Math 103B HW 2 Solutions to Selected Problems

5. **Prove that $\mathbb{Z} \times \mathbb{Z}$ is not cyclic. Does your proof work for $\mathbb{Z} \times G$ where G is any group with more than one element?**

   Solution: Suppose that $\mathbb{Z} \times \mathbb{Z} = \langle (a, b) \rangle$ is cyclic. Then there exists $n \in \mathbb{Z}$ such that $(a+1, b) = n \cdot (a, b) = (n \cdot a, n \cdot b)$. This implies that $a + 1 = n \cdot a$, so that $1 = (n-1) \cdot a$, which implies that $a \in \{-1, 1\}$ and $n - 1 \in \{-1, 1\}$. Then since $b = n \cdot b$, we get that $0 = (n-1) \cdot b$ with $n - 1 \in \{-1, 1\}$, which implies that $b = 0$. But then $(0, 1) \in \mathbb{Z} \times \mathbb{Z}$ and for any $m \in \mathbb{Z}$, we have

   $$m \cdot (a, b) = (m \cdot a, m \cdot b) = (m \cdot a, 0) \neq (0, 1),$$

   so $(0, 1) \notin \langle (a, b) \rangle$, contradicting our assumption that $\mathbb{Z} \times \mathbb{Z} = \langle (a, b) \rangle$. Hence, $\mathbb{Z} \times \mathbb{Z}$ is not cyclic.

   We can use a similar to proof to show that $\mathbb{Z} \times G$ is not cyclic if G has more than one element. Suppose that $\mathbb{Z} \times G = \langle (a, g) \rangle$ is cyclic. Then there exists $n \in \mathbb{Z}$ such that $(a+1, g) = (n \cdot a, g^n)$. This tells us that $a + 1 = n \cdot a$, which implies that $1 = (n-1) \cdot a$, so $a \in \{1, -1\}$ and $(n-1) \in \{-1, 1\}$. Then since $g = g^n$, we get that $e_G = g^{n-1}$, which implies that $g = e_G$ since $n - 1 \in \{-1, 1\}$. Since G has more than one element, there exists $h \in G \setminus \{e_G\}$. Then $(0, h) \in \mathbb{Z} \times G$, but for all $n \in \mathbb{Z}$ we have

   $$(n \cdot a, g^n) = (n \cdot a, e_G) \neq (0, h)$$

   since $h \neq e_G$. Hence, $(0, h) \notin \langle (a, g) \rangle$, contradicting our assumption that $\mathbb{Z} \times G = \langle (a, g) \rangle$. Thus, $\mathbb{Z} \times G$ is not cyclic.

8. **Is $\mathbb{Z}_3 \times \mathbb{Z}_9$ isomorphic to $\mathbb{Z}_{27}$? Why or why not?**

   Solution: $\mathbb{Z}_3 \times \mathbb{Z}_9$ is not isomorphic to $\mathbb{Z}_{27}$. Suppose, by way of contradiction, that there is an isomorphism $\varphi : \mathbb{Z}_{27} \to \mathbb{Z}_3 \times \mathbb{Z}_9$. Since isomorphisms preserve orders of elements, we get that $\varphi(1) \in \mathbb{Z}_3 \times \mathbb{Z}_9$ has order 27. However, by Theorem 8.1, the maximum order of an element of $\mathbb{Z}_3 \times \mathbb{Z}_9$ is 9, a contradiction. Hence, $\mathbb{Z}_3 \times \mathbb{Z}_9$ is not isomorphic to $\mathbb{Z}_{27}$.

