Question 1

Show that S_3 is isomorphic to $\mathrm{Aut}(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})$.

Solution: Firstly, an automorphism of $K_4 \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} = \{0, 1, 2, 3\}$ must map $e \to e$. And as the rest of the elements are all of order 2, then it must map a non-trivial element 1 with either $1 \to 1, 2, 3$. Next, to maintain that the map is an isomorphism, it must map 2 to either $1, 2, 3$ with the condition that it must map 1 and 2 to different element. Therefore it must map 3 to the remaining element. This shows that $|\mathrm{Aut}(K_4)| \leq 6$

Next, consider a group S_3 that permutes element $\{1, 2, 3\}$ and the action of S_3 on K_4 such that $\sigma \cdot 0 = 0$ and $\sigma \cdot g = \sigma(g)$. Then the action is well defined as $\sigma \cdot \sigma' \cdot g = \sigma(\sigma'(g)) = \sigma \circ \sigma'(g)$ and $id \cdot g = g$. Now, the group action corresponds bijectively to a homomorphism from S_3 to $\mathrm{Aut}(K_4)$. The kernel of the homomorphism is the set $\{\sigma \mid \sigma g = g \forall g\} = \{id\}$. Lastly, as $|\mathrm{Aut}(K_4)| \leq 6$, it follows that the image of the homomorphism must be $\mathrm{Aut}(K_4)$ so lagrange's theorem holds. Therefore, by the first isomorphism theorem, $S_3 \simeq \mathrm{Aut}(K_4)$.

Question 2

A subgroup C of G is called characteristic if $f(C) = C$ for any automorphism f of G. Show that a characteristic subgroup C is normal in G.

Solution: As $\mathrm{Inn}(G) < \mathrm{Aut}(G)$, it holds that $f(C) = C$ for all $f \in \mathrm{Inn}(G)$. As $\mathrm{Inn}(G)$ is the group of all automorphism given by conjugation, and $f(C) = C$ for any $f \in \mathrm{Inn}(G)$, then C is normal by definition.

Question 3

Let $f, g : K \to \mathrm{Aut}(H)$ be two homomorphism. Assume that there exists an automorphism $\phi : K \to K$ such that $f = g \circ \phi$. Prove that the map $H \rtimes_g K \to H \rtimes_f K$ given by $(h, k) \mapsto (h, \phi^{-1}(k))$ is an isomorphism.

Solution: Consider a map $\psi : H \rtimes_g K \to H \rtimes_f K$ given by $\psi : (h, k) \mapsto (h, \phi^{-1}(k))$. Notice that $f(k) = g(\phi(k))$, and since f and g are automorphisms, $f(\phi^{-1}(k)) = g(k)$ for any k. Then,

$$\begin{aligned}
\psi((h, k)(h', k')) &= \psi((hg(k)(h'), kk')) \\
&= (hg(k)(h'), \phi^{-1}(kk')) \\
&= (hf(\phi^{-1}(k))(h'), \phi^{-1}(k)\phi^{-1}(k')) \\
&= (h, \phi^{-1}(k)) \cdot (h', \phi^{-1}(k')) \\
&= \psi(h, k) \cdot \psi(h', k')
\end{aligned}$$

shows that ψ is a homomorphism.

Furthermore, If $\psi((h, k)) = \psi((h', k'))$, then $(h, \phi^{-1}(k)) = (h', \phi^{-1}(k'))$. Thus, $h = h'$ and $k = k'$ as ϕ is an automorphism, which means that it is an isomorphism.

Lastly, $\mathrm{im}(\psi) = \{(h, k) \mid h \in H, k \in \mathrm{im}(\phi)\}$. However, as ϕ is an automorphism, then $\mathrm{im}(\phi) = K$. Thus, $\mathrm{im}(\psi) = \{(h, k) \mid h \in H, k \in K\} = H \rtimes_g K$.

As the map ψ is a homomorphism that is surjective and injective, then it is an isomorphism.

Question 4

Classify all groups of order 325 upto isomorphism.

