

HOMEWORK 3

- (1) Let $(G, *)$ and (H, \bullet) be groups. Prove that $G \times H$ with the binary operation $(g, h) \cdot (g', h') := (g * g', h \bullet h')$ forms a group.

Proof.

(0) Clearly \cdot is a binary operation which lands in $G \times H$.

(1) $(G \times H, \cdot)$ is associative since for any $(g_1, h_1), (g_2, h_2)$, and $(g_3, h_3) \in G \times H$ we have that

$$\begin{aligned} ((g_1, h_1) \cdot (g_2, h_2)) \cdot (g_3, h_3) &= (g_1 * g_2, h_1 \bullet h_2) \cdot (g_3, h_3) \\ &= ((g_1 * g_2) * g_3, (h_1 \bullet h_2) \bullet h_3) \\ &= (g_1 * (g_2 * g_3), h_1 \bullet (h_2 \bullet h_3)) \quad (\text{since product in } G \text{ and } H \text{ are assoc}) \\ &= (g_1, h_1) \cdot (g_2 * g_3, h_2 \bullet h_3) \\ &= (g_1, h_1) \cdot ((g_2, h_2) \cdot (g_3, h_3)). \end{aligned}$$

(2) We claim that $(e_G, e_H) = e_{G \times H}$ since for all $(g, h) \in G \times H$,

$$(e_G, e_H) \cdot (g, h) = (e_G * g, e_H \bullet h) = (g, h) = (g * e_G, h \bullet e_H) = (g, h) \cdot (e_G, e_H)$$

(3) Let $(g, h) \in G \times H$. Then $(g^{-1}, h^{-1}) \in G \times H$ as well and

$$(g, h) \cdot (g^{-1}, h^{-1}) = (g * g^{-1}, h \bullet h^{-1}) = (e_G, e_H) = e_{G \times H}$$

We have therefore shown that $G \times H$ satisfies all axioms to be a group, and is therefore a group. \square

- (2) Show that the following are equivalent for elements g and h in a group.
- $(g * h)^{-1} = g^{-1} * h^{-1}$
 - $g^2 * h^2 = (g * h)^2$
 - $g * h * g^{-1} * h^{-1} = e$
 - g and h commute.
- (3) Let $f : X \rightarrow Y$ be a function. Show that $\{g \in S_X : f \circ g = f\}$ forms a group under composition (recall that S_X is the set of invertible function of X).

Proof. Let's call the set in question G . We cheat and use the two step subgroup test to show that G is a group (since G is a subset of the group S_X this test applies).

(a) $G \neq \emptyset$ since $Id_X \in G$.

(b) Suppose that $g_1, g_2 \in G$. Then

$$\begin{aligned} f \circ (g_1 \circ g_2) &= (f \circ g_1) \circ g_2 \\ &= f \circ (g_2) && (\text{since } g_1 \in G) \\ &= f && (\text{since } g_2 \in G) \end{aligned}$$

(c) Suppose that $g \in G$. Then

$$\begin{aligned} f &= f \circ Id_X \\ &= f \circ (g \circ g^{-1}) \\ &= (f \circ g) \circ g^{-1} \\ &= f \circ g^{-1} \end{aligned} \quad (\text{since } g \in G)$$

So that $f \circ g^{-1} = f$ and $g^{-1} \in G$. □

(4) Let A be a subset of a set X . Show that $\{g \in S_X : g(A) = A\}$ forms a group under composition. □

Proof. Very similar to the previous proof. □

(5) For any two sets A and B define $A\Delta B$ by $(A \cup B) - (A \cap B)$. Let X be any set and consider the power set $\mathcal{P}(X) := \{A : A \subseteq X\}$. Show that $(\mathcal{P}(X), \Delta)$ forms a group. Is this group abelian? Write down the multiplication table in the special case that $X = \{a, b\}$.

Proof. (0) By definition $A\Delta B$ is a set whenever A and B are.

