of x is $-x$.

**(c) $G = \{x \in \mathbb{R} \setminus \{0\} : x^2 \in \mathbb{Q}\}$, $*$ is multiplication. (2 marks)

Solution. One proof: Must observe that multiplication is associative, 1 is the identity and the inverse of x is $1/x$. Optionally, check that multiplication is a binary operation on G: for any $x, y \in G$ we have $x^2y^2 \in \mathbb{Q}$, since x^2, $y^2 \in \mathbb{Q}$.

Another proof: From section 6.5 of the notes, $G = \{x \in \mathbb{R} \setminus \{0\} : x^2 \in \mathbb{Q}\}$ is a subgroup of $(\mathbb{R} \setminus \{0\}, \times)$. Now need to observe that by the definition of a subgroup, this means that $(G, \times)$ is a group.

**(d) $G = \{\sigma \in S_n : \epsilon(\sigma) = 1\}$, $*$ is composition of permutations. (1 mark)

Solution. This is a group, since the signature of the product of two permutations equals the product of their signatures: $\epsilon(\sigma\tau) = \epsilon(\tau)\epsilon(\sigma)$. The identity is $\mathrm{id} = \mathrm{id}_{\{1,\ldots,n\}}$.

(e) $G = \{\sigma \in S_n : \epsilon(\sigma) = -1\}$, $*$ is composition of permutations

Solution. Not a group. One proof: $*$ is not even a binary operation on G, since $(1\ 2) \in G$ but $(1\ 2) * (1\ 2) = \mathrm{id}_{\{1,\ldots,n\}} \notin G$. (Being very careful one could treat the case $n = 1$ separately; in this case $G = \varnothing$ and a group has to be nonempty.)

Another proof: $1_G(1\ 2) = (1\ 2)$, so the identity 1_G would have to be $\mathrm{id}_{\{1,\ldots,n\}}$, but $\mathrm{id}_{\{1,\ldots,n\}} \notin G$.

(f) Let $k \in \mathbb{N}$ with $k \geq 2$, let $G = \{\sigma \in S_n : \text{the order of } \sigma \text{ is } k\}$, let $*$ be composition of permutations. (Note that the fact that $k \geq 2$ plays a role here.)

Solution. Not a group. For $*$ is not even a binary operation on G, for if $\sigma \in G$ then $\sigma^k = \sigma * \cdots * \sigma = \mathrm{id}_{\{1,\ldots,n\}} \notin G$. (Being very careful one could treat the case $n = 1$ separately; in this case $G = \varnothing$ and a group has to be nonempty.)

Another proof: For any $g \in G$ we have $1_G g = g$ and this implies that 1_G would have to be $\mathrm{id}_{\{1,\ldots,n\}}$, but $\mathrm{id}_{\{1,\ldots,n\}} \notin G$.

(g) Let $n \in \mathbb{N}$ with $n \geq 2$ and let G be the subset of S_n with two elements: $\mathrm{id}_{\{1,\ldots,n\}}$ and the transposition (12), so that $G = \{\mathrm{id}, (1, 2)\}$. Let $*$ be composition of permutations.

Solution. This is a group: composition is associative, the identity is id and $(1\ 2)$ is its own inverse.

Another proof: G is a subgroup of $(S_n, \circ)$, and therefore $(G, \circ)$ is a group.

**4. What is the definition of a subgroup? Let H be the subset of S_6 given by $H = \{\mathrm{id}, p, q, r, s, t\}$, where

$$p = (1\ 2)(3\ 6)(5\ 4), \qquad q = (1\ 3)(2\ 5)(6\ 4), \qquad r = (1\ 4)(2\ 6)(3\ 5),$$
$$s = (1\ 5\ 6)(2\ 3\ 4), \qquad t = (1\ 6\ 5)(2\ 4\ 3).$$

Is H a subgroup of $(S_6, \circ)$? Justify your answer. (3 marks)

Hint: Draw a table

	id	p	q	r	s	t
id						
p						
q						
r						
s						
t						

In each square, work out the composition of the permutation in blue on the left and the permutation in red above.

Solution. If $(G, *)$ is a group then H is a subgroup of $(G, *)$ if $H \subset G$ and $(H, *)$ is a group. Equivalently, $H \subset G$, and for any $g \in H$ and $h \in H$ we have $gh \in H$, and for any $g \in H$ we have $g^{-1} \in H$.

The multiplication table is

	id	p	q	r	s	t
id	id	p	q	r	s	t
p	p	id	t	s	r	q
q	q	s	id	t	p	r
r	r	t	s	id	q	p
s	s	q	r	p	t	id
t	t	r	p	q	id	s

and from this table we can see that for any $g \in H$ and $h \in H$ we have $gh \in H$, and for any $g \in H$ we have $g^{-1} \in H$. So H is a subgroup.