Solution: Let G be a group of order $325 = 5^2 \cdot 13$. Assume that G is non-abelian. Then, consider the sylow 5-subgroup of G of order 25. The number of such subgroup satisfies $n_5 \equiv 1 \pmod 5$ and $n_5 | 13$, so $n_5 = 1$. Since there is a unique sylow 5-subgroup of G, then the group is normal. In the same way, the number of sylow 13-subgroup satisfies $n_{13} \equiv 1 \pmod{13}$ and $n_{13} | 25$, so $n_1 3 = 1$ or 26. However, if there is also a unique sylow 13-subgroup of G, then G must be abelian as all of sylow subgroups are unique. Thus, $n_1 3 = 26$. Now, since all sylow 13-subgroup are cyclic, then they intersect trivially, so there must be $12 \times 26 = 312$ elements of order 13 in G.

Now, the unique sylow 5-subgroup contains 24 elements, none of which has order 13 by lagrange's theorem. So, G must contains at least $312 + 24 = 336$ non-trivial elements, which is not possible. This concludes that G must be abelian.

Consider that if G is abelian, then by the fundamental theorem of finite abelian group,

$$G \simeq \mathbb{Z}/325\mathbb{Z} \text{ or } G \simeq \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/65\mathbb{Z}$$

This is because $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \simeq \mathbb{Z}/pq\mathbb{Z}$ if $\gcd(p, q) = 1$.

Moreover, $\mathbb{Z}/325\mathbb{Z}$ and $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/65\mathbb{Z}$ is not isomorphism as the first one is cyclic but the latter is not.

To conclude, they are only two groups of order 325 upto isomorphism.

Question 5

A ring R is called a Boolean ring if $a^2 = a$ for all $a \in R$. Prove that every Boolean ring is commutative. And prove that only Boolean ring that is an integral domain is $\mathbb{Z}/2\mathbb{Z}$.

Solution: Let a and b be two elements in R. Then $a + b \in R$ by closure, hence $a + b = (a + b)^2 = a^2 + ab + ba + b^2 = a+ab+ba+b$. This shows that $ab+ba = 0$, so, $ab = -ba$. But, $ab \in R$ by closure, so $ab+ab = (ab+ab)^2 = ab+ab+ab+ab$, which is that $ab + ab = 0$, or $ab = -ab$. Therefore, $-ab = -ba$, or equivalently, $ab = ba$ for every a and b in R.

Now, as $a^2 = a$, then $a(a - 1) = a^2 - a = 0$. If there exist two non-zero elements a and $(a - 1)$, then R is not an integral domain. That is equivalent to saying that if there is a non-zero element x such that $x + 1$ is also non-zero, then R would not be an integral domain. But since 1 is not the additive identity, if there is at least 3 elements in R, then there must be an element that is non-zero and that is not the inverse of 1. Consider that the element, say, x satisfies that $x + 1 \neq 0$ and $x \neq 0$. So, $(x + 1)(x + 1 - 1) = (x + 1)^2 - (x + 1) = 0$ shows that $(x + 1)$ is a zero-divisor.

For the case of $R = \mathbb{Z}/2\mathbb{Z}$, it is trivial to check that $1 \cdot 1 = 1^2 = 1 \neq 0$, since 1 is the only non-zero element.

Question 6

Let R be a ring with an identity. Prove that the center $\{\, z \in R \mid zr = rz \text{ for all } r \in R \,\}$ of R is a subring that contains the identity. And prove that the center of a division ring is a field.

Solution: Let $Z = \{\, z \in R \mid zr = rz \text{ for all } r \in R \,\}$ be the center of R. Then, for $z, z' \in Z$, the sum $z + z'$ satisfies $(z + z')r = zr + z'r = rz + rz' = r(z + z')$. So, $(z + z') \in Z$. Also, inverse $-z$ satisfies $(-z)r = -zr = -rz = r(-z)$. So, $(-z) \in Z$. In addition, the product zz' also satisfies $zz'r = zrz' = rzz'$, so $(zz') \in Z$. This shows that Z is a subring of R. In addition, $1 \in R$ since $1r = r = r1$ for every $r \in R$ by definition.

