Final Practice: Solutions II

1. Practice with definitions.

(a) Give the definition of a group.

Solution. A **group** $(G, \star)$ is a set G with binary operation $\star$ such that

- $\star$ is associative: $(a \star b) \star c = a \star (b \star c)$ for all $a, b, c \in G$
- There exists an identity element $e \in G$ such that $e \star a = a \star e = a$ for all $a \in G$.
- There exist inverse elements: for all $a \in G$, there exists $a' \in G$ such that $a \star a' = a' \star a = e$.

(b) Give the definition of a cyclic group.

Solution. A group G is **cyclic** if there is some element a that generates G, i.e. $G = \langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$.

(c) Give the definition of an abelian group.

Solution. A group G is **abelian** if its binary operation is commutative. (Alternative: a group is abelian if, for all $a, b \in G$, $ab = ba$.)

(d) Give the definition of a subgroup.

Solution. A **subgroup** H of a group G is a subset of G that

- is closed under the binary operation in G, i.e. for any $a, b \in H$, $ab \in H$,
- contains the identity element $e \in G$, i.e. $e \in H$, and
- for any $a \in H$, $a^{-1} \in H$.

(e) Let G be a group. Give the definition of the order of G, $|G|$.

Solution. The **order** of G is the number of elements in (or cardinality of) G.

(f) Let G be a group and let $a \in G$. Give the definition of the order of a.

Solution. The **order** of a if the order of $|\langle a \rangle|$. Alternatively, it is the minimal $n \in \mathbb{Z}$, $n > 0$ such that $a^n = e$. If no such n exists, we say the order is infinite.

(g) Let A be a set. Give the definition of a permutation of A.

Solution. A **permutation** of A is an onto and one-to-one function $\sigma : A \to A$.

(h) Give the definition of the symmetric group.

Solution. The **symmetric group** S_n is the set of permutations of $A = \{1, 2, 3, \ldots, n\}$ with binary operation composition.

(i) Give the definition of the alternating group.

Solution. The **alternating group** A_n is the collection of all even permutations in S_n with binary operation composition.

(j) Give the definition of the dihedral group.

Solution. The **dihedral group** D_n is the set of symmetries of the regular n-gon with binary operation composition.

(k) Let H be a subgroup of a group G. Give the definition of a left coset of H.

Solution. If H is a subgroup of a group G, a **left coset** of H is a subset of the form $\{ah \mid h \in H\}$ for some element $a \in G$.

Alternatively, an acceptable answer is: if H is a subgroup of a group G, the left coset of H containing an element $a \in G$ is the subset $aH = \{ah \mid h \in H\}$.

(l) Let G_1 and G_2 be groups. Give the definition of the direct product group $G_1 \times G_2$.

Solution. Let G_1 and G_2 be groups. Define the set $G_1 \times G_2 = \{(g_1, g_2) \mid g_1 \in G_1, g_2 \in G_2\}$. For any $(g_1, g_2), (h_1, h_2) \in G_1 \times G_2$, define a binary operation on $G_1 \times G_2$ by $(g_1, g_2) \times (h_1, h_2) = (g_1 h_1, g_2 h_2)$. The **direct product** of G_1 and G_2 is the set $G_1 \times G_2$ with this binary operation.

(m) Give the definition of a normal subgroup.

Solution. A subgroup H of a group G is a **normal subgroup** if, for any $h \in H$, for all $g \in G$, $ghg^{-1} \in H$.

(n) Let H be a normal subgroup of a group G. Give the definition of the quotient group G/H.

Solution. The **quotient group** G/H is the set of cosets of H in G with binary operation $(aH)(bH) = (ab)H$.

(o) Give the definition of a homomorphism from G to G'.

Solution. A **homomorphism** is a function $\phi : G \to G'$ such that, for all $a, b \in G$, $\phi(ab) = \phi(a)\phi(b)$.

(p) Give the definition of an isomorphism from G to G'.

Solution. An **isomorphism** is a homomorphism $\phi : G \to G'$ that is onto and one-to-one.

(q) Let $\phi : G \to G'$ be a homomorphism. Give the definition of the kernel of ϕ, $\ker \phi$.

