ABSTRACT ALGEBRA I FINAL SAMPLE

MARIO L. GUTIERREZ ABED

Problem 1. (5 pts each)

a) Define a group / abelian group / cyclic group / simple group / normal subgroup of a group.

Group

A **group** $\langle G, * \rangle$ is a set G, closed under a binary operation $*$, such that the following axioms are satisfied:

- $\mathcal{G}_1$: For all $a, b, c \in G$, we have
$$(a * b) * c = a * (b * c) \quad \text{(associativity of } *)$$
- $\mathcal{G}_2$: There is an element $e \in G$ such that for all $x \in G$,
$$e * x = x * e = x. \quad \text{(identity element } e \text{ for } *)$$
- $\mathcal{G}_3$: Corresponding to each $a \in G$, there is an element $a' \in G$ such that
$$a * a' = a' * a = e. \quad \text{(inverse } a' \text{ of } a)$$

Abelian Group

A group G is said to be **abelian** if its binary operation $*$ is commutative, that is, if for any two elements $x, y \in G$, we have $x * y = y * x$.

Cyclic Group

Let G be a group and let $a \in G$. Then the subgroup $\{a^n : n \in \mathbb{Z}\}$ of G is called the **cyclic subgroup** of G generated by a and it is denoted by $\langle a \rangle$. If there exists a single element $a \in G$ that generates the entire group G, i.e. $\langle a \rangle = G$, then a is said to be a *generator* for G, and G is a **cyclic group**.

Normal Subgroup

The following are three equivalent conditions for a subgroup H of a group G to be a **normal subgroup** of G:

i) H is closed under conjugates, i.e. $ghg^{-1} \in H$ for all $g \in G$ and $h \in H$.

ii) $gHg^{-1} = H$ for all $g \in G$.

iii) Left and right cosets of H are equal. That is, $gH = Hg$ for all $g \in G$.

Simple Group

A group is said to be **simple** if it is nontrivial and has no proper nontrivial normal subgroups.

b) State Lagrange's / Cayley's theorem

Lagrange's Theorem: Let H be a subgroup of a finite group G. Then the order of H is a divisor of the order of G.

Remark: The converse of Lagrange's theorem holds if G is abelian. That is, if G is an abelian group of order n, and there exists an m that divides n, then we are guaranteed the existence of a subgroup of G of order m.

An important corollary of Lagrange's theorem states the following:

Corollary: Every group of prime order is cyclic.

Cayley's Theorem: Every group is isomorphic to a group of permutations.

c) Define a (group / ring / kernel of) homomorphism / isomorphism.

Group Homomorphism

A map ϕ from a group G into a group G' is a **homomorphism** if the homomorphism property

$$\phi(ab) = \phi(a)\phi(b)$$

holds for all $a, b \in G$.

Group Isomorphism

Let $\langle G, * \rangle$ and $\langle G', *' \rangle$ be groups. An **isomorphism** of G with G' is a bijective map $\phi\colon G \longrightarrow G'$ that satisfies the homomorphic property, i.e. for all $x, y \in G$, we have

$$\phi(x * y) = \phi(x) *' \phi(y).$$

Kernel of a Homomorphism

Let $\phi\colon G \longrightarrow G'$ be a group homomorphism. The subgroup containing all the elements of G that are mapped to the identity element in G',

$$\phi^{-1}[\{e'\}] = \{x \in G \mid \phi(x) = e'\}$$

is called the **kernel** of ϕ, and it is denoted by $\ker(\phi)$.

Kernel of an Isomorphism

Same as the kernel of a homomorphism, which is defined above, although obviously ϕ in this case is bijective.

Ring Homomorphism

For rings $\mathcal{R}$ and $\mathcal{R}'$, a map $\phi\colon \mathcal{R} \longrightarrow \mathcal{R}'$ is a **ring homomorphism** if the following two conditions are satisfied for all $a, b \in \mathcal{R}$:

(1) $$\phi(a + b) = \phi(a) + \phi(b),$$

(2) $$\phi(ab) = \phi(a)\phi(b).$$

d) Define a ring / division ring / zero divisor / integral domain / ideal / field.

Ring

A **ring** $\langle \mathcal{R}, +, \cdot \rangle$ is a set $\mathcal{R}$ together with two binary operations "+" and "$\cdot$", which we call addition and multiplication, defined on $\mathcal{R}$ such that the following axioms hold:

- $\mathfrak{R}_1$: $\langle \mathcal{R}, + \rangle$ is an abelian group.
- $\mathfrak{R}_2$: Multiplication is associative.