19. **If r is a divisor of m and s is a divisor of n, find a subgroup of $\mathbb{Z}_m \times \mathbb{Z}_n$ that is isomorphic to $\mathbb{Z}_r \times \mathbb{Z}_s$.**

    Below, we will use the following facts

Lemma 1. *Suppose G_1 and G_2 are groups and $H_1 \leq G_1$ and $H_2 \leq G_2$. Then $(H_1 \times H_2) \leq (G_1 \times G_2)$.*

Proof. Exercise. $\square$

Lemma 2 (Problem 8.16)**.** *If G_1, G_2, H_1, H_2 are groups such that $G_1 \cong H_1$ and $G_2 \cong H_2$, then $G_1 \times G_2 \cong H_1 \times H_2$.*

Proof. Since $G_1 \cong H_1$ and $G_2 \cong H_2$, there exist isomorphisms $\varphi_1 : G_1 \to H_1$ and $\varphi_2 : G_2 \to H_2$. Define a function $\varphi : G_1 \times G_2 \to H_1 \times H_2$ by $\varphi(g_1, g_2) = (\varphi_1(g_1), \varphi_2(g_2))$. As an exercise, show that φ is an isomorphism (using the fact that φ_1 and φ_2 are isomorphisms). $\square$

Solution: We know that the subgroup $\langle \frac{m}{r} \rangle \leq \mathbb{Z}_m$ is cyclic of order r (so it is isomorphic to $\mathbb{Z}_r$), and the subgroup $\langle \frac{n}{s} \rangle \leq \mathbb{Z}_n$ is cyclic of order s (so it is isomorphic to $\mathbb{Z}_s$). Then $\langle \frac{m}{r} \rangle \times \langle \frac{n}{s} \rangle$ is a subgroup of $\mathbb{Z}_m \times \mathbb{Z}_n$ by Lemma 1 and it is isomorphic to $\mathbb{Z}_r \times \mathbb{Z}_s$ by Lemma 2.

35. **Prove that $\mathbb{R}^* \times \mathbb{R}^*$ is not isomorphic to $\mathbb{C}^*$.**

Solution: By way of contradiction, suppose that there exists an isomorphism $\varphi : \mathbb{C}^* \to \mathbb{R}^* \times \mathbb{R}^*$. Note that i has order 4 in $\mathbb{C}^*$, which implies that $\varphi(i) \in \mathbb{R}^* \times \mathbb{R}^*$ has order 4 as well since isomorphisms preserve orders of elements. We claim that the only elements of finite order in $\mathbb{R}^* \times \mathbb{R}^*$ are $\{(1,1), (-1,1), (1,-1), (-1,-1)\}$, which will lead to a contradiction since these elements all have order either 1 or 2. To see this, suppose $(a, b) \in \mathbb{R}^* \times \mathbb{R}^*$ has finite order. Then there is $n \in \mathbb{Z}_+$ such that $(1,1) = (a,b)^n = (a^n, b^n)$, so $a^n = b^n = 1$, which tells us that a and b have finite order in $\mathbb{R}^*$. But the only elements of finite order in $\mathbb{R}^*$ are 1 and -1, so the only elements of finite order in $\mathbb{R}^* \times \mathbb{R}^*$ are $\{(1,1), (-1,1), (1,-1), (-1,-1)\}$, as claimed. As stated above, this is a contradiction.

36. **Let**

$$H = \left\{ \begin{bmatrix} 1 & a & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \middle| \, a, b \in \mathbb{Z}_3 \right\}.$$

Show that H is an abelian group of order 9. Is H isomorphic to $\mathbb{Z}_9$ or $\mathbb{Z}_3 \times \mathbb{Z}_3$?

Solution: Let $\begin{bmatrix} 1 & a & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & c & d \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \in H$ (i.e. $a, b, c, d \in \mathbb{Z}_3$). Then

$$\begin{bmatrix} 1 & a & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & c & d \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & c+a & d+b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \in H,$$

so H is closed under matrix multiplication. Similarly,

$$\begin{bmatrix}1 & c & d\\0 & 1 & 0\\0 & 0 & 1\end{bmatrix}\begin{bmatrix}1 & a & b\\0 & 1 & 0\\0 & 0 & 1\end{bmatrix} = \begin{bmatrix}1 & a+c & b+d\\0 & 1 & 0\\0 & 0 & 1\end{bmatrix} = \begin{bmatrix}1 & c+a & d+b\\0 & 1 & 0\\0 & 0 & 1\end{bmatrix}$$

which shows that matrix multiplication is commutative on H. Also, we know that matrix multiplication is associative, and clearly $\begin{bmatrix}1 & 0 & 0\\0 & 1 & 0\\0 & 0 & 1\end{bmatrix} \in H$ is the identity element of H. Finally, the above computations show that the inverse of $\begin{bmatrix}1 & a & b\\0 & 1 & 0\\0 & 0 & 1\end{bmatrix} \in H$ is $\begin{bmatrix}1 & -a & -b\\0 & 1 & 0\\0 & 0 & 1\end{bmatrix} \in H$. Hence, H is an abelian group.