Solution. The **kernel** of ϕ is the set $\ker \phi = \{g \in G \mid \phi(g) = e'\}$.

(r) Let $\phi : G \to G'$ be a homomorphism and let H be a subgroup of G. Give the definition of the image of H, $\phi[H]$.

Solution. The **image** of H is the set $\phi[H] = \{g' \in G' \mid g' = \phi(h) \text{ for some } h \in H\}$.

(s) Let $\phi : G \to G'$ be a homomorphism and let H' be a subgroup of G'. Give the definition of the inverse image of H', $\phi^{-1}[H']$.

Solution. The **inverse image** of H' is the set $\phi^{-1}[H'] = \{g \in G \mid \phi(g) \in H'\}$.

(t) Give the definition of a simple group.

Solution. A **simple group** is a group G with no proper, nontrivial normal subgroups.

(u) Give the definition of a group action of G on a set X.

Solution. Let X be a set and let G be a group. An **action of** G **on** X is a function $\star : G \times X \to X$ such that

- $e \star x = x$ for all $x \in X$, and
- $(g_1 g_2) \star x = g_1 \star (g_2 \star x)$ for all $g_1, g_2 \in G$ and $x \in X$.

(v) Let G be a group acting on a set X and let $x \in X$. Give the definition of the stabilizer of x, G_x.

Solution. The **stabilizer of** x is the set $G_x = \{g \in G \mid g \star x = x\}$.

(w) Let G be a group acting on a set X and let $x \in X$. Give the definition of the orbit of x, $G \cdot x$.

Solution. The **orbit of** x is the set $G \cdot x = \{y \in X \mid y = g \star x \text{ for some } g \in G\}$.

(x) Let G be a group acting on a set X and let $g \in G$. Give the definition of the fixed points of g, X_g.

Solution. Tthe **fixed points of** g is the set $X_g = \{x \in X \mid g \star x = x\}$.

2. Practice with big theorems. These are things you can state and use on the exam without proving them.

(a) State the classification of subgroups of finite cyclic groups $\mathbb{Z}_n$.

Solution. All subgroups of $\mathbb{Z}_n$ are of the form $\langle a \rangle$. The subgroup $\langle a \rangle$ has n/d elements, where $d = \gcd(n, a)$ and this *uniquely determines the subgroup*: $\langle a \rangle = \langle b \rangle$ if and only if $\gcd(n, a) = \gcd(n, b)$, so there is exactly one subgroup of $\mathbb{Z}_n$ corresponding to each divisor of n.

(b) State Cayley's Theorem.

Solution. Every group is isomorphic to a subgroup of a permutation group.

(c) State Lagrange's Theorem.

Solution. Let G be a finite group and let H be a subgroup of G. Then, $|G| = |H|(G : H)$. In particular, $|H|$ divides $|G|$.

(d) State the Fundamental Homomorphism Theorem.

Solution. Let $\phi : G \to G'$ be any homomorphism. Then, $G/\ker\phi \cong \phi[G]$.

3. Practice with explicit groups and properties.

(a) Is $(\mathbb{Z}, \star)$ a group, where $a \star b = a - b$?

Solution. This is not a group because $a \star b$ is not associative: $a \star (b \star c) = a - (b - c) = a - b + c$, but $(a \star b) \star c = (a - b) - c = a - b - c$. If $c \neq 0$, then $a \star (b \star c) \neq (a \star b) \star c$.

(b) Is $(\mathbb{Q}, \star)$ a group, where $a \star b = ab/2$?

Solution. This is a not group. The identity must be 2 because because, for any element $a \in \mathbb{Q}$, $a \star 2 = 2 \star a = a$. But, if the identity is 2, $0 \in \mathbb{Q}$ has no inverse because $0 \star a = 0 \neq 2$.

(c) Find all subgroups of the group $\mathbb{Z}_{10}$ and give all possible generators for each subgroup.

Solution. The divisors of 10 are $1, 2, 5, 10$, and the subgroup $\langle a \rangle$ is generated by any element b such that $\gcd(10, a) = \gcd(10, b)$, so the subgroups are:

- $\langle 1 \rangle = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ generated by $1, 3, 7$, or 9.
- $\langle 2 \rangle = \{0, 2, 4, 6, 8\}$ generated by $2, 4, 6$ or 8.
- $\langle 5 \rangle = \{0, 5\}$ generated by 5.
- $\langle 0 \rangle = \{0\}$ generated by 0.