▶ $\mathfrak{R}_3$: For all $a, b, c \in \mathcal{R}$, the *left distributive law*, $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ and the *right distributive law* $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$ hold.

Remark: A ring in which multiplication is commutative is called a **commutative ring**. A ring that has a multiplicative identity is called a **ring with unity**; the multiplicative identity element 1 is called **unity**.

Division Ring

A **division ring** is a ring in which every nonzero element is a unit.

Remark (Definition of a unit): Let $\mathcal{R}$ be a ring with unity $1 \neq 0$. An element u in $\mathcal{R}$ is called a **unit** of $\mathcal{R}$ if it has a multiplicative inverse in $\mathcal{R}$, i.e. a unit is just an invertible element in $\mathcal{R}$.

Field

A **field** is a commutative division ring.

Zero Divisor

If a and b are two nonzero elements of a ring $\mathcal{R}$ such that $ab = 0$, then a and b are called **zero divisors** or **divisors of zero**. (Note that both a and b must be nonzero!)

Integral Domain

An **integral domain** $\mathcal{D}$ is a commutative ring with unity $1 \neq 0$ and containing no zero divisors.

Ideal

An additive subgroup $\mathcal{I}$ of a ring $\mathcal{R}$ satisfying the property $a\mathcal{I} \subseteq \mathcal{I}$ and $\mathcal{I}b \subseteq \mathcal{I}$ for all $a, b \in \mathcal{R}$, is called an **ideal** $\mathcal{I}$ of $\mathcal{R}$. (Note that an ideal is the ring's analogue of a normal subgroup, that is, you can think of an ideal as a "normal" subring. Also, just as the kernel of a group homomorphism is a normal subgroup, we have that the kernel of a ring homomorphism is an ideal.)

Problem 2. (4 pts each) In each part give an example (with a brief explanation) that satisfies the given conditions or briefly explain why no such example exists.

a) A group of order 4 isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Solution. The Klein-4 group $V = \{e, a, b, ab\}$, which satisfies $a^2 = b^2 = (ab)^2 = e$, is such an example. According to the *Fundamental Theorem of Finitely Generated Abelian Groups*[1], we have, up to isomorphism, two groups of order 4, namely $\mathbb{Z}_4$ and $\mathbb{Z}_2 \times \mathbb{Z}_2$. We also know that there is, up to isomorphism, only one cyclic group structure of a given order. Since $\mathbb{Z}_4$ is cyclic, V must be isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$ (since V is not cyclic.) □

b) The smallest nonabelian group G.

Solution. The permutation group S_3 has minimum order for any nonabelian group. That is, if G is some nonabelian group, then we must have $|G| \geq 6$. □

c) A nonabelian group G such that every proper subgroup is abelian.

Solution. The nonabelian group S_3 is such an example. To see why take each of its proper subgroups

$$\{\rho_0\}, \quad \{\rho_0, \mu_1\}, \quad \{\rho_0, \mu_2\}, \quad \{\rho_0, \mu_3\}, \quad \{\rho_0, \rho_1, \rho_2\},$$

which are of order 1, 2, 2, 2, and 3, respectively. Since the minimum order for any nonabelian group is 6, we can see that all of the proper subgroups of the nonabelian group S_3 are abelian. □

d) A subring of the ring $\mathcal{R} = \mathbb{Z}_6$.

Solution. $S = \{0, 2, 4\}$ is such an example. Recall that in order for a subset S of a ring $\mathcal{R}$ to be a subring of $\mathcal{R}$, S must be closed under the operations induced by $\mathcal{R}$. That is, we must have that $ab \in S$ and $a + b \in S$ for all $a, b \in S$, and $0 \in S$, where 0 is the additive identity of $\mathcal{R}$. Since $S = \{0, 2, 4\}$ satisfies these conditions, we conclude that it is a subring of $\mathbb{Z}_6$. □

[1]Here's the statement of the theorem: Every finitely generated abelian group G is isomorphic to a direct product of cyclic groups in the form

$$\mathbb{Z}_{(p_1)^{r_1}} \times \mathbb{Z}_{(p_2)^{r_2}} \times \cdots \times \mathbb{Z}_{(p_n)^{r_n}} \times \mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z},$$

where the p_i are primes (not necessarily distinct) and the r_i are positive integers. The direct product is unique except for possible rearrangements of the factors.

e) A subring of a ring $\mathcal{R}$ having unity different from $\mathcal{R}$'s.

