# Homework assignment 2 - Solutions
# Abstract algebra

Erik Lindell

**Question 1**. (2 points)

Let $G = \left\{ \begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix} : a, b \in \mathbb{R},\ a > 0 \right\}$ and let $N = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} : b \in \mathbb{R} \right\}$.

i) Show that $N \trianglelefteq G$ and prove that $G/N$ is isomorphic to $\mathbb{R}$. (Hint: use that $\mathbb{R}_{>0}$ with multiplication is isomorphic with $\mathbb{R}$ with addition.)

ii) Either find a non-trivial normal subgroup $M \trianglelefteq G$ that is properly contained in $N$, or show that no such subgroup exists.

**Solution.**

i) To show that $N$ is normal, let

$$B = \begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix} \in N, \qquad A = \begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix} \in G.$$

Note that

$$A^{-1} = \frac{1}{aa^{-1}} \begin{pmatrix} a^{-1} & -b \\ 0 & a \end{pmatrix} = \begin{pmatrix} a^{-1} & -b \\ 0 & a \end{pmatrix}.$$

We thus ges that

$$ABA^{-1} = \begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix} \begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a^{-1} & -b \\ 0 & a \end{pmatrix} = \begin{pmatrix} a & ac+b \\ 0 & a^{-1} \end{pmatrix} \begin{pmatrix} a^{-1} & -b \\ 0 & a \end{pmatrix} = \begin{pmatrix} 1 & -ab + a^2c + ab \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a^2c \\ 0 & 1 \end{pmatrix} \in N.$$

Thus $N$ is normal. To prove that $G/B \cong \mathbb{R}$, we define a map

$$\phi : G \to \mathbb{R}_{>0}$$

by

$$\phi\left( \begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix} \right) = a.$$

We have

$$\phi\left( \begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix} \begin{pmatrix} c & d \\ 0 & c^{-1} \end{pmatrix} \right) = \phi\left( \begin{pmatrix} ac & ad + bc^{-1} \\ 0 & a^{-1}c^{-1} \end{pmatrix} \right) = ac = \phi\left( \begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix} \right) \phi\left( \begin{pmatrix} c & d \\ 0 & c^{-1} \end{pmatrix} \right).$$

Thus $\phi$ is a group homomorphism. Since for any $a \in \mathbb{R}_{>0}$ we have for example

$$A_a = \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \in G$$

and $\phi(A_a) = a$, $\phi$ is surjective. Furthermore, $A \in G$ is in the kernel of $\phi$ if and only if $a = 1$, in which case also $a^{-1} = 1$, so

$$\ker(\phi) = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \mid b \in \mathbb{R} \right\} = N.$$

By the first isomorphism theorem, we get that

$$\mathbb{R}_{>0} \cong G/\ker(\phi) = G/N.$$

Since $(\mathbb{R}_{>0}, \cdot) \cong (\mathbb{R}, +)$, we get

$$G/N \cong \mathbb{R}.$$

**Remark.** Note that by proving that $N$ is the kernel of a homomorphism, we have proved that it is a normal subgroup independently of the first part of the solution, where we proved this directly.

ii) Suppose that $M \trianglelefteq G$ and $M \subseteq N$. If $M$ is non-trivial, there exists some $b \in \mathbb{R} \setminus \{0\}$ such that

$$B = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \in M.$$

Now let $x \in \mathbb{R}$ be arbitrary. Then there exists an $a \in \mathbb{R}_{>0}$ such that $a^2 b = x$ or $a^2 b = -x$ (choose $\sqrt{\pm x/b}$ depending on the sign of $x/b$). In the first case, we get by normality and the calculation in (a), that

$$\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a^{-1} & 0 \\ 0 & a \end{pmatrix} = \begin{pmatrix} 1 & a^2 b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \in M.$$

In the second case, we get similarly that

$$\begin{pmatrix} 1 & -x \\ 0 & 1 \end{pmatrix} \in M.$$

Since $M$ is a subgroup and thus closed under inverses, we get in either case that

$$\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \in M.$$

Thus every element of $N$ is also in $M$, so since $M \subset N$, we get $M = N$. This proves that no non-trivial subgroup $M \trianglelefteq G$ can be properly contained in $N$.