(d) Find all subgroups of the group $\mathbb{Z}_{12}$ and give all possible generators for each subgroup.

Solution. As above, we get the following:

- $\langle 1 \rangle = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$ generated by $1, 5, 7$, or 11.
- $\langle 2 \rangle = \{0, 2, 4, 6, 8, 10\}$ generated by 2 or 10.
- $\langle 3 \rangle = \{0, 3, 6, 9\}$ generated by 3 or 9.
- $\langle 4 \rangle = \{0, 4, 8\}$ generated by 4 or 8
- $\langle 6 \rangle = \{0, 6\}$ generated by 6
- $\langle 0 \rangle = \{0\}$ generated by 0.

(e) Give all possible generators of $M_9 = \{a \in \mathbb{Z}_9 \mid \gcd(a, 9) = 1\}$.

Solution. The elements of M_9 are $M_9 = \{1, 2, 4, 5, 7, 8\}$. To determine the generators, we can ask about the subgroup generated by each element (recalling that the binary operation here is *multiplication*, not addition):

- $\langle 1 \rangle = \{1\}$
- $\langle 2 \rangle = \{2, 4, 8, 7, 5, 1\} = M_9$
- $\langle 4 \rangle = \{4, 7, 1\}$
- $\langle 5 \rangle = \{5, 7, 8, 4, 2, 1\} = M_9$
- $\langle 7 \rangle = \{7, 4, 1\}$
- $\langle 8 \rangle = \{8, 1\}$

Looking at the list, we see that the only elements that generate all of M_9 are 2 and 5.

(f) Let $D = \{\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \mid a, b \in \mathbb{R}, ab \neq 0\}$. Is D a subgroup of $GL_2(\mathbb{R})$? Is D a normal subgroup of $GL_2(\mathbb{R})$?

Solution. D is a subgroup of $GL_2(\mathbb{R})$. We check the properties:

- Closed? If $A_1 = \begin{bmatrix} a_1 & 0 \\ 0 & b_1 \end{bmatrix}$, $a_1 b_1 \neq 0$, and $A_2 = \begin{bmatrix} a_2 & 0 \\ 0 & b_2 \end{bmatrix}$, $a_2 b_2 \neq 0$, then $A_1 A_2 = \begin{bmatrix} a_1 a_2 & 0 \\ 0 & b_1 b_2 \end{bmatrix}$ and $a_1 a_2 b_1 b_2 \neq 0$, so $A_1 A_2 \in D$.
- Identity? $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ so $I \in D$.
- Inverses? If $A = \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$, $ab \neq 0$, then $A^{-1} = \begin{bmatrix} 1/a & 0 \\ 0 & 1/b \end{bmatrix}$ so $A^{-1} \in D$.

Therefore, D is a subgroup.

However, D is not a normal subgroup. For it to be normal, we must have $BAB^{-1} \in D$ for any matrix $A \in D$ and $B \in GL_2(\mathbb{R})$. However, this is false: if $A = \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$ and $B = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$, then $B^{-1} = \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix}$, so $BAB^{-1} = \begin{bmatrix} a & -a+b \\ 0 & b \end{bmatrix}$. If $a \neq b$, then $BAB^{-1} \notin D$.

(g) Let $\sigma = (123)(45) \in S_6$. What is the order of σ?

Solution. The order of σ is the least common multiple of the lengths of the cycles, so the order of $\sigma = 6$.

(h) Let $\sigma = (123)(45) \in S_6$. What is σ^{-1}?

Solution. We compute the inverse as $\sigma^{-1} = (132)(45)$.

(i) Let $\sigma = (123)(45)$ and let $\tau = (235)$. What is $\sigma\tau$?

Solution. We compute $\sigma\tau = (12)(345)$.

(j) What is the order of the element $(2, 5)$ in $\mathbb{Z}_4 \times \mathbb{Z}_{15}$?

Solution. In a direct product $G_1 \times G_2$, the order of the element (g_1, g_2) is equal to the least common multiple of the order of g_1 and the order of g_2. So, $\text{ord}(2, 5) = \text{lcm}(2, 3) = 6$.

