Solutions of exercise sheet 2

The content of the marked exercise **(*)** should be known for the exam.

1. For each of the following groups G and subsets $H \subseteq G$, decide if H is a subgroup of G (in that case, we write $H \leq G$).

1. $G = \mathrm{SL}_2(\mathbb{R})$ and $H = \left\{ \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} : x \in \mathbb{R} \right\}$.
2. $G = \mathrm{Sym}(\mathbb{N})$ and $H = \{\sigma \in G : \sigma(n) \neq n \text{ for only finitely many } n \in \mathbb{N}\}$.
3. $G = \mathrm{Sym}(\mathbb{N})$ and $H = \{\sigma \in G : \sigma(n) = n \text{ for only finitely many } n \in \mathbb{N}\}$.
4. G is any group and $H = f^{-1}(H')$, where $f : G \to G'$ is a group homomorphism and H' is a subgroup of G'.
5. $G = \mathrm{Sym}(X)$ and $H = \mathrm{Aut}(X)$, for a fixed group X.
6. G is any group and $H = G_{\mathrm{tor}} := \{g \in G : \exists n \in \mathbb{N}^* : g^n = 1\}$. Prove that $H \leq G$ when G is finite or abelian, but this does not occur when $G = \mathrm{Sym}(\mathbb{N})$.

Solution:

1. Yes. G is the multiplicative group consisting of 2×2 matrices with coefficient in $\mathbb{R}$ having determinant 1, so that $H \subseteq G$. Clearly the identity matrix lies in H. For each $x, y \in \mathbb{R}$, we have
$$\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & x+y \\ 0 & 1 \end{pmatrix}$$
so that H is closed under multiplication and contains for all $x \in \mathbb{R}$ the inverse $\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & -x \\ 0 & 1 \end{pmatrix}$. Hence $H \leq G$.
2. Yes. By definition $1 \in H$. For each $\sigma \in \mathrm{Sym}(\mathbb{N})$ let us denote $I_\sigma := \{n \in \mathbb{N} : \sigma(n) \neq n\}$. This means that $\sigma \in H$ if and only if $|I_\sigma| < \infty$. Then for all $\sigma \in S_n$ we have $I_{\sigma^{-1}} = I_\sigma$ since $\sigma^{-1}(x) \neq x$ if and only if $x \neq \sigma(x)$, implying that for $\sigma \in H$ one has $\sigma^{-1} \in H$.
As concerns multiplication, let $\sigma, \tau \in H$. We have that if $n \in (\mathbb{N} \setminus I_\sigma) \cap (\mathbb{N} \setminus I_\tau) = \mathbb{N} \setminus (I_\sigma \cup I_\tau)$, then n is fixed by σ and τ, and of course it is fixed by $\sigma\tau$, namely, $n \in \mathbb{N} \setminus I_{\sigma\tau}$. Hence $\mathbb{N} \setminus (I_\sigma \cup I_\tau) \subseteq \mathbb{N} \setminus I_{\sigma\tau}$ implying that $I_\sigma \cup I_\tau \supseteq I_{\sigma\tau}$. Then $I_{\sigma\tau}$ happens to be finite, so that $\sigma\tau \in H$.
3. No, because $1_G = \mathrm{id}_{\mathbb{N}} \notin H$.

4. Yes. This is immediately proved by saying that for $x, y \in H$ one has $f(1_G) = 1_{G'}$, $f(xy) = f(x)f(y)$ and $f(x^{-1}) = f(x)^{-1}$, and those three elements lie all in H' precisely because H' is a subgroup of G'. Then 1_G, xy and x^{-1} lie all in $H = f^{-1}(H')$.
5. Yes. First, notice that id_X is a group automorphism of X. Composition of automorphisms is an automorphism: for all $x, y \in X$ and $f, g \in \mathrm{Aut}(X)$ we have $(f \circ g)(x \cdot y) = f(g(x) \cdot g(y)) = (f \circ g)(x) \cdot (f \circ g)(y))$. Finally, for $g = f^{-1} \in \mathrm{Aut}(X)$ we have $f(g(x)g(y)) = f(g(x))f(g(y)) = xy$, so that by bijectivity $g(xy) = g(x)g(y)$ and g is an automorphism of groups.
6. If G is finite, $G_{\text{tor}} = G$ by Exercise 1.5 from last exercise sheet, and of course it is a subgroup of G.

   If G is abelian, for all $x, y \in G_{\text{tor}}$ we have positive integer m, n such that $g^m = h^n = 1_G$. Then applying induction and using commutativity we get $(gh)^{mn} = g^{mn}h^{mn} = (g^m)^n(h^n)^m = 1_G$, so that $gh \in G_{\text{tor}}$. Clearly $1_G \in G_{tor}$. If $g^n = 1$ for $g \in G$ and $n > 0$, then applying induction we get $(g^{-1})^n = (g^n)^{-1} = 1_G^{-1} = 1_G$. Hence $G_{\text{tor}} \leq G$ when G is abelian.