Solution. Take the ring $\mathbb{Z}_6$, which has unity 1:

$$1 \cdot 0 = 0, \quad 1 \cdot 1 = 1, \quad 1 \cdot 2 = 2, \quad 1 \cdot 3 = 3, \quad 1 \cdot 4 = 4, \quad 1 \cdot 5 = 5,$$

and observe that the subring $\{0, 2, 4\}$ has unity 4:

$$4 \cdot 0 = 0, \quad 4 \cdot 2 = 2, \quad 4 \cdot 4 = 4.$$ □

f) A ring without unity.

Solution. $2\mathbb{Z} = \{\dots, -2, 0, 2, \dots\}$ is such an example. Notice that there is no multiplicative identity in this ring. That is, there is no element $a \in 2\mathbb{Z}$ such that $ax = x \ \forall x \in 2\mathbb{Z}$. □

g) An integral domain containing only two units.

Solution. $\mathbb{Z}$ is such an example. Notice that $\mathbb{Z}$ is a commutative ring with unity and has no zero divisors, hence it is an integral domain. Also, the only units in $\mathbb{Z}$ are 1 and -1. □

h) A field that is not an integral domain.

Solution. No such example can possibly exist. A field is a commutative division ring, and division rings have the property that all nonzero elements are units. In order to have this property it must be true that there are no zero divisors, meaning that a field must also be an integral domain. □

i) An integral domain that is not a field.

Solution. $\mathbb{Z}$ is such an example. Notice that $\mathbb{Z}$ has no zero divisors, hence it is an integral domain. However in order for $\mathbb{Z}$ to be a field, it would have to be a commutative division ring. It certainly is commutative, however it is not a division ring because the only units in $\mathbb{Z}$ are 1 and -1. □

Problem 3. (5 pts each)

a) Let $\sigma = (1, 4, 6)(2, 7, 5, 3)$. Then find σ^{-2} and express it as a product of transpositions.

Solution. Notice that $\sigma^{-2} = (\sigma^2)^{-1}$. Hence we compute σ^2 first and then find its inverse:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 7 & 2 & 6 & 3 & 1 & 5 \end{pmatrix}$$
$$\implies \sigma^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 5 & 7 & 1 & 2 & 4 & 3 \end{pmatrix}$$
$$\implies \sigma^{-2} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 5 & 7 & 6 & 2 & 1 & 3 \end{pmatrix}.$$

Now we express our result as a product of transpositions:

$$(1,4,6)(2,5)(3,7) = (1,6)(1,4)(2,5)(3,7). \qquad \square$$

b) Find the order of $(8,10)$ in $\mathbb{Z}_{12} \times \mathbb{Z}_{18}$.

Solution. First we need to determine the order of 8 in $\mathbb{Z}_{12}$ and the order of 10 in $\mathbb{Z}_{18}$. To do that we must divide the order of the group $\mathbb{Z}_n$ by the gcd of n and the element that we wish to determine the order of.

Since the gcd of 12 and 8 is 4, we see that the order of 8 in $\mathbb{Z}_{12}$ is $12/4 = 3$. Similarly, since the gcd of 18 and 10 is 2, we see that the order of 10 in $\mathbb{Z}_{18}$ is $18/2 = 9$.

Finally, to determine the order of $(8,10)$ in $\mathbb{Z}_{12} \times \mathbb{Z}_{18}$, we just need to determine the *least common multiple* (**lcm**) of 3 and 9, which in this case is 9.

So we have $|(8,10)|_{\mathbb{Z}_{12}\times\mathbb{Z}_{18}} = 9$. $\square$

c) Find all abelian groups, up to isomorphism, of order 200.