(k) What is the order of the element $(2, 5)$ in $\mathbb{Z}_3 \times \mathbb{Z}_8$?

Solution. As above, $\text{ord}(2, 5) = \text{lcm}(3, 8) = 24$.

(l) Prove that D_5 is not isomorphic to a subgroup of S_4.

Solution. Lagrange's Theorem says that, for any group G and subgroup H, $|H|$ divides $|G|$. Because $|D_5| = 10$ and $|S_4| = 24$, and 10 does not divide 24, D_5 cannot be isomorphic to a subgroup of S_4.

(m) List the left cosets of $H = \langle(12)\rangle$ in S_3. Are the left cosets equal to the right cosets?

Solution. We list the left cosets:

- $H = \{\iota, (12)\}$
- $(13)H = \{(13), (123)\}$
- $(23)H = \{(23), (132)\}$

The right cosets are:

- $H = \{\iota, (12)\}$
- $H(13) = \{(13), (132)\}$
- $H(23) = \{(23), (123)\}$

These are not equal: $(13)H \neq H(13)$ and $(23)H \neq H(23)$.

(n) Show that $\phi : \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ given by $\phi(n) = (n, 2n)$ is a homomorphism. What is $\ker \phi$? What is $\phi[\mathbb{Z}]$?

Solution. To check that ϕ is a homomorphism, we must check that $\phi(n + m) = \phi(n) + \phi(m)$. We compute:

$$\phi(n + m) = (n + m, 2(n + m))$$

and

$$\phi(n) + \phi(m) = (n, 2n) + (m, 2m) = (n + m, 2n + 2m).$$

These are equal, so ϕ is a homomorphism.

Then, we compute $\ker \phi = \{n \in \mathbb{Z} \mid \phi(n) = (0, 0)\}$. Because $\phi(n) = (n, 2n)$ is $(0, 0)$ if and only if $n = 0$, we see that $\ker \phi = \{0\}$.

Finally, $\phi[\mathbb{Z}] = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid \phi(n) = (a, b)\}$, and all possible outputs of ϕ are of the form $(n, 2n)$, so $\phi[\mathbb{Z}] = \{(n, 2n) \mid n \in \mathbb{Z}\}$.

(o) Show that $\phi : M_2(\mathbb{R}) \to \mathbb{R}$ given by $\phi(\begin{bmatrix} a & b \\ c & d \end{bmatrix}) = a + d$ is a homomorphism. What is $\ker \phi$?

Solution. The binary operation in $M_2(\mathbb{R})$ is addition, so we need to check that $\phi(A+B) = \phi(A)+\phi(B)$. If $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ and $B = \begin{bmatrix} e & f \\ g & h \end{bmatrix}$, then

$$\phi(A + B) = \phi\left(\begin{bmatrix} a + e & b + f \\ c + g & d + h \end{bmatrix}\right) = a + e + d + h$$

and

$$\phi(A) + \phi(B) = a + d + e + h.$$

These are equal, so ϕ is a homomorphsim.
Then, $\ker\phi = \{A \in M_2(\mathbb{R}) \mid \phi(A) = 0\}$, and $\phi(A) = a + d = 0$ if and only if $d = -a$, so $\ker\phi = \{A \in M_2(\mathbb{R}) \mid A = \begin{bmatrix} a & b \\ c & -a \end{bmatrix}\}$.

(p) Let $G = \mathbb{Z}_8$. List the cosets of $H = \{0, 4\}$. Find a group G' and homomorphism $\phi : G \to G'$ such that $\ker\phi = H$ and use it to determine to what group G/H is isomorphic.

Solution. The cosets are: $H = \{0, 4\}$, $1 + H = \{1, 5\}$, $2 + H = \{2, 6\}$, and $3 + H = \{3, 7\}$.
Let $G' = \mathbb{Z}_4$. Then, the function $\phi : \mathbb{Z}_8 \to \mathbb{Z}_4$ given by $\phi(n) = n \mod 4$ is a homomorphism (you should know how to prove this!) and $\ker\phi = \{n \in \mathbb{Z}_8 \mid n = 0 \mod 4\} = \{0, 4\} = H$. Because ϕ is onto, $\phi[\mathbb{Z}_8] = \mathbb{Z}_4$, so the Fundamental Homomorphism Theorem tells us that $\mathbb{Z}_8/H \cong \mathbb{Z}_4$.