**Question 2**. (2 points)

Let $G_i$ for $i = 1, \cdots, n$ be finite groups of relatively prime order. Show that $\mathrm{Aut}(G_1 \times G_2 \times \cdots \times G_n)$, the group of automorphisms of $G_1 \times G_2 \times \cdots \times G_n$, is isomorphic to the direct product $\mathrm{Aut}(G_1) \times \cdots \times \mathrm{Aut}(G_n)$.

**Solution.** Let us start by proving this for $n = 2$ and then use induction. We define a map

$$\Phi : \mathrm{Aut}(G_1) \times \mathrm{Aut}(G_2) \to \mathrm{Aut}(G_1 \times G_2)$$

by

$$\Phi(\varphi_1,\varphi_2)(g_1,g_2) = (\varphi_1(g_1),\varphi_2(g_2)),$$

for $(g_1,g_2) \in G_1 \times G_2$. To see that this well-defined, note that since $\varphi_1$ and $\varphi_2$ are homomorphisms, we have

$$\begin{aligned}
\Phi(\varphi_1,\varphi_2)\left((g_1,g_2)\cdot(h_1,h_2)\right) &= \Phi(\varphi_1,\varphi_2)(g_1h_1,g_2h_2) = \\
&= (\varphi_1(g_1h_1),\varphi_2(g_2h_2)) \\
&= (\varphi_1(g_1)\varphi(h_1),\varphi_2(g_2)\varphi_2(h_2)) \\
&= (\varphi_1(g_1),\varphi_2(g_2))\cdot(\varphi_1(h_1),\varphi_2(h_2)) \\
&= (\Phi(\varphi_1,\varphi_2)(g_1,g_2))\cdot(\Phi(\varphi_1,\varphi_2)(h_1,h_2))
\end{aligned}$$

so $\Phi(\varphi_1,\varphi_2): G_1\times G_2 \to G_1\times G_2$ is a homomorphism. Furthermore, since $\varphi_1$ and $\varphi_2$ are invertible, we have a homomorphism

$$\Phi(\varphi_1^{-1},\varphi_2^{-1})$$

which is clearly inverse to $\Phi(\varphi_1,\varphi_2)$, proving that $\Phi(\varphi_1,\varphi_2)$ is indeed in $\mathrm{Aut}(G_1\times G_2)$.

Next, let us prove that $\Phi$ is a homomorphism. For $(g_1,g_2)\in G_1\times G_2$ we have

$$\begin{aligned}
\Phi((\varphi_1,\varphi_2)\circ(\psi_1,\psi_2))(g_1,g_2) &= \Phi(\varphi_1\circ\psi_1,\varphi_2\circ\psi_2)(g_1,g_2) \\
&= ((\varphi_1\circ\psi_1)(g_1),(\varphi_2\circ\psi_2)(g_2)) \\
&= (\varphi_1(\psi_1(g_1)),\varphi_2(\psi_2(g_2))) \\
&= \Phi(\varphi_1,\varphi_2)(\psi_1(g_1),\psi_2(g_2)) \\
&= \left(\Phi(\varphi_1,\varphi_2)\circ\Phi(\psi_1,\psi_2)\right)(g_1,g_2)
\end{aligned}$$

so

$$\Phi((\varphi_1,\varphi_2)\circ(\psi_1,\psi_2)) = \Phi(\varphi_1,\varphi_2)\circ\Phi(\psi_1,\psi_2),$$

and thus $\Phi$ is a homomorphism.

We want to prove that $\Phi$ is injective and surjective. For injectivity, note that if $\Phi(\varphi_1,\varphi_2)\in\ker(\Phi)$, i.e. if

$$\Phi(\varphi_1,\varphi_2) = \mathrm{Id}_{G_1\times G_2},$$

we have for any $(g_1,g_2)\in G_1\times G_2$ that

$$(g_1,g_2) = \Phi(\varphi_1,\varphi_2)(g_1,g_2) = (\varphi_1(g_1),\varphi_2(g_2)),$$

so $\varphi_1(g_1) = g_1$ and $\varphi_2(g_2) = g_2$, meaning that $\varphi_1 = \mathrm{Id}_{G_1}$ and $\varphi_2 = \mathrm{Id}_{G_2}$ and thus $(\varphi_1,\varphi_2)$ is the identity element in $\mathrm{Aut}(G_1)\times\mathrm{Aut}(G_2)$, meaning that $\ker(\Phi)$ is trivial and thus that $\Phi$ is injective.

