8 Prove that if $GCD(a,m) = 1$ then the cyclic subgroup $\langle a \rangle$ of $\mathbb{Z}_m$ is the whole group.

Solution. We just need to show that $a$ is of order $m$. Suppose for a contradiction that $a$ is of order $n < m$, i.e. that $na \equiv 0 \pmod{m}$. Then $a$ is a non-zero zero divisor in $\mathbb{Z}_m$. But we know that $a$ is a unit since $GCD(a,m) = 1$, so this is a contradiction.

9 Prove that if $H, K \subset G$ are subgroups then $H \cap K$ is too.

Solution. Clearly $e \in H, e \in K$ since they are subgroups, so $e \in H \cap K$.

Take $h_1, h_2 \in H \cap K$. Then $h_1, h_2 \in H$ so since $H$ is a subgroup $h_1h_2 \in H$. Similarly, $h_1h_2 \in K$. Hence $h_1h_2 \in H \cap K$.

Take $h \in H \cap K$. Then $h \in H$ so $h^{-1} \in H$ since $H$ is a subgroup. Similarly, $h^{-1} \in K$. Hence $h^{-1} \in H \cap K$.

That is the three things we needed to check!

13 (a) Prove that every subgroup of a cyclic group is cyclic. (b) Prove that if $k | m$ then $\mathbb{Z}_m$ has a subgroup of order $k$. (c) If $a \in G$ has order $n$, prove that the order of $a^k$ is $\frac{n}{GCD(k,n)}$.

Solution. We proved (a) and (b) in class.

(c) To find the order of $a^k$, we need to find the smallest natural number $m$ such that $(a^k)^m = e$, i.e. $a^{km} = e$. Since $a$ has order $n$, this is equivalently the smallest natural number $m$ such that $n | km$.

Write

$$n = p_1^{a_1} \cdots p_r^{a_r}, \quad k = p_1^{b_1} \cdots p_r^{b_r},$$

where $p_1, \ldots, p_r$ are distinct primes and $a_1, \ldots, a_r, b_1, \ldots, b_r \geq 0$. Then it is obvious that the smallest $m$ such that $n | km$ is equal to

$$p_1^{a_1 - \min(a_1,b_1)} \cdots p_r^{a_r - \min(a_r,b_r)}.$$

Since

$$GCD(n,k) = p_1^{\min(a_1,b_1)} \cdots p_r^{\min(a_r,b_r)},$$

this is equal to $n/GCD(n,k)$.

17 I hope you were able to fill in the multiplication tables. There is only ONE answer in each case!!!

25 Find the orders of the groups $GL(2,\mathbb{Z}_p)$ and $SL(2,\mathbb{Z}_p)$.

Solution. $GL(2,\mathbb{Z}_p)$ is of order $(p^2 - 1)(p^2 - p)$, $SL(2,\mathbb{Z}_p)$ is of order $p(p^2 - 1)$.

• Exercises 6.2: 1,2,5(a)(b)(c).

1 Show that the Klein 4 group is not isomorphic to $\mathbb{Z}_4$. 

1
Proof. Its elements have order 1, 2, 2, 2 so there is no element of order 4 so it cannot be isomorphic to \( \mathbb{Z}_4 \).

2 Prove that \( \mathbb{Z}_2 \times \mathbb{Z}_7 \cong \mathbb{Z}_6 \).

Proof. The number \( 3 \in \mathbb{Z}_2 \times \mathbb{Z}_7 \) is of order 6. Hence it generates the whole group, and the whole group is cyclic of order 6. The exact isomorphism to \( \mathbb{Z}_6 \) would map \( 3 \mapsto 1, 2 \mapsto 2, 6 \mapsto 3, 4 \mapsto 4, 5 \mapsto 5, 1 \mapsto 0 \).

5(a) This is the Klein 4 group.
5(b) This is the cyclic group of order 4.
5(c) This is the quaternion group from p.173 Example 2(b).