(q) Let $G = \mathbb{Z}\times\mathbb{Z}$ and let $H = \langle(-1, 1)\rangle$. List the cosets of H in G. Find a homomorphism $\phi : G \to \mathbb{Z}$ with $\ker\phi = H$, and use it to determine to what group G/H is isomorphic.

Solution. The cosets are:

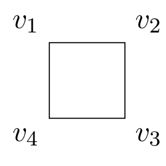
$$\begin{aligned}
H &= \{\dots, (-1, 1), (-2, 2), (-3, 3), (-4, 4), \dots\} \\
(1, 0) + H &= \{\dots, (0, 1), (-1, 2), (-2, 3), (-3, 4), \dots\} \\
(2, 0) + H &= \{\dots, (1, 1), (0, 2), (-1, 3), (-2, 4), \dots\} \\
(3, 0) + H &= \{\dots, (2, 1), (1, 2), (0, 3), (-1, 4), \dots\} \\
&\vdots \\
(n, 0) + H &= \{\dots, (n - 1, 1), (n - 2, 2), (n - 3, 3), (n - 4, 4), \dots\} \\
&\vdots
\end{aligned}$$

The elements in the coset $(a, 0) + H$ are all pairs $(n, m) \in \mathbb{Z} \times \mathbb{Z}$ such that $n + m = a$.
Let $\phi : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ be given by $\phi(n, m) = n + m$. Then,

$$\ker\phi = \{(n, m) \mid n + m = 0\} = \{(n, m) \mid n = -m\} = H$$

and ϕ is onto, so the Fundamental Homomorphism Theorem says $\mathbb{Z} \times \mathbb{Z}/H \cong \mathbb{Z}$.

(r) Let $X = \{v_1, v_2, v_3, v_4\}$ be the vertices of the square:



D_4 acts on X. What is G_{v_2}?

Solution. CONVENTION: $D_4 = \{e, r, r^2, r^3, f, fr, fr^2, fr^3\}$ where r is rotation 90 degrees clockwise, f is the flip across the vertical axis of symmetry, and fr^i means first do r^i, then do f. With this convention, $G_{v_2} = \{g \in D_4 \mid g \star v_2 = v_2\}$. We check the different elements and find that $G_{v_2} = \{e, fr^3\}$. (If you use a different convention, you may get a different answer.)

(s) Let $X = \mathbb{Z}\times\mathbb{Z}$ and let $G = \mathbb{Z}$. Is the function $G\star X$ given by $a\star(n,m) = (n+a, m-a)$ a group action? What is $G\cdot(1,1)$?

Solution. We check that this is a group action: first, $0\star(n,m) = (n+0, m-0) = (n,m)$. Second, we need that $(a+b)\star(n,m) = a\star(b\star(n,m))$, so we check: $(a+b)\star(n,m) = (n+a+b, m-(a+b))$ and $a\star(b\star(n,m)) = a\star(n+b, m-b) = (n+b+a, m-b-a)$. These are equal, so this is a group action.

Then, $G\cdot(1,1)$ is the orbit of $(1,1)$, so all possible elements of the form $(1+a, 1-a)$. You can leave it at that: $G\cdot(1,1) = \{(1+a, 1-a) \mid a \in \mathbb{Z}\}$, or, for a more geometric description, note that this takes the point $(1,1)$ and shifts the x coordinate up by a and the y coordinate down by a. If you draw a picture of these, you will see that these elements are those on the line $y = 2-x$.

4. Practice with proofs.

(a) If G is abelian and $\phi : G \to G'$ is an onto homomorphism, prove that G' is abelian. Give an example to show that this is false if ϕ is not onto.

Solution. Let g, h be elements of G'. We must show that $gh = hg$. Because ϕ is onto, there is an element $a \in G$ such that $\phi(a) = g$ and there is an element $b \in G$ such that $\phi(b) = h$. Therefore,

$$\begin{aligned} gh &= \phi(a)\phi(b) \\ &= \phi(ab) \quad \text{because } \phi \text{ is a homomorphism} \\ &= \phi(ba) \quad \text{because } G \text{ is abelian} \\ &= \phi(b)\phi(a) \\ &= hg \end{aligned}$$

so $gh = hg$ and G' is abelian.

