

Solutions to Homework 2

Problem 1. Recall that $P(X)$ denotes the set of all subsets of X (the book denotes it by P_X). Prove that $P(X)$ with the binary operation $\div$ (symmetric difference) is a group (see problem C to chapter 3 in the textbook).

Solution. In homework 1 it was proved that $\div$ is associative, commutative, and has the empty set as the identity. Thus it remains to show that every element in $P(X)$ has the inverse, i.e. that for every subset A of X there is a subset B such that $A \div B = \emptyset$. Note that $B = A$ works:

$$A \div A = (A \cup A) \setminus (A \cap A) = A \setminus A = \emptyset.$$

Thus $P(X)$ is indeed an abelian group and each element in $P(X)$ is its own inverse.

Problem 2. a) Let G be a group with the binary operation $\cdot$, A any set and $f : A \rightarrow G$ a bijection. Define a binary operation $*$ on A as follows:

$$a * b = f^{-1}(f(a) \cdot f(b)).$$

Prove that A with $*$ as binary operation is a group. What is the identity of this group?

b) Apply part a) to the following cases. In each case find an explicit formula for $a * b$ (compare it to problem A in chapter 3 in the textbook).

1. $G = \mathbb{R}$ with addition, $A = \mathbb{R}$, $f(x) = x + k$ (k a fixed real number)
2. $G = \mathbb{R} \setminus \{0\}$ with multiplication, $A = \mathbb{R} \setminus \{0\}$, $f(x) = x/2$.
3. $G = \mathbb{R} \setminus \{0\}$ with multiplication, $A = \mathbb{R} \setminus \{-1\}$, $f(x) = x + 1$.
4. $G = \mathbb{R}$ with addition, $A = (-1, 1)$, $f(x) = \operatorname{arctanh}(x)$ is the inverse function to the hyperbolic tangent $\tanh(x) = (e^x - e^{-x})/(e^x + e^{-x})$. Hint: Prove that

$$\tanh(x + y) = \frac{\tanh(x) + \tanh(y)}{1 + \tanh(x) \tanh(y)}.$$

Solution. a) Note that $f(a * b) = f(a) \cdot f(b)$ for any a, b in A . Thus

$$\begin{aligned} a * (b * c) &= f^{-1}(f(a) \cdot f(b * c)) = f^{-1}(f(a) \cdot (f(b) \cdot f(c))) = \\ &= f^{-1}((f(a) \cdot f(b)) \cdot f(c)) = f^{-1}(f(a * b) \cdot f(c)) = (a * b) * c. \end{aligned}$$

This shows that $*$ is associative. Let e be the identity of G and let $u = f^{-1}(e)$. We claim that u is the identity for $*$:

$$\begin{aligned} u * a &= f^{-1}(f(u) \cdot f(a)) = f^{-1}(e \cdot f(a)) = f^{-1}(f(a)) = a, \\ a * u &= f^{-1}(f(a) \cdot f(u)) = f^{-1}(f(a) \cdot e) = f^{-1}(f(a)) = a. \end{aligned}$$

Let $a \in A$. Then $f(a)$ is in G so it has the inverse $f(a)^{-1}$ in G . Define $b = f^{-1}(f(a)^{-1})$. We claim that $a * b = u = b * a$, so b is the inverse of a in A :

$$a * b = f^{-1}(f(a) \cdot f(b)) = f^{-1}(f(a) \cdot f(a)^{-1}) = f^{-1}(e) = u$$

and similar computation yields $b * a = u$. This completes our verification that A with the binary operation $*$ is a group.

b) 1. We have $f^{-1}(x) = x - k$. Thus

$$a * b = ((a + k) + (b + k)) - k = a + b + k.$$

$-k$ is the identity in this group.

2. We have $f^{-1}(x) = 2x$. Thus

$$a * b = 2((a/2)(b/2)) = ab/2.$$

2 is the identity.

3. We have $f^{-1}(x) = x - 1$. Thus

$$a * b = (a + 1)(b + 1) - 1 = ab + a + b.$$

0 is the identity.

4. We have $f^{-1}(x) = \tanh x$. Let $s = \operatorname{arctanh}(a)$ and $t = \operatorname{arctanh}(b)$. Then

$$a * b = \tanh(s + t) = \frac{\tanh(s) + \tanh(t)}{1 + \tanh(s)\tanh(t)} = \frac{a + b}{1 + ab}.$$

$\tanh(0) = 0$ is the identity.