   If $G = \mathrm{Sym}(\mathbb{N})$, then G_{tor} is not a subgroup. We assume here that $0 \in \mathbb{N}$. For example, consider the permutation $\sigma, \tau \in \mathrm{Sym}(\mathbb{N})$ defined by

$$\sigma(k) = \begin{cases} k+1 & \text{for } k \text{ even} \\ k-1 & \text{for } k \text{ odd} \end{cases} \qquad \tau(k) = \begin{cases} 0 & \text{for } k = 0 \\ k+1 & \text{for } k \text{ odd} \\ k-1 & \text{for } k > 0 \text{ even} \end{cases}$$

   Then it can be easily checked that $\sigma^2 = \tau^2 = \mathrm{id}_{\mathbb{N}}$, so that $\sigma, \tau \in G_{\text{tor}}$. On the other hand, for k an even natural number, we have $(\sigma\tau)(k) = \sigma(k+1) = k+2$, which is again even, so that an easy induction gives $(\sigma\tau)^n(k) = k + 2n$ for every $n > 0$, which is never equal to k, so that $(\sigma\tau)^n \neq \mathrm{id}_{\mathbb{N}}$ for every positive integer n, and $\sigma\tau \notin G_{tor}$.

2. Prove that the following maps are homomorphisms of groups. Find their kernel and image.

1. The absolute value $|\cdot| : \mathbb{C}^\times \to \mathbb{R}^\times$, where $|x + iy| = \sqrt{x^2 + y^2}$ for $x, y \in \mathbb{R}$.
2. $f : \mathbb{R} \to \mathbb{C}^\times$, defined by $f(x) = e^{ix}$.
3. $g : \mathbb{R} \to \mathrm{GL}_2(\mathbb{R})$, defined by $g(t) = \begin{pmatrix} \cosh(t) & \sinh(t) \\ \sinh(t) & \cosh(t) \end{pmatrix}$.

Solution:

1. Given two complex numbers $z = a + ib$ and $w = c + id$, we have

$$\begin{aligned} |zw| &= |(ac - bd) + i(ad + bc)| = \sqrt{(ac - bd)^2 + (ad + bc)^2} \\ &= \sqrt{a^2c^2 + b^2d^2 + a^2d^2 + b^2c^2} = \sqrt{(a^2 + b^2)(c^2 + d^2)} = |z| \cdot |w| \end{aligned}$$

See next page!

so that the absolute value is a homomorphism of groups. Let us know compute kernel and image of the absolute value.

$$\ker(|\cdot|) = \{z \in \mathbb{C} : |z| = 1\}$$

It is the unit circle in the complex plane, which can also be written down as $\{x+iy \in \mathbb{C} : x^2+y^2 = 1\}$. As concerns the image, we claim that $\mathrm{Im}(f) = R^+$. For $r \in R^+$ we have $|r| = \sqrt{r^2} = r$, so that $R^+ \subseteq \mathrm{Im}(f)$. By definition $\mathrm{Im}(f) \subseteq R_{\geq 0}$ and since the only solution of the 2-variable equation $\sqrt{a^2+b^2} = 0$ is $a = b = 0$, we have that $\mathrm{Im}(f) \subseteq R^+$.

2. $e^{i(x+y)} = e^{ix}e^{iy}$ as property of the complex exponential, so that f is a group homomorphism. We have that $e^{ix} = \cos(x) + i\sin(x)$ is 1 if and only if $x \in 2\pi\mathbb{Z}$, so that $\ker(f) = 2\pi\mathbb{Z}$. As concerns the image, notice that $e^{ix} = \cos(x) + i\sin(x)$, $x \in \mathbb{R}$ is a parametrization of the unit circle of the complex plane: $|e^{ix}| = \sqrt{\cos(x)^2 + \sin(x)^2} = 1$ for every x, and for each couple of real numbers $(a, b) \in \mathbb{R}^2$ s.t. $a^2 + b^2 = 1$ there exists a real number x such that $\cos(x) = a$ and $\sin(x) = b$.
3. Considering the entries of a matrix $g(s)g(t)$ for real s and t, we need to compute

$$\cosh(s)\cosh(t) + \sinh(s)\sinh(t) = \frac{(e^s + e^{-s})(e^t + e^{-t})}{4} + \frac{(e^s - e^{-s})(e^t - e^{-t})}{4} = \\ = \frac{e^{s+t} + e^{-s-t}}{2} = \cosh(s+t)$$

and

$$\cosh(s)\sinh(t) + \sinh(s)\cosh(t) = \frac{(e^s + e^{-s})(e^t - e^{-t})}{4} + \frac{(e^s - e^{-s})(e^t + e^{-t})}{4} = \\ = \frac{e^{s+t} - e^{-s-t}}{2} = \sinh(s+t)$$