Solution. We are going to apply the *Fundamental Theorem of Finitely Generated Abelian Groups*. Let us start by factoring out 200 into prime powers:

$$\begin{aligned} 200 &= 2^3 \times 5^2 \\ &= 2^3 \times 5 \times 5 \\ &= 2^2 \times 2 \times 5^2 \\ &= 2^2 \times 2 \times 5 \times 5 \\ &= 2 \times 2 \times 2 \times 5^2 \\ &= 2 \times 2 \times 2 \times 5 \times 5. \end{aligned}$$

We can see that we have, up to isomorphism, six abelian groups of order 200. These groups are $\mathbb{Z}_{2^3} \times \mathbb{Z}_{5^2}$, $\mathbb{Z}_{2^3} \times \mathbb{Z}_5 \times \mathbb{Z}_5$, $\mathbb{Z}_{2^2} \times \mathbb{Z}_2 \times \mathbb{Z}_{5^2}$, $\mathbb{Z}_{2^2} \times \mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_5$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{5^2}$, and $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_5$. $\square$

Problem 4. (9 pts) Let G be a group and H be a nonempty subset of G. Prove that if for all $a, b \in H$, we have $ab^{-1} \in H$, then H is a subgroup of G. Does the converse hold? If so, prove it. If not, find a counterexample.

Proof. Both the statement and its converse do indeed hold, as we are now going to show. That is, we are going to prove that a nonempty subset H of a group G is a subgroup of G if and only if, for all $a, b \in H$, we have $ab^{-1} \in H$.

($\Rightarrow$) Let H be a subgroup of G. Then, since H is itself a group, for all $a, b \in H$, we must have $b^{-1} \in H$ and so $ab^{-1} \in H$ because H must be closed under the induced operation.

($\Leftarrow$) Conversely, suppose that H is nonempty and $ab^{-1} \in H$ for all $a, b \in H$. Then taking $b = a$, we see that $aa^{-1} = e$ is in H. Taking $a = e$, and $b = a$, we see that $ea^{-1} = a^{-1} \in H$. Thus H contains the identity element and the inverse of each element. For closure, note that for $a, b \in H$, we also have $ab^{-1} \in H$ and thus $a(b^{-1})^{-1} = ab \in H$.

Thus we have shown that a nonempty subset H of a group G is a subgroup of G if and only if, for all $a, b \in H$, we have $ab^{-1} \in H$, as desired. □

Problem 5. (16 pts) (ANY **TWO** OF THESE WILL BE CHOSEN)

a) Prove the following: A group homomorphism $\phi\colon G \to G'$ is injective if and only if $\ker(\phi) = \{e\}$.

Proof. ($\Rightarrow$) Suppose that ϕ is injective. We know by a previous theorem that if ϕ is a group homomorphism, then $\phi(e) = e'$, where e' is the identity element in G'. But then since we are assuming that ϕ is injective, we see that e is the only element mapped into e' by ϕ, so that $\ker(\phi) = \{e\}$.

($\Leftarrow$) The proof for this direction offered in our text has some big ass gaps, so we are going to fix that:
Conversely, assume $\ker(\phi) = \{e\}$ and for every $a, b \in G$ let $\phi(a) = \phi(b)$. Notice that the elements mapped into $\phi(a) \in G'$ are precisely the elements of the left coset $a\{e\} = \{a\} \in G$. We are now going to show that any two elements a and b in G have the same image under ϕ if and only if they are in the same coset of the kernel $\{e\}$:

$$\begin{aligned}
\phi(a) = \phi(b) &\iff \phi(a)[\phi(b)]^{-1} = e' \\
&\iff \phi(a)\phi(b^{-1}) = e' && \text{(By a previous proposition)} \\
&\iff \phi(ab^{-1}) = e' && \text{(By the homomorphism property)} \\
&\iff ab^{-1} \in \{e\} && \text{(Since } \ker(\phi) = \{e\}\text{)} \\
&\iff \{e\}a = \{e\}b. && \text{(By a previous proposition)}
\end{aligned}$$

Since cosets represent equivalence classes, we know that if $\{e\}a = \{e\}b$, then necessarily we must have $a = b$, which shows that ϕ is injective. □

b) Let $\phi\colon G \to G'$ be a group homomorphism. Show that $\ker(\phi)$ is a normal subgroup of G.

Proof. First of all, from a previous result we already know that $\ker(\phi)$ is a subgroup of G. What we are going to do now is try to show that this subgroup is normal. We can do this by showing that $\ker(\phi)$ is closed under conjugates, i.e. we want to show that for $g \in G$ and $h \in \ker(\phi)$, we have $ghg^{-1} \in \ker(\phi)$.[2]
Now let e' be the identity element in G'. Then,

$$\begin{aligned}
\phi(ghg^{-1}) &= \phi(g)\phi(h)\phi(g^{-1}) && \text{(By the homomorphic property)}\\
&= \phi(g)e'\phi(g^{-1}) && \text{(Since } h \in \ker(\phi)\text{)}\\
&= \phi(g)\phi(g^{-1})\\
&= \phi(g)\phi(g)^{-1} && \text{(By a previous proposition)}\\
&= e'.
\end{aligned}$$

Hence, $ghg^{-1} \in \ker(\phi)$, which indicates that $\ker(\phi)$ is closed under conjugates, hence it is a normal subgroup of G. □

c) Let $\phi\colon G \longrightarrow G'$ be a group homomorphism of G onto G'. Show that if G is abelian, then G' must also be abelian.

