Solutions of exercise sheet 1

1. Let $(G, \cdot)$ be a group. We say that G is *abelian* if $\forall x, y \in G$, $x \cdot y = y \cdot x$. For $g \in G$ we define the *order* of g, which we denote $\mathrm{ord}_G(g)$, as the minimal positive integer n such that $g^n = 1_G$, if such n exists. Else we say that g has infinite order. Prove the following statements for a group G:

1. If $e \in G$ is s.t. $\forall x \in G$, $e \cdot x = x$, then $e = 1_G$.
2. G is abelian if and only if the inversion map $G \to G$, $x \mapsto x^{-1}$ is a group homomorphism.
3. If $g^2 = 1_G$ for every $g \in G$, then G is abelian.
4. If $g \in G$ has finite order, g^{-1} is a power of g.
5. If G is finite, every $g \in G$ has finite order.

Solution:

1. Suppose that for all $x \in G$ we have $e \cdot x = x$. Applying this for $x = 1_G$ we get $e = e \cdot 1_G = 1_G$.
2. We have that G is abelian if and only if $xy = yx$ for all $x, y \in G$, if and only if $xyx^{-1}y^{-1} = 1_G$ for all $x, y \in G$, if and only if $x^{-1}y^{-1} = y^{-1}x^{-1}$ for all $x, y \in G$. Being $(xy)^{-1} = y^{-1}x^{-1}$, the last statement is equivalent to saying that $x^{-1}y^{-1} = (xy)^{-1}$ for all $x, y \in G$, that is, that the inversion respects multiplication. Hence G is abelian if and only if the inversion map is a group homomorphism.
3. $g^2 = 1_G$ means $g = g^{-1}$, and this situation occurs for all $g \in G$ if and only if the inversion coincides with the identity, in which case it is a group homomorphism and by previous point G is abelian.
4. If $g \in G$ has finite order, then there exists $n > 0$ such that $g^n = 1_G$. Then $g^{n-1}g = 1_G$, so that $g^{n-1} = g^{-1}$ and the inverse of g is a power of g.
5. Let $g \in G$ and consider the map $\beta_g : \mathbb{N} \to G$ sending $n \mapsto g^n$. If G is finite, then β_g cannot be injective. Hence there exists two natural numbers $m < n$ such that $g^m = g^n$. Multiplying by g^{-m} gives $g^{n-m} = 1$, and being $n - m > 0$ we get that g has finite order.

2. We will here consider *monoids*, which are defined in the same way as groups, but without inversion map. More precisely, a *monoid* consists of a set S together with a map $- \cdot - : G \times G \to G$ and a distinguished element $1_S \in S$ satisfying the following axioms:

Please turn over!

- $\forall x, y, z \in S$, $(x \cdot y) \cdot z = x \cdot (y \cdot z)$
- $\forall x \in S$, $1_S \cdot x = x \cdot 1_S = x$

We say that $y \in S$ is a *left* (resp., *right*) *inverse* of $x \in S$ if $y \cdot x = 1_S$ (resp., $x \cdot y = 1_S$).

Let X be a non-empty set and consider the set of functions $\mathrm{End}(X) = \{f : X \to X\}$.

1. Prove that $\mathrm{End}(X)$, together with the composition of functions $\circ$, is a monoid for every set X.
2. Prove that $f \in \mathrm{End}(X)$ has a left (resp., right) inverse if and only if f is injective (resp., surjective).
3. For which sets X does there exist $f \in \mathrm{End}(X)$ which has a left inverse but no right inverse?

[You can use this formulation of the axiom of choice: Let $\{X_i\}_{i \in I}$ be a family of non-empty sets indexed by $I \neq \varnothing$. Then there exists a family $\{x_i\}_{i \in I}$ such that $x_i \in X_i$]

Solution:

1. It is easy to check associativity by assuming $f, g, h \in \mathrm{End}(X)$ and comparing the functions $(f \circ g) \circ h$ and $f \circ (g \circ h)$ on each element $x \in X$. Both of them map indeed $x \mapsto f(g(h(x)))$. Hence they are the same function. Moreover, it is clear that composing a function f with the identity $\mathrm{id}_X : x \mapsto x$ we get again f, so that $\mathrm{id}_X = 1_{\mathrm{End}(X)}$.
2. Suppose $f \in \mathrm{End}(X)$ has a left inverse $g : X \to X$, i.e. $g \circ f = \mathrm{id}_X$. Then if $f(x) = f(y)$ for $x, y \in X$, we get $x = g(f(x)) = g(f(y)) = y$, proving injectivity of f. Now suppose that f has a right inverse $h : X \to X$, i.e. $f \circ h = \mathrm{id}_X$. Then for each $x \in X$, we have that $x = f(h(x))$, proving surjectivity of f. So we have proved the "only if" part, and we are left to construct left and right inverses.