For surjectivity, let $\varphi\in\mathrm{Aut}(G_1\times G_2)$. We want to show that $\varphi = \Phi(\varphi_1,\varphi_2)$ for some automorphisms $\varphi_1\in\mathrm{Aut}(G_1)$ and $\varphi_2\in\mathrm{Aut}(G_2)$. If $(g_1,1)\in G_1\times G_2$ we have that $|\varphi(g_1,1)| = |(g_1,1)|$ since $\varphi$ is an automorphism. Note that $|(g_1,1)| = |g_1|$, so if $\varphi(g_1,g_2) = (h_1,h_2)$, we have

$$|g_1| = |(h_1,h_2)| = \mathrm{lcm}(|h_1|,|h_2|).$$

This means in particular that $|h_2|$ divides $|g_1|$, which in turn divides $|G_1|$. But $|h_2|$ also divides $|G_2|$, so since $\gcd(|G_1|,|G_2|) = 1$, we must have $|h_2| = 1$ and thus $h_2 = 1$. Summarizing, we have that

$$\varphi(g_1,1) = (h_1,1)$$

for some $h_1 \in G_1$. If we let $\iota_1 : G_1 \to G_1 \times G_2$ denote the homomorphism $\iota(g_1) = (g_1, 1)$ and we let $\pi_1 : G_1 \times G_2 \to G_1$ denote the homomorphism $\pi_1(g_1, g_2) = g_1$, we can thus define a homomorphism $\varphi_1 : G_1 \to G_1$ by

$$\varphi_1 = \pi_1 \circ \varphi \circ \iota_1.$$

This homomorphism has an inverse given by

$$\pi_1 \circ \varphi^{-1} \circ \iota_1$$

so $\varphi_1 \in \mathrm{Aut}(G_1)$ and we have

$$\varphi(g_1, 1) = (\varphi_1(g_1), 1).$$

Similarly, we obtain an automorphism $\varphi_2 \in \mathrm{Aut}(G_2)$ such that

$$\varphi(1, g_2) = (1, \varphi_2(g_2)).$$

Thus

$$\varphi(g_1, g_2) = \varphi((g_1, 1) \cdot (1, g_2)) = \varphi(g_1, 1)\varphi(1, g_2) = (\varphi_1(g_1), 1) \cdot (1, \varphi_2(g_2)) = (\varphi_1(g_1), \varphi_2(g_2)),$$

so $\varphi = \Phi(\varphi_1, \varphi_2)$ and $\Phi$ is surjective, finishing the proof.

**Question 3**. (2 points)

Let $G$ be the group of rigid motions of $\mathbb{R}^3$ preserving the unit cube $[0, 1]^3$.

Find the order of the group $G$, by means of the orbit-stabilizer theorem.

**Solution.** Let $X$ be the set of faces of the cube. Note that $G$ acts on $X$ via its action on the cube. This action is transitive, since for any pair of faces, we can find a rigid motion which takes the first face to the second. Furthermore, the stabilizer of a face $x \in X$ is given by the identity and the rotations by $\pi/2, \pi$ and $3\pi/2$ around the line through the center of the face and the center of the cube. Thus the stabilizer is of order 4. Combining these facts, the orbit stabilizer theorem tells us that

$$|G| = |Gx||G_x| = 6 \cdot 4 = 24.$$

**Question 4**. (2 points)

Let $\Gamma = \mathrm{SL}(2, \mathbb{Z})$. Let $n \geq 1$ be an integer. The principal congruence subgroup of level $n$ in $\Gamma$, denoted $\Gamma(n)$, is defined as follows

$$\Gamma(n) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2, \mathbb{Z}) \colon a, d \equiv 1 \bmod n, \text{ and } b, c \equiv 0 \bmod n \right\}.$$

i) Show that $\Gamma(n)$ is normal in $\mathrm{SL}(2, \mathbb{Z})$.

ii) Show that $\mathrm{SL}(2, \mathbb{Z})/\Gamma(n)$ is isomorphic to $\mathrm{SL}(2, \mathbb{Z}_n)$.

