Solutions

Problems 3, exercise 4

Show that

$$G = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \right\}$$

is a subgroup of $\mathrm{GL}(\mathbb{Z})$ isomorphic to $\{1, -1, i, -i\}$.

Solution.

We denote by

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},\ J = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix},\ A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},\ B = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

The subset $G \subset GL(\mathbb{Z})$ is a subgroup. Indeed, direct computations show that $AB = I,\ A^2 = B^2 = J,\ JA = -A = B,\ JB = -B = A$, and so on.

Consider the map $\varphi : G \to \{1, -1, i, -i\}$ defined by $\varphi(I) = 1,\ \varphi(J) = -1,\ \varphi(A) = i, \varphi(B) = -i$. On can check that φ is a group homomorphism. Indeed, we have for example

$$\varphi(AB) = \varphi(I) = 1; \quad \text{while} \quad \varphi(A)\varphi(B) = i \times (-i) = 1,$$

so $\varphi(AB) = \varphi(A)\varphi(B)$. All cases must be checked!

By definition of the map φ, we have $\ker(\varphi) = \{I\}$ the identity element of G, thus φ is injective. Clearly, φ is surjective, since every element of $\{1, -1, i, -i\}$ has an antecedent. It follows that φ is an isomorphism of groups.

Problems 3, exercise 5

Show that the circle group $\mathbb{C}^0 = \{z \in \mathbb{C}, |z| = 1\}$ is not isomorphic to $\mathbb{R}^*$.

Solution.

Suppose that $\varphi : \mathbb{C}^0 \to \mathbb{R}^*$ is an isomorphism of groups. Then, we have

$$\varphi(-1) = \varphi(i^2) = \varphi(i)^2, \tag{1}$$

as well as

$$1 = \varphi(1) = \varphi((-1)^2) = \varphi(-1)^2. \tag{2}$$

It follows from Eq. (2) that $\varphi(-1) = \pm 1$. But since φ is an isomorphism, we must have $\varphi(-1) = -1$, otherwise φ would not be injective.

Then, putting $\varphi(-1) = -1$ in Eq. (1), we obtain $-1 = \varphi(i)^2 \in \mathbb{R}^*$. Now, we see the contradiction : $\varphi(i)^2$ is a square in $\mathbb{R}^*$, therefore we must have $\varphi(i)^2 > 0$. Thus, the equality $-1 = \varphi(i)^2$ is impossible and such an isomorphism φ cannot exist.

Problems 4, exercise 1

Let G be the group $< a > \times < b >$, where $|a| = 8,\ |b| = 12$. Let $K =< (a^2, b^3) >$. Compute the order of $\overline{(a^4, b)} \in G/K$.

Solution.

First, note that $G = \Big\{(a^i, b^j),\ i \leq 7, j \leq 11\Big\}$. In the quotient G/K, we have

$$\overline{(a^4, b)}^2 = \overline{(a^8, b^2)} = \overline{(1, b^2)}.$$

The last equality holds because $|a| = 8$. Then, we have

$$\overline{(a^4, b)}^3 = \overline{(1, b^2)(a^4, b)} = \overline{(a^4, b^3)} = \overline{(1, 1)}.$$

Thus, it follows that the element $\overline{(a^4, b)}$ has roder 3 in the quotient G/K.

Problems 4, exercise 2

Show that $\mathbb{Q}\,/\,\mathbb{Z}$ is an infinite abelian group in which every element has a finite order.

Solution.

Let us show that every element in $\mathbb{Q}\,/\,\mathbb{Z}$ has finite order. Let $x \in \mathbb{Q}\,/\,\mathbb{Z}$. Then, there exists $p, q, k \in \mathbb{Z}$ such that $x = \frac{p}{q} + k$. We can suppose that $\gcd(p, q) = 1$. We have $qx = p + kq \in Z$, thus $\overline{qx} = \overline{1} \in \mathbb{Q}\,/\,\mathbb{Z}$. It follows that $|x| \leq q$. Actually the order of x is exactly equal to q : suppose that there exists $s < q$ such that $\overline{qx} = \overline{1}$. Then, we would have $s(\frac{p}{q} + k) \in \mathbb{Z}$, thus $q|sp$. Since $\gcd(p, q) = 1$, it follows that $q|s$, which is a contradiction.

Let us show that $\mathbb{Q}\,/\,\mathbb{Z}$ is infinite. Let $q \in \mathbb{Z}$ and consider the family $F = \{\frac{1}{q} + k,\ k \in \mathbb{Z}\}$. Then, F is a infinite subset of $\mathbb{Q}\,/\,\mathbb{Z}$.

Problems 4, exercise 3

Let G be a group and H a subgroup. Recall that the *index* of H in G, denoted by $[G : H]$, is the number of left cosets of H. If there is a chain of inclusions of subgroups $K \subset H \subset G$, show that

$$[G : K] = [G : H][H : K].$$

Solution.

We assume that $[G : H] < \infty,\ [H : K] < \infty$.