Proof. Let G be abelian and let ϕ be a homomorphism of G onto G'. For $a', b' \in G'$, we want to show that $a'b' = b'a'$. Since ϕ is an onto homomorphism, there exists $a, b \in G$ such that $\phi(a) = a'$, $\phi(b) = b'$, and $\phi(ab) = \phi(a)\phi(b) = a'b'$.
But then

$$\begin{aligned}
a'b' = \phi(a)\phi(b) &= \phi(ab)\\
&= \phi(ba) && \text{(since } G \text{ is abelian)}\\
&= \phi(b)\phi(a) && \text{(since } \phi \text{ is a homomorphism)}\\
&= b'a'.
\end{aligned}$$

Thus we have proven that G' is abelian. □

[2]The proof on the book sucks because they prove this result by showing that the right and left cosets are equal, which is not hard to prove but the proof is considerably longer. Follow my proof instead ☺.

d) Prove that every cyclic group is abelian.

Proof. Let G be a cyclic group and let a be a generator for G so that $G = \langle a \rangle = \{a^n : n \in \mathbb{Z}\}$. If g_1 and g_2 are any two elements of G, there exist integers r and s such that $g_1 = a^r$ and $g_2 = a^s$. Then,

$$\begin{aligned} g_1 g_2 = a^r a^s &= a^{r+s} \\ &= a^{s+r} && \text{(since } \mathbb{Z} \text{ is abelian)} \\ &= a^s a^r \\ &= g_2 g_1. \end{aligned}$$

Thus we have proven that G is abelian. □

e) Let $\phi\colon G \longrightarrow G'$ be a group homomorphism with kernel H. Show that the map $\mu\colon G/H \longrightarrow \phi[G]$ defined by $\mu(gH) = \phi(g)$ for each $g \in G$ is an isomorphism.

Proof. This is the famous *Fundamental Homomorphism Theorem*. Before proving that our map μ is an isomorphism we need to make sure that it is well defined map. That is, we need to make sure that if $g_1 H$ is the same coset as $g_2 H$, then $\mu(g_1 H) = \mu(g_2 H)$, where $g_1, g_2 \in G$. Indeed by a previous theorem we know that if $f : G \longrightarrow G'$ is any homomorphism with kernel H, then for all $a, b \in G$ we have that $f(a) = f(b)$ iff $aH = bH$. In other words, this theorem tells us that any two elements a and b in G have the same image under f if and only if they are in the coset of H. Hence by invoking this theorem, we are guaranteed that our function μ is well defined. Now let us show that μ is in fact an isomorphism:

- (*Injectivity*) If $\mu(g_1 H) = \mu(g_2 H)$, then $\phi(a) = \phi(b)$, and by the theorem that we called upon when we showed that μ was well defined, we have that $g_1 H = g_2 H$.
- (*Surjectivity*) Every element of $\phi[G]$ is of the form $\phi(g) = \mu(gH)$, so μ is obviously onto.
- (*Homomorphic property*) Notice that the homomorphic property holds:

$$\begin{aligned} \mu(g_1 H \cdot g_2 H) &= \mu(g_1 g_2 H) && \text{(by the binary operation on } G/H) \\ &= \phi(g_1 g_2) \\ &= \phi(g_1)\phi(g_2) && \text{(by the homomorphic property of } \phi) \\ &= \mu(g_1 H)\mu(g_2 H). \end{aligned}$$