**Solution.**

i) Let $B \in \Gamma(n)$ and $A \in \mathrm{SL}(2,\mathbb{Z})$ and let us write

$$B = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \quad A = \begin{pmatrix} e & f \\ g & h \end{pmatrix}.$$

Then

$$A^{-1} = \begin{pmatrix} e & f \\ g & h \end{pmatrix}^{-1} = \frac{1}{eh - fg} \begin{pmatrix} h & -f \\ -g & e \end{pmatrix} = \begin{pmatrix} h & -f \\ -g & e \end{pmatrix},$$

since $A \in \mathrm{SL}(2,\mathbb{Z})$, so $\det(A) = eh - fg = 1$. We thus get

$$\begin{aligned} ABA^{-1} &= \begin{pmatrix} e & f \\ g & h \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} h & -f \\ -g & e \end{pmatrix} \\ &= \begin{pmatrix} ae + cf & be + fd \\ ag + hc & bg + hd \end{pmatrix} \begin{pmatrix} h & -f \\ -g & e \end{pmatrix} \\ &= \begin{pmatrix} h(ae + cf) - g(be + fd) & -f(ae + cf) + e(be + fd) \\ h(ag + hc) - g(bg + hd) & -f(ag + hc) + e(bg + hd) \end{pmatrix} \end{aligned}$$

Since $a \equiv d \equiv 1 \bmod n$, $b \equiv c \equiv 0 \bmod n$ and $eh - fg = 1$, we get

$$\begin{aligned} h(ae + cf) - g(be + fd) &\equiv he - gf \equiv 1 \bmod n, \\ -f(ae + cf) + e(be + fd) &\equiv -ef + ef \equiv 0 \bmod n, \\ h(ag + hc) - g(bg + hd) &\equiv gh - gh \equiv 0 \bmod n, \\ -f(ag + hc) + e(bg + hd) &\equiv -fg + eh \equiv 1 \bmod n. \end{aligned}$$

Thus $ABA^{-1} \in \Gamma(n)$.

ii) We define a map

$$\phi : \mathrm{SL}(2,\mathbb{Z}) \to \mathrm{SL}(2,\mathbb{Z}_n)$$

by

$$\phi\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) = \begin{pmatrix} \bar{a} & \bar{b} \\ \bar{c} & \bar{d} \end{pmatrix},$$

where we write $\bar{x}$ for equivalence class in $\mathbb{Z}_n$ of $x \in \mathbb{Z}$. This is well defined since if $ad - bc = 1$ we have $\bar{a}\bar{d} - \bar{b}\bar{c} = \overline{ad - bc} = \bar{1}$. That it is a homomorphism follows since this equivalence relation is compatible with all operations used in matrix multiplication. Specifically, we have

$$\begin{aligned} \phi\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} e & f \\ g & h \end{pmatrix}\right) &= \phi\left(\begin{pmatrix} ae + bg & af + bh \\ ce + dg & cf + dh \end{pmatrix}\right) \\ &= \begin{pmatrix} \overline{ae + bg} & \overline{af + bh} \\ \overline{ce + dg} & \overline{cf + dh} \end{pmatrix} \\ &= \begin{pmatrix} \bar{a}\bar{e} + \bar{b}\bar{g} & \bar{a}\bar{f} + \bar{b}\bar{h} \\ \bar{c}\bar{e} + \bar{d}\bar{g} & \bar{c}\bar{f} + \bar{d}\bar{h} \end{pmatrix} \\ &= \begin{pmatrix} \bar{a} & \bar{b} \\ \bar{c} & \bar{d} \end{pmatrix} \begin{pmatrix} \bar{e} & \bar{f} \\ \bar{g} & \bar{h} \end{pmatrix} \\ &= \phi\begin{pmatrix} a & b \\ c & d \end{pmatrix} \phi\begin{pmatrix} e & f \\ g & h \end{pmatrix}. \end{aligned}$$

We note that a matrix

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

is in the kernel of $\phi$ if and only if $\bar{a} = \bar{d} = \bar{1}$ and $\bar{b} = \bar{c} = \bar{0}$, which is precisely the definition of when a matrix is in $\Gamma(n)$. Thus $\ker(\phi) = \Gamma(n)$.