Problem 3. Let a, b be real numbers, $a \neq 0$. Define the function $T_{a,b} : \mathbb{R} \rightarrow \mathbb{R}$ by $T_{a,b}(x) = ax + b$. Let G be the set of all such functions, i.e.

$$G = \{T_{a,b} : a, b \in \mathbb{R}, a \neq 0\}.$$

a) Prove that G with composition of functions as the binary operation is a group.

b) Suppose that $z \neq 0$. Show that $T_{a,b}$ and $T_{1,z}$ commute iff $a = 1$.

Solution: a) First we need to check that G is closed under composition. We have

$$(T_{a,b} * T_{c,d})(x) = T_{a,b}(cx + d) = a(cx + d) + b = acx + ad + b = T_{ac,ad+b}(x)$$

so

$$T_{a,b} * T_{c,d} = T_{ac,ad+b}. \quad (1)$$

Thus G is closed under composition. Composition of functions is an associative operation so the associativity axiom is satisfied automatically. According to (1), we have $T_{a,b} * T_{1,0} = T_{a,b} = T_{1,0} * T_{a,b}$ so $e = T_{1,0}$. Finally, given $T_{a,b}$ we look for $T_{x,y}$ such that $T_{x,y} * T_{a,b} = e = T_{1,0}$. By (1), $T_{x,y} * T_{a,b} = T_{xa,ab+y}$ so we want $xa = 1$ and $xb + y = 0$, i.e. $x = a^{-1}$ and $y = -a^{-1}b$. Thus $T_{a^{-1},-a^{-1}b}$ is the inverse of $T_{a,b}$. This completes our proof that G is a group.

b) By (1), $T_{a,b} * T_{1,z} = T_{a,az+b}$ and $T_{1,z} * T_{a,b} = T_{a,b+z}$. Thus $T_{a,b}$ and $T_{1,z}$ commute iff $az + b = b + z$, i.e. $(a - 1)z = 0$. Since $z \neq 0$, the last condition is equivalent to $a = 1$.

Problem 4. Let G be a group such that $g^2 = e$ for every $g \in G$. Prove that G is abelian.

Solution: Let $g, h \in G$. We have

$$e = (g * h)^2 = (g * h) * (g * h) = g * (h * g) * h.$$

We also have

$$e = g^2 * h^2 = (g * g) * (h * h) = g * (g * h) * h.$$

Thus

$$g * (h * g) * h = g * (g * h) * h$$

and by cancelling g on the left and h on the right we arrive at $h * g = g * h$. This shows that G is abelian.

Problem 5. Let G be the set of all bijections $f : \mathbb{Z} \rightarrow \mathbb{Z}$ which preserve distance, i.e. such that $|f(i) - f(j)| = |i - j|$ for all integers i, j .

a) Show that G is a subgroup of $S_{\mathbb{Z}}$. It is called the **infinite dihedral group** and it is often denoted by D_{∞} .

b) The group G contains elements T, S such that $T(a) = a + 1$ and $S(a) = -a$ for all integers a . Prove that $S * T = T^{-1} * S$. Show that the subgroup $\langle T \rangle$ is infinite. What is $\langle S \rangle$?

c) Show that if $F \in G$ and $F(0) = 0$ then either $F = 1$ (the identity) or $F = S$.

d) Show that every element of G is of the form T^i or ST^i for a unique integer i .

e) Suppose that $T^5 S^7 T^3 = S^a T^b$. Find a and b .

Solution: a) Let $f, g \in G$ and $i, j \in \mathbb{Z}$. Then

$$|(f * g)(i) - (f * g)(j)| = |f(g(i)) - f(g(j))| = |g(i) - g(j)| = |i - j|$$

so $f * g \in G$. Also,

$$|i - j| = |f(f^{-1}(i)) - f(f^{-1}(j))| = |f^{-1}(i) - f^{-1}(j)|$$

so $f^{-1} \in G$. Clearly the identity I is in G , so G is a subgroup of $S_{\mathbb{Z}}$.

b) Note that $T^{-1}(a) = a - 1$ for all $a \in \mathbb{Z}$. Thus

$$(S * T)(a) = S(T(a)) = S(a + 1) = -(a + 1) = -a - 1$$

and

$$(T^{-1} * S)(a) = T^{-1}(S(a)) = T^{-1}(-a) = -a - 1$$

for all $a \in \mathbb{Z}$. It follows that $S * T = T^{-1} * S$.

Observe now that for any integer m we have $T^m(0) = m$. It follows that if $m \neq n$ then $T^m \neq T^n$ so $\langle T \rangle$ is infinite. Since $S^2 = I$, we have $\langle S \rangle = \{I, S\}$.

c) Since $|F(1)| = |F(0) - F(1)| = |0 - 1| = 1$, we have $F(1) = 1$ or $F(1) = -1$.