Thus we have shown that μ is an isomorphism from G/H to $\phi[G]$, as desired. □

f) Let $\phi\colon G \to G'$ be a group homomorphism of G into G' and $H = \ker(\phi)$. Let $a \in G$. Then show that

$$\phi^{-1}\left[\{\phi(a)\}\right] = \{x \in G \mid \phi(x) = \phi(a)\} = aH.$$

Proof. Let us call the above set S. We want to prove that S is in fact the left coset aH of H. Let us take an element $x \in S$ so that $\phi(x) = \phi(a)$. Multiplying on the left by $\phi(a)^{-1}$, we get

$$\begin{aligned} &\phi(a)^{-1}\phi(x) = e' && \text{(where } e' \text{ is the identity of } G') \\ &\implies \phi(a^{-1})\phi(x) = e' && \text{(by a previous theorem)} \\ &\implies \phi(a^{-1}x) = e' && \text{(by the homomorphic property)} \\ &\implies a^{-1}x \in H. \end{aligned}$$

Hence we have that $a^{-1}x = h$ for some $h \in H$, and so multiplying by a on both sides we get $x = ah \in aH$. This shows that $S \subseteq aH$.

Now to conclude our proof we need to show that $aH \subseteq S$. Let $y \in aH$, so that $y = ah$ for some $h \in H$. Then,

$$\phi(y) = \phi(ah) = \phi(a)\phi(h) = \phi(a)e' = \phi(a),$$

so that $y \in \{x \in G \mid \phi(x) = \phi(a)\}$.

Since we have proven that $S \subseteq aH$ and $S \supseteq aH$, it follows that $S = \phi^{-1}[\{\phi(a)\}] = \{x \in G \mid \phi(x) = \phi(a)\} = aH$, as desired. □

g) Prove that the cancellation law holds in a ring $\mathcal{R}$ if and only if $\mathcal{R}$ has no zero divisors.

Proof. ($\Rightarrow$) Let $\mathcal{R}$ be a ring in which the cancellation law holds and suppose $ab = 0$ for some $a, b \in \mathcal{R}$. Then in order to show that $\mathcal{R}$ has no zero divisors, we must show that either a or b is 0.
If $a \neq 0$, then $ab = a0 \implies b = 0$ by cancellation laws. Similarly, $b \neq 0 \implies a = 0$, so there can be no zero divisors if we assume that the cancellation law holds.

($\Leftarrow$) To prove in the other direction, suppose that $\mathcal{R}$ has no zero divisors and suppose that $ab = ac$ with $a \neq 0$. Then we have

$$\begin{aligned} ab - ac &= a(b - c) \quad \text{(by the distributive property of } \mathcal{R} \text{)} \\ &= 0. \end{aligned}$$

Since $a \neq 0$, and since $\mathcal{R}$ has no zero divisors, we must have $b - c = 0 \implies b = c$. A similar argument shows that $ba = ca$ with $a \neq 0$ implies $b = 0$. This shows that if $\mathcal{R}$ has no zero divisors, then the cancellation law holds.

Thus it has been shown that the cancellation law holds in a ring $\mathcal{R}$ if and only if $\mathcal{R}$ has no zero divisors, as desired. □

h) Prove that for $n \geq 3$, S_n is nonabelian.

Proof. Let $\alpha, \beta \in S_n$ be defined by

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & \dots \\ 1 & 3 & 2 & \dots \end{pmatrix} \quad \text{and} \quad \beta = \begin{pmatrix} 1 & 2 & 3 & \dots \\ 3 & 2 & 1 & \dots \end{pmatrix}$$

That is, we "permute" the first three elements of both α and β and fix the rest. Then we have

$$\begin{aligned} \alpha\beta &= \begin{pmatrix} 1 & 2 & 3 & \dots \\ 1 & 3 & 2 & \dots \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & \dots \\ 3 & 2 & 1 & \dots \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 & 3 & \dots \\ 2 & 3 & 1 & \dots \end{pmatrix}, \end{aligned}$$

while

$$\begin{aligned} \beta\alpha &= \begin{pmatrix} 1 & 2 & 3 & \dots \\ 3 & 2 & 1 & \dots \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & \dots \\ 1 & 3 & 2 & \dots \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 & 3 & \dots \\ 3 & 1 & 2 & \dots \end{pmatrix}. \end{aligned}$$

We can thus see that $\alpha\beta \neq \beta\alpha$, which shows that S_n is nonabelian for $n \geq 3$. □

i) Let H and K be groups. Let $(h_1, k_1), (h_2, k_2) \in H \times K$. Show that $H \times K$ is a group under the binary operation $(h_1, k_1)(h_2, k_2) = (h_1h_2, k_1k_2)$, where h_1h_2 and k_1k_2 are elements of H and K, respectively.