It now follows by the first isomorphism theorem that $\mathrm{SL}(2,\mathbb{Z})/\Gamma(n) \cong \mathrm{im}(\phi)$. However, proving that $\phi$ is surjective is not trivial (it doesn't follow immediately from the surjectivity of the homomorphism $\mathbb{Z} \to \mathbb{Z}_n$) and actually quite difficult for general $n$. In the case where $n = p$ is a prime, the proof can be simplified somewhat:

**Proof of surjectivity when $\mathbf{n} = \mathbf{p}$ is prime.** Suppose that

$$A = \begin{pmatrix} \bar{a} & \bar{b} \\ \bar{c} & \bar{d} \end{pmatrix} \in \mathrm{SL}(2,\mathbb{Z}_p).$$

The strategy will be to factor $A$ as a product of matrices that are easy to prove lie in the image of $\phi$. Since $\phi$ is a homomorphism, this will prove that $A$ is also in the image. To this end, note that for any integer $a$, the matrices

$$\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & -1 \\ 1-a & a \end{pmatrix} \tag{1}$$

have determinant 1 and are thus in $\mathrm{SL}(2,\mathbb{Z})$. Reducing these matrices modulo $p$ thus gives us matrices in the image of $\phi$.

In the first step of our proof, we will reduce to the case where $A$ is a diagonal matrix. Note that since $A$ is invertible, we have that either $\bar{a} \neq \bar{0}$ or $\bar{b} \neq \bar{0}$. We can assume, without loss of generality, that $\bar{a} \neq \bar{0}$, since in the case where $\bar{b} \neq 0$ we can instead consider the matrix obtained as follows:

$$\begin{pmatrix} \bar{a} & \bar{b} \\ \bar{c} & \bar{d} \end{pmatrix} \begin{pmatrix} \bar{0} & \bar{1} \\ -\bar{1} & \bar{0} \end{pmatrix} = \begin{pmatrix} -\bar{b} & \bar{a} \\ -\bar{d} & \bar{c} \end{pmatrix}.$$

The assumption that $\bar{a} \neq 0$ allows us to perform Gaussian elimination on $A$. More specifically, since $p$ is a prime it follows that $\bar{a}$ has a multiplicative inverse in $\mathbb{Z}_p$, so the following matrix product is well-defined[1]:

$$\begin{pmatrix} \bar{1} & \bar{0} \\ -\bar{a}^{-1}\bar{c} & \bar{1} \end{pmatrix} \begin{pmatrix} \bar{a} & \bar{b} \\ \bar{c} & \bar{d} \end{pmatrix} = \begin{pmatrix} \bar{a} & \bar{b} \\ \bar{0} & -\bar{a}^{-1}\bar{b}\bar{c} + \bar{d} \end{pmatrix}.$$

Note that since $\bar{a}(-\bar{a}^{-1}\bar{b}\bar{c} + \bar{d}) = \bar{a}\bar{d} - \bar{c}\bar{d} = \bar{1}$ by assumption, we have that $-\bar{a}^{-1}\bar{b}\bar{c} + \bar{d} = a^{-1} \neq \bar{0}$. We thus have the following well defined matrix product:

$$\begin{pmatrix} \bar{1} & -\bar{a}\bar{b} \\ \bar{0} & \bar{1} \end{pmatrix} \begin{pmatrix} \bar{a} & \bar{b} \\ \bar{0} & \bar{a}^{-1} \end{pmatrix} = \begin{pmatrix} \bar{a} & \bar{0} \\ \bar{0} & \bar{a}^{-1} \end{pmatrix}.$$

If we let

$$U = \begin{pmatrix} \bar{1} & \bar{0} \\ -\bar{a}^{-1}\bar{c} & \bar{1} \end{pmatrix}, \quad V = \begin{pmatrix} \bar{1} & -\bar{a}\bar{b} \\ \bar{0} & \bar{1} \end{pmatrix},$$

[1]Note that the reason we can do Gaussian elimination is because $p$ being a prime implies that $\mathbb{Z}_n$ is a field.