Next, if R is a division ring, then any element in R has an inverse. The center Z contains the element that is commutative over the multiplicative operation and that Z is subring implies that Z is a commutative ring. Moreover, since any element in R has an inverse, any element in Z must have an inverse. Therefore, Z is a commutative division ring, which proves that Z is a field.

Question 7

Let x be a nilpotent element (i.e. $x^m = 0$ for some $m \in \mathbb{Z}^+$) of the commutative ring R with an identity. Prove that x is either zero or a zero divisor.

Solution: Assume that $x \neq 0$, then let m be the least integer such that $x^m = 0$, so that $x^{m-1} \neq 0$. Then $x \cdot x^{m-1} = x^m = 0$ where neither x nor x^{m-1} is zero. So, x is a zero divisor.

Therfore, $x = 0$ or x is a zero divisor must holds.

Question 8

Let x be a nilpotent element (i.e. $x^m = 0$ for some $m \in \mathbb{Z}^+$) of the commutative ring R with an identity. Prove that $1 + rx$ is a unit in R for all $r \in R$.

Solution: For any element x, consider an integer m such that $x^m = 0$. If m is even, then consider $x^{m+1} = x^m \cdot x = 0$.

Now,

$$1 = 1 + r^m x^m = 1 + (rx)^m = (1 + rx)(1 - rx + (rx)^2 - \cdots + (rx)^{m-1})$$

. holds for any value of r as $x^m = 0$. Then $(1 + rx)^{-1} = (1 - rx + (rx)^2 - \cdots + (rx)^{m-1})$ by definition. Hence, $(1 + rx)$ is invertible.

Question 9

Let $K = \mathbb{Q}$ and let p be a prime integer. For any $x \in \mathbb{Q}$, we can write uniquely as $x = p^n \frac{c}{d}$ where $p \nmid c$ and $p \nmid d$. Define $v_p(x) = n$. Prove that v_p is a discrete valuation on K.

Solution: Define v_p as in the problem statement. Note that since $x = p^n \frac{c}{d}$ is a unique representation (according to the fundamental theorem of arithmetric), then v_p is well-defined.

Let $x = p^n \frac{a}{b}$, and $y = p^m \frac{c}{d}$, where p does not divide any of a, b, c, d. Without loss of generality, let $n < m$.

Consider $v_p(xy) = v_p(p^n \frac{a}{b} p^m \frac{c}{d}) = v_p(p^{n+m} \frac{ac}{bd})$ where $p \nmid ac$ and $p \nmid bd$. So, $v_p(xy) = n + m = v_p(x) + v_p(y)$

Next, consider $v_p(x + y) = v_p(\frac{p^n a}{b} + \frac{p^m c}{d}) = v_p(\frac{p^n ad + p^m cb}{bd} = p^n \frac{ad + p^{m-n} cb}{bd})$. So $v_p(x + y) = v_p(p^n) + v_p(\frac{ad + p^{m-n} cb}{bd}) \geq n = \min(n, m) = \min(v_p(x), v_p(y))$.

Thus, v_p is a discrete valuation on K.

Question 10

In problem 9, prove that the ring of all rational numbers whose denominators are relatively prime to p is a discrete valuation ring.

Solution: As $v_p : p^n \frac{a}{c} \mapsto n$ is a discrete valuation on $\mathbb{Q}$, then $\mathbb{Q}_v = \{ a \in \mathbb{Q}^\times \mid v_p(a) \leq 0 \} \cup \{ 0 \}$ is a discrete valuation ring by definition.

Consider that for a rational number r in its simplest form that the denominator is divisible by p, then $r = \frac{a}{p^n b}$ for some positive integer n, and a, b relatively prime to p. Thus, $v_p(r) = -n < 0$.

Otherwise, if the denominator is not divisible by p, then $f = \frac{p^n a}{b}$ for some non-negative integer n, and a, b relatively prime to p. Thus, $v_p(r) = n \geq 0$.

So, $\mathbb{Q}_v = \left\{ \frac{c}{d} \in \mathbb{Q}^\times \mid d \text{ is not divisible by } p \right\} \cup \{ 0 \}$. Hence, the set of all rational numbers whose denominators are relatively prime to p is a discrete valuation ring.