so that

$$g(s)g(t) = \begin{pmatrix} \cosh(s) & \sinh(s) \\ \sinh(s) & \cosh(s) \end{pmatrix} \begin{pmatrix} \cosh(t) & \sinh(t) \\ \sinh(t) & \cosh(t) \end{pmatrix} = \\ = \begin{pmatrix} \cosh(s+t) & \sinh(s+t) \\ \sinh(s+t) & \cosh(s+t) \end{pmatrix} = g(s+t)$$

and g is a group homomorphism.
Now let us compute the kernel of g. We have

$$\ker(g) = \{s \in \mathbb{R} : \cosh(s) = 1, \sinh(s) = 0\} = \{0\}$$

because $\sinh(s) = 0$ is equivalent to $e^x = e^{-x}$, i.e. $x = 0$ (being $x \in \mathbb{R}$). Hence the map g is injective, and $\mathbb{R} \cong \mathrm{Im}(g)$. It can be easily shown that

$$\mathrm{Im}(g) = \left\{ \begin{pmatrix} x & y \\ y & x \end{pmatrix} : x^2 - y^2 = 1, x > 0 \right\} \leq \{A \in SL_2(\mathbb{R}) | A^T = A\}$$

3. Let G be a group and assume that $S \subset G$ is a generating subset for G, i.e. $G = \langle S \rangle$.

1. Assume that $f, g : G \to H$ are two group homomorphisms and that $f(s) = g(s)$ for all $s \in S$. Prove: $f = g$.
2. Assume that $\forall s, t \in S$ we have $st = ts$. Prove that G is abelian.
3. If $s^2 = 1$ for all $s \in S$, does it follow that $x^2 = 1_G$ for all $g \in G$?

Solution: NB. The subgroup $\langle S \rangle \leq G$ generated by S can be equivalently defined as the subset $H = \{s_1 \cdot \cdots \cdot s_m \in G : \forall i \in I, s_i \in S \text{ or } s_i^{-1} \in S\}$ or as the intersection $K = \bigcap_{S \subseteq L \leq G} L$. The two definitions coincide. Indeed, both H and K are easily shown to be subgroups. S is a subset of H by definition, so that by construction $K \leq H$, since H need to appear as one of the L's in the intersection defining K. But $S \subseteq K$ by definition, and being K closed under multiplication and taking inverses, it has to contain all the elements in H, giving $H \leq K$. Hence $H = K$.

1. Let $x \in G$. Being G generated by S, there are some elements $s_1, \ldots, s_m \in S$ and signs $\varepsilon_1, \ldots, \varepsilon \in \{\pm 1\}$ such that $x = s_1^{\varepsilon_1} \cdots s_n^{\varepsilon_n}$. Then comparing $f(x) = g(x)$, by writing down x as the product above and using that f and g respect products and taking inverses. Being x arbitrary, we have $f = g$.
2. We can use an argument which is very similar to the one in the previous point. Writing down arbitrary x and y as products of elements in S and inverses of elements in S, commuting x and y becomes possible after proving that also couples of elements (s, t^{-1}) and (s^{-1}, t^{-1}), where $s, t \in S$, do commute. For couples of elements (s, t^{-1}) we have $t(st^{-1}) = (ts)t^{-1} = stt^{-1} = s$, and this equality gives $t^{-1}s = st^{-1}$. For couples of elements (s^{-1}, t^{-1}) we have $s^{-1}t^{-1} = (ts)^{-1} = (st)^{-1} = t^{-1}s^{-1}$. This completes the proof.
3. The answer is negative. You can consider $G = \langle \sigma, \tau \rangle \leq \mathrm{Sym}(\mathbb{N})$, with σ and τ defined as in the Solution of Exercise 6.1 of this Exercise sheet. Clearly, $\sigma^2 = \tau^2 = 1_G \neq (\sigma\tau)^2$.

4. Consider the real *Möbius transformations*, that is, the following set of rational functions with coefficients in $\mathbb{R}$:

$$G = \left\{ f(X) = \frac{aX + b}{cX + d} : \ a, b, c, d \in \mathbb{R}, ad - bc \neq 0 \right\},$$

together with the composition of functions $\circ$.

1. Prove that $(G, \circ)$ is a group.
2. Find a subgroup H of G such that $(H, \circ) \cong (\mathbb{R}, +)$ as groups.
3. Consider the map

$$\alpha : \mathrm{GL}_2(\mathbb{R}) \to G$$
$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \frac{aX + b}{cX + d}$$

Prove that α is a group homomorphism. Determine its kernel and its image.