If ϕ is not onto, this is false. For example, D_3 is not abelian. Let $H = \langle r\rangle = \{e, r, r^2\}$. H is abelian because H is cyclic, but there is a homomorphism $\phi : H \to D_3$ just given by $\phi(h) = h$, but D_3 is not abelian.

(b) If G is a group such that $x^2 = e$ for all $x \in G$, prove that G is abelian.

Solution. Let x, y be elements of G. We must show that $xy = yx$. By assumption, $xy \in G$ so $(xy)^2 = e$, so $xyxy = e$. Multiplying both sides by x on the left and using that $x^2 = e$, we get $yxy = x$. Now, multiply both sides on the left by y and use that $y^2 = e$ to get $xy = yx$. Hence, G is abelian.

(c) For sets H and K, define the intersection $H \cap K$ to be

$$H \cap K = \{x \mid x \in H \text{ and } x \in K\}.$$

Show that if H and K are subgroups of a group G, then $H \cap K$ is a subgroup of G. Furthermore, show that if H and K are normal, then $H \cap K$ is normal.

Solution. Because H and K are subgroups, they both contain e, so $e \in H \cap K$. For any $a \in H \cap K$, because H and K are subgroups, $a^{-1} \in H$ and $a^{-1} \in K$, so $a^{-1} \in H \cap K$. For any $a, b \in H \cap K$, because H and K are subgroups, $ab \in H$ and $ab \in K$, so $ab \in H \cap K$. Therefore, $H \cap K$ is a subgroup.

To show that it is normal, let $h \in H \cap K$ and let $g \in G$. Because H and K are normal, $ghg^{-1} \in H$ and $ghg^{-1} \in K$, so $ghg^{-1} \in H \cap K$. Therefore, $H \cap K$ is normal.

(d) Let G_1 and G_2 be groups and let $G_1 \times G_2$ be the direct product. Prove that, if $|G_1| = p$ and $|G_2| = q$, where p and q are distinct prime numbers, then $G_1 \times G_2$ is cyclic.

Solution. Let $a \in G_1$ and $b \in G_2$ be non-identity elements. By Lagrange's Theorem, the order of any element divides the order of the group. Because they are non-identity elements, their order is > 1, so we must have $\text{ord}a = p$ and $\text{ord}b = q$. Then, $\text{ord}(a, b) = \text{lcm}(p, q)$, but p and q are distinct prime numbers, so $\text{lcm}(p, q) = pq$. Therefore, $\langle(a, b)\rangle = pq$, but $G_1 \times G_2$ has exactly pq elements, so $\langle(a, b)\rangle = G_1 \times G_2$ and hence $G_1 \times G_2$ is cyclic.

(e) Let G_1, G_2 be groups and let $\phi : G_1 \times G_2 \to G_1$ be the function $\phi(g_1, g_2) = g_1$. Prove that ϕ is a homomorphism and prove that $\ker \phi \cong G_2$.

Solution. We first show that ϕ is a homomorphism. If (g_1, g_2) and (h_1, h_2) are elements of $G_1 \times G_2$, then $\phi(g_1h_1, g_2h_2) = g_1h_1 = \phi(g_1, g_2)\phi(h_1, h_2)$, so ϕ is a homomorphism.

Then, $\ker \phi = \{(g_1, g_2) \mid \phi(g_1, g_2) = e_1\}$, so $\ker \phi = \{(e_1, g_2) \in G_1 \times G_2\}$. To show this is isomorphic to G_2, consider the function $\psi : G_2 \to \ker \phi$ given by $\psi(g_2) = (e_1, g_2)$. We can check that ψ is a homomorphism, and it is onto and one-to-one, so ψ is an isomorphism.

(f) Let G and G' be finite groups and let $\phi : G \to G'$ be a group homomorphism. Show that $|\phi[G]|$ divides $|G|$ and $|G'|$. Using this, determine all homomorphisms $\phi : \mathbb{Z}_r \to \mathbb{Z}_s$ where $\gcd(r, s) = 1$.