Suppose that $[G : H] = m$. Thus, we have a partition of G given by

$$G = g_1 H \sqcup \cdots \sqcup g_m H, \quad g_1, \cdots g_m \in G.$$

Similarly, if $[H : K] = n$, we have a partition of H given by

$$H = h_1 K \sqcup \cdots \sqcup h_n K, \quad h_1, \cdots h_n \in H.$$

Therefore, for all $1 \leq i \leq m$, we have

$$g_i H = g_i h_1 K \sqcup \cdots \sqcup g_i h_n K,$$

which is a partition of $g_i H$, because the map $x \mapsto g_i x$ is invertible. Therefore, we have

$$G = \sqcup_{i=1}^m g_i H = \sqcup_{i=1}^m \sqcup_{j=1}^n g_i h_j K.$$

It follows that $[G : K] = m \times n$.

Problems 4, exercise 4

Recall the circle group $\mathbb{C}^0 = \{z \in \mathbb{C}, |z| = 1\}$. Show that the group $\mathbb{C}^\times/\mathbb{C}^0$ is isomorphic to $(\mathbb{R}, +)$.

Solution.

First, notice that $\mathbb{C}^0$ is a normal subgroup of $\mathbb{C}^\times$, thus it is legit to consider the quotient group $\mathbb{C}^\times \,/\, \mathbb{C}^0$. Consider the map

$$\varphi : \mathbb{C}^\times \,/\, \mathbb{C}^0 \to (\mathbb{R}, +), \quad \overline{z} \mapsto \ln(|z|).$$

First, we show that φ is a group homomorphism. Let $z, w \in \mathbb{C}^\times$.

$$\varphi(\overline{zw}) = \ln(|z||w|) = \ln(|z|) + \ln(|w|) = \varphi(\overline{z}) + \varphi(\overline{w}),$$

thus φ is a group homomorphism. Moreover, we have $\ker(\varphi) = \{\overline{1}\}$, so φ is injective. It remains to show that φ is surjective. Let $x \in \mathbb{R}$. We know that $x = \ln(e^x)$. Thus, it suffices to find $\overline{z} \in \mathbb{C}^\times \,/\, \mathbb{C}^0$ such that $|z| = e^x$, which is always possible. Thus φ is surjective, and it follows that it is an isomorphism.

Problems 4, exercise 4

Classify the groups of order 6 by considering the following cases :

1. there is an element of order 6 ;
2. there is an element of order 3 and no element of order 6 ;
3. all elements have order 1 or 2.

Solution.

1. Suppose that G contains an element of order 6. Let's denote it by x. It follows that $G = \{1, x, x^2, x^3, x^4, x^5\}$ and $G \cong C_6$, the cyclic group of order 6.
2. Suppose that G contains an element of order 3 and no element of order 6. Let's denote it by x. Let $y \neq x$. The possible orders for y are 1,2,3 or 6 ; but 1 and 6 are impossible since the identity is the only element of order 1 and 6 is ruled out by assumption.

   Suppose that $|y| = 3$. Then, we have the subgroup inclusion

   $$H = \{1, x, x^2, y, y^2, xy\} \subset G.$$

   (Note that the element xy is distinct of all others elements in H, otherwise we would have $y = 1$ or $y = x$, which are both a contradiction)

   But the element x^2y must also belong to the subgroup H. Since $|H| \leq |G| = 6$, the element x^2y must be equal to one of the element already in H. Let's figure out which one.

   - Is $x^2y = x$? In that case, we would have $xy = 1$, which is impossible since $x^{-1} = x^2$.
   - Is $x^2y = x^2$? In that case, we would have $y = 1$, which is impossible since y has order 3.
   - Is $x^2y = y$? In that case, we would have $x^2 = 1$, which is impossible since x has order 3.
   - Is $x^2y = y^2$? In that case, we would have $x^2 = y$. It follows that $xy = x^3 = 1$, and we already ruled out this case.
   - Is $x^2y = 1$? In that case, we would have $x =$, which is impossible since x has order 3.

Therefore, we have a contradiction, because we just showed that H must have at least 7 elements. We deduce that such an y cannot exists : that there is no $y \neq x$ such that $|y| = 3$.

Therefore, $|y| = 2$ and $G = \{1, x, x^2, y, xy, x^2y\}$. Then, there are two cases.
First case. The case where $xy = yx$. Then, $G \cong <x> \times <y> \cong C_3 \times C_2$.
Second case. The case where $xy \neq yx$. Then, $G \cong S_3$ and the isomorphism is given by $x \mapsto (123)$, $y \mapsto (12)$.

3. Suppose that all the elements have order 1 or 2. Then, $\forall x \in G,\ x \neq 1$, we have $x^2 = 1$. Then, G is given by
$$G = \{1, x, y, xy, z, xz, yz\}.$$
All those elements are different, since the maps $L_g : h \mapsto gh$ is a bijection for all $g \in G$. Since $(xy)^2 = 1$, we get $xy = yx$, which is impossible. Thus that case do no occur.