4. Determine all Möbius transformations of order 1 and 2 (they are also called *involutions*).

1. First, we need to show that the composition of two Möbius functions is still a Möbius function. For $i = 1, 2$, let $f_i = (a_i X + b_i)/(c_i X + d_i)$, with $a_i d_i - b_i c_i \neq 0$. Then

$$f_1 \circ f_2 = \frac{a_1 \frac{a_2 X + b_2}{c_2 X + d_2} + b_1}{c_1 \frac{a_2 X + b_2}{c_2 X + d_2} + d_1} = \frac{(a_1 a_2 + b_1 c_2)X + (a_1 b_2 + b_1 d_2)}{(c_1 a_2 + d_1 c_2)X + (c_1 b_2 + d_1 d_2)}$$

as point (3) suggests, the four coefficients of $f_1 \circ f_2$ are precisely the ones of the matrix $A_1 \cdot A_2$, where $A_i = \begin{pmatrix} a_i & b_i \\ c_i & d_i \end{pmatrix}$. Then applying Binet's theorem about determinants we have $\det(A_1 A_2) = \det(A_1)\det(A_2) \neq 0$ so that the coefficients we wrote for $f_1 \circ f_2$ satisfy the inequality $ad - bc \neq 0$. Associativity of composition can then be inferred by associativity of matrix product, and the neutral element of G is $\mathrm{id}_{\mathbb{R}} = X$, obtained for $a = d = 1$ and $b = c = 0$. The inverse of the transformation f_1 exists and can be defined as $f_1^{-1} = \frac{dX - b}{-cX + a}$.
2. It is enought to consider the subgroup of functions of the form $f = X + r$, $r \in R$. Composing two such functions we are just summing the two correspondent real numbers. [This subgroup is actually the image of the subgroup in Exercise 1.1 via the morphism in the next point]
3. We have already proved that α is a morphism in Point 1.

$$\begin{aligned} \ker(\alpha) &= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{R}) \middle| \frac{aX + b}{cX + d} = X \right\} \\ &= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| a = d \neq 0, b = c = 0 \right\} \end{aligned}$$

It is the group of invertible diagonal matrices, which is isomorphic to $R^\times$. The map α is surjective by definition, since four coefficients defining a Möbius function can be always be put in a 2×2 matrix so that it is invertible.
4. We look for transformations satisfying $f^2 = \mathrm{id}_{\mathbb{R}}$. i.e. $f = f^{-1}$. Considering a Möbius transformation of the form $f = (aX + b)/(cX + d)$ we get

$$\frac{aX + b}{cX + d} = \frac{dX - b}{-cX + a} \Leftrightarrow (aX + b)(-cX + a) = (cX + d)(dX - b)$$
$$\Leftrightarrow c(a + d)X^2 + (a^2 - d^2)X + b(a + d) = 0 \Leftrightarrow \left(a = -d \text{ or } \begin{cases} c = b = 0 \\ a = d \end{cases} \right)$$

and we have three possibilities:

- $a = d = 0$. The we get a Möbius function of the form $f = b/(cX)$, where $b \neq 0 \neq c$ (so that $ad - bc1 \neq 0$). Such an involution can just be written as $f = k/X$, for $k \in \mathbb{R}^\times$.
- $a = -d \neq 0$. We get an involution of the form $f = (aX + b)/(cX - a)$, and being $a \neq 0$ we can divide by a and write $f = (X + \lambda)/(\mu X - 1)$, for $\lambda, \mu \in \mathbb{R}$ such that $\lambda\mu \neq 1$.

Please turn over!

- $a = d \neq 0$. Then we need $b = c = 0$, and we get the identity $f = X$.

In conclusion, all the non-trivial involution are

$$f = \frac{k}{X}, k \neq 0 \text{ and } f = \frac{X+\lambda}{\mu X - 1}, \lambda\mu \neq 1$$

5. **(*)** As you have been told in class, Cayley's theorem allows us to embed every group into a symmetric group. Prove it by showing in detail that the following is a well-defined injective group homomorphism:

$$\begin{aligned} \chi : G &\to \mathrm{Sym}(G) \\ g &\mapsto \chi_g : (x \mapsto g \cdot x) \end{aligned}$$

Solution (sketch):

There are three things which need to be proven:

1. χ is a map, i.e. $\chi_g \in \mathrm{Sym}(G)$. One has to prove that the association $x \mapsto g \cdot x$ is a bijection.
2. χ is a group homomorphism, i.e. $\chi_{gh} = \chi_g \circ \chi_h$. This can be tested on elements $x \in G$.
3. χ is injective (easily done by comparing χ_g and $\chi_{g'}$ on 1_G).

Instead of proving directly that χ_g is bijective, one can first prove the equality in the second step (considering χ_g as a non-necessarily bijective map $G \to G$). Then $\chi_{g^{-1}}$ is an inverse of χ_g for all $g \in G$, so that those maps are all bijective.