Solution. By the Fundamental Homomorphism Theorem, $\phi[G] \cong G/\ker \phi$, so $|\phi[G]| = |G/\ker \phi|$. Because $\ker \phi$ is a subgroup of G and $|G/\ker \phi|$ is the number of cosets of $\ker \phi$, by Lagrange's Theorem, we know that $|G| = |\ker \phi||G/\ker \phi|$. In particular, $|G/\ker \phi|$ divides $|G|$, so $|\phi[G]|$ divides $|G|$. Because $\phi[G]$ is a subgroup of G', Lagrange's Theorem also says that $|\phi[G]|$ divides $|G'|$.

Now, let us apply this to $\phi : \mathbb{Z}_r \to \mathbb{Z}_s$ when $\gcd(r, s) = 1$. Let $H = \phi[\mathbb{Z}_r]$. The previous paragraph shows that $|H|$ divides r and $|H|$ divides s, but $\gcd(r, s) = 1$, so $|H| = 1$. Because H is a subgroup, we know $0 \in H$, so $|H| = 1$ implies that $H = \{0\}$. Therefore, $\phi[\mathbb{Z}_r] = \{0\}$, so any homomorphism $\phi : \mathbb{Z}_r \to \mathbb{Z}_s$ must be the trivial homomorphism $\phi(a) = 0$.

(g) Let $\phi : G \to G'$ be any group homomorphism. Prove that $\ker \phi$ is a subgroup of G and that $\ker \phi$ is a normal subgroup of G.

Solution. By definition, $\ker \phi = \{g \in G \mid \phi(g) = e'\}$. Because ϕ is a homomorphism, $\phi(e) = e'$, so $e' \in \ker \phi$. If $h \in \ker \phi$, then $\phi(h) = e'$. Therefore, $e' = \phi(e) = \phi(hh^{-1}) = \phi(h)\phi(h^{-1}) = \phi(h^{-1})$, so $\phi(h^{-1}) = e'$ and $h^{-1} \in \ker \phi$. Finally, we must show that $\ker \phi$ is closed. Given any $h_1, h_2 \in \ker \phi$, $\phi(h_1h_2) = \phi(h_1)\phi(h_2) = e'e' = e'$, so $h_1h_2 \in \ker \phi$. Therefore, $\ker \phi$ is a subgroup.

To prove that $\ker \phi$ is normal, let h be any element of $\ker \phi$ and $g \in G$. We must prove that $ghg^{-1} \in \ker \phi$. Because ϕ is a homomorphism, $\phi(ghg^{-1}) = \phi(g)\phi(h)\phi(g)^{-1}$. Because $h \in \ker \phi$, this implies $\phi(ghg^{-1}) = \phi(g)\phi(g)^{-1} = e'$, so $ghg^{-1} \in \ker \phi$. Hence, $\ker \phi$ is normal.

(h) Let $\phi : G \to G'$ be an onto homomorphism. Let N be a normal subgroup of G. Show that $\phi[N]$ is a normal subgroup of G'.

Solution. Let $h' \in \phi[N]$ be any element and let $g' \in G'$. We must show that $g'h'g'^{-1} \in \phi[N]$. Because $h' \in \phi[N]$, $h' = \phi(h)$ for some $h \in N$, and because ϕ is onto, $g' = \phi(g)$ for some $g \in G$. Because ϕ is a homomorphism, $g'h'g'^{-1} = \phi(ghg^{-1})$, but N is normal, so $ghg^{-1} \in N$, and therefore $g'h'g'^{-1} \in \phi[N]$.

(i) For $n \geq 2$, prove that S_n is not a simple group.

Solution. Let $H = A_n$. We will show that A_n is normal. Let $\sigma \in A_n$ be an even permutation and let $\tau \in S_n$ be any permutation. If τ is even, τ^{-1} is also even, so $\tau\sigma\tau^{-1}$ is even (even + even + even = even). If τ is odd, τ^{-1} is also odd, hence $\tau\sigma\tau^{-1}$ is even (odd + even + odd = even). Hence, for any τ, $\tau\sigma\tau^{-1} \in A_n$. Therefore, S_n contains a proper nontrivial normal subgroup, so S_n is not simple.