Now, we claim that H is isomorphic to $\mathbb{Z}_3 \times \mathbb{Z}_3$. To see this, define a function $\varphi : \mathbb{Z}_3 \times \mathbb{Z}_3 \to H$ by

$$\varphi(a,b) = \begin{bmatrix}1 & a & b\\0 & 1 & 0\\0 & 0 & 1\end{bmatrix}.$$

From the defintion of H, it is clear that φ is a bijection. Also, for $(a,b),(c,d) \in \mathbb{Z}_3 \times \mathbb{Z}_3$, we have

$$\varphi((a,b)+(c,d)) = \varphi(a+c,b+d) = \begin{bmatrix}1 & a+c & b+d\\0 & 1 & 0\\0 & 0 & 1\end{bmatrix} = \begin{bmatrix}1 & a & b\\0 & 1 & 0\\0 & 0 & 1\end{bmatrix}\begin{bmatrix}1 & c & d\\0 & 1 & 0\\0 & 0 & 1\end{bmatrix} = \varphi(a,b)\varphi(c,d).$$

Hence, φ is a homomorphism as well, and is therefore an isomorphism.

60. **Give an example of an infinite non-abelian group that has exactly six elements of finite order.**

Solution: We claim that $\mathbb{Z}\times S_3$ is an infinite non-abelian group with exactly six elements of finite order. First, it is clear that $\mathbb{Z} \times S_3$ is infinite since $\mathbb{Z}$ is infinite, and $\mathbb{Z} \times S_3$ is non-abelian since

$$(0,(1\,2))(0,(2\,3)) = (0,(1\,2\,3)) \neq (0,(1\,3\,2)) = (0,(2\,3))(0,(1\,2)).$$

Finally, the elements of finite order in $\mathbb{Z}\times S_3$ are precisely the elements of the form (a,σ) where a has finite order in $\mathbb{Z}$ and σ has finite order in S_3. The only element of finite order in $\mathbb{Z}$ is 0, and all 6 elements of S_3 have finite order, so there are exactly 6 elements of $\mathbb{Z} \times S_3$ of finite order (namely the elements of the form $(0,\sigma)$ for any $\sigma \in S_3$).

61. **Give an example to show that there exists a group with elements a and b such that $|a| = |b| = \infty$, but $|ab| = 2$.**

Solution: In $\mathbb{R}^*$, we have that 2 and $-\frac{1}{2}$ both have infinite order, but $-\frac{1}{2} \cdot 2 = -1$ has order 2. For an example that involves direct products, note that $(1,1), (-1,0) \in \mathbb{Z} \times \mathbb{Z}_2$ both have infinite order, but $(1,1) + (-1,0) = (0,1)$ has order 2.

69. **Use the results presented in this chapter to prove that $U(55)$ is isomorphic to $U(75)$.**

Solution: We have

$$\begin{aligned}
U(55) &\cong U(5) \times U(11) && \text{by Theorem 8.3, since 5 and 11 are coprime} \\
&\cong \mathbb{Z}_4 \times \mathbb{Z}_{10} && \text{by the paragraph at the bottom of page 161} \\
&\cong \mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_5 && \text{since } \mathbb{Z}_{10} \cong \mathbb{Z}_2 \times \mathbb{Z}_5 \text{ by Corollary 2 to Theorem 8.2} \\
&\cong \mathbb{Z}_2 \times \mathbb{Z}_{20} && \text{since } \mathbb{Z}_{20} \cong \mathbb{Z}_4 \times \mathbb{Z}_5 \text{ by Corollary 2 to Theorem 8.2} \\
&\cong U(3) \times U(25) && \text{by the paragraph at the bottom of page 161} \\
&\cong U(75) && \text{by Theorem 8.3, since 3 and 25 are coprime.}
\end{aligned}$$