   If $f : X \to X$ is injective, then we can can pick $x_0 \in X$ and define a function $g : X \to X$ sending $f(x) \mapsto x$ and $X \setminus f(X) \ni y \mapsto x_0$. This is a well-defined action by injectivity of f, and for all $x \in X$ we have $g(f(x)) = x$ by definition, so that g is a left inverse of g.

   If $f : X \to X$ is surjective, we can use axiom of choice (as stated in the exercise), with $I := X \neq \varnothing$ and $X_y = f^{-1}(y) \neq \varnothing$. Considering the resulting family $\{x_y\}_{y \in X}$ we can define $h : X \to X$ via $h(y) = x_y$. Then we obtain, $\forall y \in X$, $f(h(y)) = f(x_y) = y$, meaning that h is a right inverse of f.
3. The situation in which there is a function with left inverse but without any right inverse occurs precisely when X is infinite. Via the axiom of choice, one can prove that a set X is infinite if it is Dedekind infinite, that is, there exists a proper subset X' such that $|X| = |X'|$, say via $\phi : X \to X'$. Then ϕ can also be seen as a map $X \to X$, which by construction happens to be injective but not surjective. On the other hand, an injective map $f : X \to X$ gives a one-to-one correspondence $X \leftrightarrow \mathrm{Im}(f)$, and if f is not surjective $\mathrm{Im}(f)$ is a proper subset of X, which needs to be infinite.

See next page!

3. Show that there are precisely two non-isomorphic groups of order 4, and construct their multiplication table.

Solution:

We consider a group G with 4 distinct elements $1, a, b$ and c. Then $a \cdot b \in G$ can only be equal to 1 or c ($ab = a$ gives $b = 1$, and $ab = b$ gives $a = 1$). So we can start writing down two different tables of multiplication:

$$(A)\ \begin{array}{c|cccc} \cdot & 1 & a & b & c \\ \hline 1 & 1 & a & b & c \\ a & a & 1 & & \\ b & b & & & \\ c & c & & & \end{array} \qquad \text{and} \qquad (B)\ \begin{array}{c|cccc} \cdot & 1 & a & b & c \\ \hline 1 & 1 & a & b & c \\ a & a & c & & \\ b & b & & & \\ c & c & & & \end{array}$$

Cancellation law implies that, similarly as in a Sudoku, in a single row or column we cannot get twice the same element. Using this rule on both tables and completing them in all possible ways we obtain

$$(A_1)\ \begin{array}{c|cccc} \cdot & 1 & a & b & c \\ \hline 1 & 1 & a & b & c \\ a & a & 1 & c & b \\ b & b & c & 1 & a \\ c & c & b & a & 1 \end{array} \qquad (A_2)\ \begin{array}{c|cccc} \cdot & 1 & a & b & c \\ \hline 1 & 1 & a & b & c \\ a & a & 1 & c & b \\ b & b & c & a & 1 \\ c & c & b & 1 & a \end{array} \qquad \text{and} \qquad (B)\ \begin{array}{c|cccc} \cdot & 1 & a & b & c \\ \hline 1 & 1 & a & b & c \\ a & a & c & 1 & b \\ b & b & 1 & c & a \\ c & c & b & a & 1 \end{array}$$

But the tables (A_2) and (B) are the same up to renaming $a \mapsto c$ and $c \mapsto a$, while (A_1) is the only one where all elements have order ≤ 2. In conclusion we have two non-isomorphic groups of order 4.

4. Consider the set $\mathbb{Z} \times \mathbb{Z}$ together with the binary operation $*$ defined by

$$(a, h) * (b, k) = (a + (-1)^h b, h + k)$$

1. Show that $(\mathbb{Z} \times \mathbb{Z}, *)$ is a group and that it is not abelian.
2. Find all elements having finite order.
3. Consider the projection maps $\pi_1, \pi_2 : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ defined by $\pi_1((m, n)) = m$ and $\pi_2((m, n)) = n$. Determine if they are morphism of groups $(\mathbb{Z} \times \mathbb{Z}, *) \to (\mathbb{Z}, +)$.

Solution:

1. Let us first prove that $(\mathbb{Z} \times \mathbb{Z}, *)$ is a group:
   - **Associativity.** It is easy to check that $((a, h) * (b, k)) * (c, l) = (a, h) * ((b, k) * (c, l)) = (a + (-1)^h b + (-1)^{h+k} c, h + k + l)$, for all $a, b, c, h, k, l \in \mathbb{Z}$.
   - **Neutral element.** Solving $(e, i) * (a, h) = (a, h)$ (for all $a, h \in \mathbb{Z}$) gives $e = i = 0$. Since we have $(a, h) * (0, 0) = (a, h)$, we get $1_G = (0, 0)$.

Please turn over!