we note that $U, V \in \mathrm{SL}(2, \mathbb{Z}_p)$ and also that $U, V$ are both in the image of $\phi$, since any matrices of the form

$$\begin{pmatrix} \bar{1} & \bar{0} \\ \bar{\alpha} & \bar{1} \end{pmatrix}, \quad \begin{pmatrix} \bar{1} & \bar{\alpha} \\ \bar{0} & \bar{1} \end{pmatrix}$$

are in the image of $\phi$. This means that we can write

$$A = U^{-1} V^{-1} \begin{pmatrix} \bar{a} & \bar{0} \\ \bar{0} & \bar{a}^{-1} \end{pmatrix},$$

with the two first matrices in the product being in the image of $\phi$. If we can prove that any diagonal matrix in $\mathrm{SL}(2, \mathbb{Z}_p)$ is in the image of $\phi$, we are thus finished. This follows by the factorization

$$\begin{pmatrix} \bar{1} & -\bar{1} \\ 1 - \bar{a}^{-1} & \bar{a}^{-1} \end{pmatrix} \begin{pmatrix} \bar{1} & \bar{0} \\ \bar{1} - \bar{a} & \bar{1} \end{pmatrix} \begin{pmatrix} \bar{1} & \bar{a}^{-1} \\ \bar{0} & \bar{1} \end{pmatrix} = \begin{pmatrix} \bar{a} & -\bar{1} \\ 0 & a^{-1} \end{pmatrix} \begin{pmatrix} \bar{1} & \bar{a}^{-1} \\ \bar{0} & \bar{1} \end{pmatrix} = \begin{pmatrix} \bar{a} & 0 \\ \bar{0} & \bar{a}^{-1} \end{pmatrix}.$$

**Remark 1.** A similar strategy for the proof works in the case where $n$ is not prime, but more work has to be done to get around the fact that nonzero elements in $\mathbb{Z}_n$ don't necessarily have multiplicative inverses in this case, so Gaussian elimination has to be replaced by an alternative method.

**Remark 2.** Note that as in the solution to Question 1, proving that $\Gamma(n)$ is the kernel of a homomorphism proves that it is a normal subgroup, independently of the direct proof in (i).

**Question 5**. (2 points)

Let $n \geq 1$ and consider the subgroups

$$\mu_n = \{z \in \mathbb{C} \mid z^n = 1\},$$
$$S^1 = \{z \in \mathbb{C} \mid |z| = 1\},$$

of $\mathbb{C}^\times$. Show that $S^1 \cong \mathbb{C}^\times / (\mu_n \mathbb{R}_{>0})$, where $\mu_n \mathbb{R}_{>0}$ is the product of the subgroups.

**Solution.** Let us define a map $\phi : \mathbb{C}^\times \to S^1$ by

$$\phi(z) = \left( \frac{z}{|z|} \right)^n.$$

This is a homomorphism, since

$$\phi(z_1 z_2) = \left( \frac{z_1 z_2}{|z_1 z_2|} \right)^n = \left( \frac{z_1 z_2}{|z_1||z_2|} \right)^n = \left( \frac{z_1 z}{|z_1|} \right)^n \left( \frac{z_2}{|z_2|} \right)^n = \phi(z_1)\phi(z_2).$$

If $w \in S^1$, i.e. $|w| = 1$, we also have $|w^{1/n}| = |w|^{1/n} = 1$ and thus

$$\phi(w^{1/n}) = (w^{1/n})^n = w,$$

so $\phi$ is surjective.

Finally, we will show that the kernel is $\mu_n\mathbb{R}_{>0}$. The elements of $\mu_n$ are of the form $e^{2\pi ik/n}$, for $k$ an integer, so this means that $z \in \mu_n\mathbb{R}_{>0}$ if and only if $z = re^{2\pi ik/n}$ for $r \in \mathbb{R}_{>0}$ and any integer $k$. Thus

$$\phi(z) = e^{2\pi ikn/n} = e^{2\pi ik} = 1,$$

so $z \in \ker(\phi)$. Conversely, any complex number $z$ can be written as $re^{i\theta}$ for some $r \in \mathbb{R}_{>0}$ and $\theta \in [0, 2\pi)$, so if $z \in \ker(\phi)$ we have

$$1 = \phi\left(re^{i\theta}\right) = e^{i\theta n}.$$

This means that $\theta n = 2\pi k$, for some integer $k$, or in other words $\theta = 2\pi k/n$, so

$$z = re^{2\pi ik/n} \in \mu_n\mathbb{R}_{>0}.$$

Thus $\ker(\phi) = \mu_n\mathbb{R}_{>0}$, so it follows by the first isomorphism theorem that $S^1 \cong \mathbb{C}^\times/(\mu_n\mathbb{R}_{>0})$.