(1) One could prove associativity by a straight forward set theoretical argument. Here is a slightly slicker proof. For any function $f : X \rightarrow \mathbb{Z}_2$ we define a subset of X , denoted as $V(f)$, as the set of all elements of X which map to 1 under f . Conversely, for any subset A of X define a function which takes the value one on A and 0 on the complement of A . This gives us a one-to-one correspondence between the subsets of X and the functions from X to \mathbb{Z}_2 . Now it's easy to check that if $A = V(f)$ and $B = V(g)$ that $V(f)\Delta V(g) = V(f+g)$. Thus if $C = V(h)$ then $(A\Delta B)\Delta C = V(f+g+h) = A\Delta(B\Delta C)$.

(2) Since for any set $A \subset X$ we have that $A\Delta\emptyset = (A \cup \emptyset) - (A \cap \emptyset) = A - \emptyset = A$ we have that \emptyset is the identity of Δ .

(3) Let $A \subset X$. Then $A\Delta A = A \cup A - A \cap A = A - A = \emptyset$, then inverse of any set under Δ is the set itself. □

(6) Show that the set of matrices of the form

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

(with $a, b, c \in \mathbb{Z}$) forms a group under matrix multiplication called the (or a since one needn't take a, b, c to live in the integers to get a group, one could take $\mathbb{C}, \mathbb{R}, \mathbb{Q}$ or any other so called *ring* as well) Heisenberg group. Is this group abelian?

Proof. We call the set in question H . Since $H \subset \text{GL}(3, \mathbb{R})$, we can again cheat and use the 2 step subgroup test to show that H is a group.

(a) The identity matrix is in H (take $a = b = c = 0$) so that H is not empty.

(b) For any

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

and

$$\begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix}$$

in H we have that

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a+x & y+az+b \\ 0 & 1 & c+z \\ 0 & 0 & 1 \end{pmatrix}$$

which is still in H so that H is closed under matrix multiplication.

(c) For any

$$A := \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}$$

in H ,

$$A^{-1} := \begin{pmatrix} 1 & -a & ac-b \\ 0 & 1 & -c \\ 0 & 0 & 1 \end{pmatrix}$$

which is still in H . □

(7) Let g be an element of a group. Show that $(g^{-1})^{-1} = g$ (**hint** use the uniqueness of inverses).

Proof. Done in previous homework. □

(8) Let G be a group of even order. Show that G contains a non-identity element whose square is the identity.

Proof. Let G^* be the set of non-identity elements of G . Since G has even order G^* has odd order. Define a function from $I : G^* \rightarrow G^*$ which takes every element $g \mapsto g^{-1}$. Since inverses are unique, this is single valued, and by the previous problem, $I \circ I = Id_{G^*}$. As such, the pairs $\{g, I(g)\}$ partition G^* . Since G^* has an odd number of elements, at least one such pair must contain only a single element. That is $g = I(g) = g^{-1}$. □

(9) Show that set of n by n matrices of determinant 1 with integer entries (again entries could lie in any ring) forms a group called the *special linear group* and denoted $SL(n, \mathbb{Z})$ (hint, you may wish to use the fact that $\det(AB) = \det(A)\det(B)$).

Proof. We again cheat and use the 2 step subgroup test (since these matrices are contained inside of the group $GL(n, \mathbb{R})$).

- The set of such matrices are not empty since the identity matrix is in $SL(n, \mathbb{Z})$.

- The formula for matrix multiplication

$$(AB)_{i,k} = \sum_{j=1}^n A_{i,j} B_{j,k}$$

shows closure (since the sum and products of integers are integers).

- For arbitrary matrices $AA^* = \det(A)I$ (where A^* is the adjoint of A) shows that if $\det(A) = 1$, then A^{-1} exists and is equal to A^* . Furthermore, since A^* is obtained from taking determinants of submatrices of A , A^* also has integer entries in the special case that A does. Hence

$$A^{-1} = A^* \in \text{SL}(n, \mathbb{Z}). \quad \square$$