- **Inverse element.** Solving $(a,h)*(b,k) = (0,0)$ gives conditions $k=-h$ and $b=-(-1)^h a$. Such condition guarantees (b,k) to be a left inverse as well:

$$(-(-1)^h a, -h)*(a,h) = (-(-1)^h a + (-1)^{-h} a, 0) = 0$$

since h and $-h$ have the same parity.

The fact that the group is not abelian can be checked considering $(0,1)*(1,0) = (-1,1) \neq (1,1) = (1,0)*(0,1)$.

2. We denote any n-repeated multiplication by $*$ as an n-th power. With an easy induction one can show that the second entry of $(a,h)^n$ is nh, which can be zero for $n>0$ only if $h=0$. Hence elements of finite order are of the form $(a,0)$. But the same easy induction gives $(a,0)^n = (na,0)$, which is zero for positive n only if $a=0$. Hence 1_G is the only element of finite order.
3. We see that π_1 fails to be a morphism of groups:

$$\pi_1((0,1)*(1,0)) = \pi_1((-1,1)) = -1 \neq 0+1 = \pi_1((0,1)) + \pi_1((1,0))$$

On the other hand, π_2 is a morphism of groups $(\mathbb{Z}\times\mathbb{Z}, *) \to (\mathbb{Z}, +)$ since for all $a,b,h,k \in \mathbb{Z}$ we have the equality:

$$\pi_2((a,h)*(b,k)) = \pi_2((a+(-1)^h b, h+k)) = h+k = \pi_2((a,h)) + \pi_2((b,k))$$

5. (*) Fix an integer $n>1$ and consider the symmetric group $S_n := \mathrm{Sym}(\{1,\dots,n\})$. For $p(X_1,\dots,X_n) \in \mathbb{C}[X_1,\dots,X_n]$ and $\sigma \in S_n$, define $p_\sigma = p(X_{\sigma(1)},\dots,X_{\sigma(n)})$. Let $f := \prod_{1\le i<j\le n}(X_i - X_j) \in \mathbb{C}[X_1,\dots,X_n]$.

1. Prove that for every permutation $\sigma \in S_n$, there exists a unique element $\alpha(\sigma) \in \{\pm 1\}$ such that $f_\sigma(X) = \alpha(\sigma) f$.
2. Show that the resulting map

$$\alpha : S_n \to \{\pm 1\}$$

is a group homomorphism.

3. Let $a \neq b$ be elements of $\{1,\dots,n\}$, and consider the permutation $\tau \in S_n$ switching a and b and fixing all the other elements. Show that $\alpha(\tau) = -1$.

Solution (sketch):

1. Since each factor of f can be found once again in f_σ, eventually with a changed signed, we get that f_σ and f are the same up to a sign. This can be formalized in several ways, e.g. defining quantities $a_{ij}(\sigma) := \mathrm{sign}(\sigma(j)-\sigma(i))$, so that

$$X_{\sigma(j)} - X_{\sigma(i)} = a_{ij}(\sigma)(X_{\max(\sigma(i),\sigma(j))} - X_{\min(\sigma(i),\sigma(j))})$$

and comparing the product formulas for f and f_σ.

See next page!

2. We have $\alpha(\sigma) = f_\sigma/f$, and

$$\alpha(\sigma\tau) = \frac{f_{\sigma\tau}}{f} = \frac{f_{\sigma\tau}}{f_\sigma}\frac{f_\sigma}{f} = \frac{f_{\sigma\tau}}{f_\sigma}\alpha(\sigma)$$

so that we are left to prove that $f_{\sigma\tau}/f_\sigma = f_\tau/f$. To prove this, one can first show that the following equalities hold for any $p, q \in \mathbb{C}[X_1, \ldots, X_n]$:

- $p_{\sigma\tau} = (p_\tau)_\sigma$
- $(pq)_\sigma = p_\sigma q_\sigma$

Then

$$\frac{f_{\sigma\tau}}{f_\sigma} = \frac{(f_\tau)_\sigma}{f_\sigma} = \left(\frac{f_\tau}{f}\right)_\sigma = \frac{f_\tau}{f}$$

because $\frac{f_\tau}{f} = \alpha(\tau) \in \{\pm 1\}$ is a polynomial which is fixed by σ.

3. To see that a permutation τ switching two elements a and b and fixing the others has negative value of α it is enough to consider what happens to the sign of the factors $X_i - X_j$ distinguishing some cases. Without loss of generality one can assume that $a < b$:

- The factor $X_a - X_b$ changes sign.
- For $i < a$, the factors $X_i - X_a$ and $X_i - X_b$ are unchanged, and the same occurs to then factors $X_a - X_i$ and $X_b - X_i$ when $b < i$.
- For $a < i < b$, the factors $X_a - X_i$ and $X_i - X_b$ change all sign, but they are in an even quantity (precisely, they are $2(b - a - 1)$.

In total, we have an odd number of sign changes, so that $\alpha(\tau) = -1$.