Suppose first that $F(1) = 1$. Let $n > 0$. Note that n is the only integer whose distance from 0 is n and whose distance from 1 is $n - 1$. But $|F(n) - 0| = |F(n) - F(0)| = |n - 0| = n$ and $|F(n) - 1| = |F(n) - F(1)| = |n - 1| = n - 1$. It follows that $F(n) = n$ for all positive integers n . Similarly, if $n < 0$, then n is the only integer whose distance from 0 is $|n|$ and whose distance from 1 is $|n| + 1$. Since $|F(n) - 0| = |F(n) - F(0)| = |n - 0| = |n|$ and

$|F(n) - 1| = |F(n) - F(1)| = |n - 1| = |n| + 1$, we see that $F(n) = n$. This proves that $F = I$.

Suppose now that $F(1) = -1$. Then $(S * F)(0) = S(F(0)) = S(0) = 0$ and $(S * F)(1) = S(F(1)) = S(-1) = 1$. We just showed that this implies the equality $SF = I$, i.e. $F = S^{-1} = S$.

d) Let $G(0) = i$. Note that $T^i(0) = i$. Thus $(T^{-i} * G)(0) = 0$. By part c), we have either $T^{-i} * F = I$ or $T^{-1} * F = S$. In the former case, $F = T^i$ and in the latter case $F = T^i * S = S * T^{-i}$.

e) Note that $S^7 = S$ and $T^m * S = S * T^{-m}$ for any integer m . Thus

$$T^5 * S^7 * T^3 = T^5 * S * T^3 = S * T^{-5} * T^3 = S * T^{-2}.$$

Problem 6. In the group $GL_2(\mathbb{C})$ of all invertible 2×2 matrices with entries in complex numbers consider the matrices $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $i = \begin{pmatrix} \sqrt{-1} & 0 \\ 0 & -\sqrt{-1} \end{pmatrix}$, $j = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, $k = ij = \begin{pmatrix} 0 & \sqrt{-1} \\ \sqrt{-1} & 0 \end{pmatrix}$. Let Q_8 be the set $\{I, -I, i, -i, j, -j, k, -k\}$.

a) Show that Q_8 is a subgroup of $GL_2(\mathbb{C})$. Write the table of multiplication in Q_8 . Q_8 is called the **quaternion group**.

b) List all subgroups of Q_8 .

Solution: a) Note that:

- $I \cdot a = a \cdot I = a$ for all $a \in Q_8$ (i.e. I is the identity in Q_8);
- $(-I)a = a(-I) = -a$ for all $a \in Q_8$;
- $ii = (-i)(-i) = jj = (-j)(-j) = kk = (-k)(-k) = -I$;
- $ij = (-i)(-j) = (-j)i = j(-i) = k$; $ji = (-j)(-i) = (-i)j = i(-j) = -k$;
- $jk = (-j)(-k) = (-k)j = k(-j) = i$; $kj = (-k)(-j) = (-j)k = j(-k) = -i$;
- $ki = (-k)(-i) = (-i)k = i(-k) = j$; $ik = (-i)(-k) = (-k)i = k(-i) = -j$;
- $i^{-1} = -i$, $j^{-1} = -j$, $k^{-1} = -k$.

This shows that Q_8 is closed under multiplication and inverses, so it is a subgroup of $GL_2(\mathbb{C})$. Here is the table of multiplication.

*	I	$-I$	i	$-i$	j	$-j$	k	$-k$
I	I	$-I$	i	$-i$	j	$-j$	k	$-k$
$-I$	$-I$	I	$-i$	i	$-j$	j	$-k$	k
i	i	$-i$	$-I$	I	k	$-k$	$-j$	j
$-i$	$-i$	i	I	$-I$	$-k$	k	j	$-j$
j	j	$-j$	$-k$	k	$-I$	I	i	$-i$
$-j$	$-j$	j	k	$-k$	I	$-I$	$-i$	i
k	k	$-k$	j	$-j$	$-i$	i	$-I$	I
$-k$	$-k$	k	$-j$	j	i	$-i$	I	$-I$

b) The subgroups of Q_8 are: $\langle I \rangle = \{I\}$, $\langle -I \rangle = \{-I, I\}$, $\langle i \rangle = \{I, i, -I, -i\}$, $\langle j \rangle = \{I, j, -I, -j\}$, $\langle k \rangle = \{I, k, -I, -k\}$ and Q_8 . In particular, every proper subgroup of Q_8 is cyclic.