Proof. The fact that $H \times K$ is closed under the binary operation is painfully obvious by the way the operation is defined. Now let us check the axioms:

- (*Associativity*) We have

$$[(h_1, h_2)(k_1, k_2)](g_1, g_2) = (h_1k_1, h_2k_2)(g_1, g_2) = (h_1k_1g_1, h_2k_2g_2),$$

and

$$(h_1, h_2)[(k_1, k_2)(g_1, g_2)] = (h_1, h_2)(k_1g_1, k_2g_2) = (h_1k_1g_1, h_2k_2g_2).$$

- (*Identity*) Let e_1, e_2 be the identity elements in H and K, respectively. Then,

$$(h_1, k_1)(e_1, e_2) = (h_1e_1, k_1e_2) = (h_1, k_1) \quad \text{and} \quad (e_1, e_2)(h_1, k_1) = (e_1h_1, e_2k_1) = (h_1, k_1).$$

- (*Inverse*) Let h_1^{-1} and k_1^{-1} be the inverses of $h_1 \in H$ and $k_1 \in K$, respectively. Then,

$$(h_1, k_1)(h_1^{-1}, k_1^{-1}) = (h_1h_1^{-1}, k_1k_1^{-1}) = (e_1, e_2).$$

Hence we have shown that $H \times K$ is a group under the defined binary operation. □

j) Prove that a group is abelian if every element except the identity has order 2.

Proof. Let us assume that every element except the identity has order 2, that is $a^2 = a \cdot a = e$ for every element $a \neq e \in G$. Then we want to show that, for any two elements $a, b \in G$, we have $ab = ba$. Let $a, b \in G$. Then

$$\begin{aligned} & a^2 = e \\ \implies & a^{-1}a^2 = a^{-1}e \\ \implies & a = a^{-1} \end{aligned} \qquad \text{and} \qquad \begin{aligned} & b^2 = e \\ \implies & b^{-1}b^2 = b^{-1} \cdot e \\ \implies & b = b^{-1} \end{aligned}$$

Since a and b are distinct elements of G and G is a group, we have that $ab \in G$, hence $(ab)^2 = e$. Then, by the above argument we have

$$\begin{aligned} & ab = (ab)^{-1} \\ \implies & ab = b^{-1}a^{-1} \\ \implies & ab = ba. \quad (\text{since } b^{-1} = b \text{ and } a^{-1} = a). \end{aligned}$$

Thus G is abelian, as was to be proved. □

k) Let ϕ be a homomorphism of a ring $\mathcal{R}$ with unity onto a nonzero ring $\mathcal{R}'$. Suppose u is a unit in $\mathcal{R}$. Then show that $\phi(u)$ is a unit in $\mathcal{R}'$.

Proof. The condition that ϕ maps $\mathcal{R}$ onto a nonzero ring $\mathcal{R}'$ shows that no unit of $\mathcal{R}$ is in $\ker(\phi)$, for if $\ker(\phi)$ contains a unit u, then it contains $(ru^{-1})u = r$ for all $r \in \mathcal{R}$, which would mean that $\ker(\phi) = \mathcal{R}$ and $\mathcal{R}'$ would be the zero ring, since ϕ is assumed to be an onto map.

Now let u be a unit in $\mathcal{R}$. Because $\phi[\mathcal{R}] = \mathcal{R}'$ (i.e. ϕ is onto), we know that $\phi(1)$ is unity $1'$ in $\mathcal{R}'$. From the fact that $uu^{-1} = u^{-1}u = 1$, we obtain

$$\phi(uu^{-1}) = \phi(u)\phi(u^{-1}) = 1' \quad \text{and} \quad \phi(u^{-1}u) = \phi(u^{-1})\phi(u) = 1'.$$

Thus $\phi(u)$ is a unit of $\mathcal{R}'$, and its inverse is $\phi(u^{-1})$. □

l) Let $\mathcal{R}$ be a commutative ring and let $a \in \mathcal{R}$. Show that $I_a = \{x \in \mathcal{R} \mid ax = 0\}$ is an ideal of $\mathcal{R}$.

Proof. Let $x, y \in I_a$ so that $ax = ay = 0$. Then

$$a(x + y) = ax + ay = 0 + 0 = 0 \implies (x + y) \in I_a.$$
$$a(xy) = (ax)y = 0y = 0 \implies xy \in I_a.$$

Because $a0 = 0$ and $a(-x) = -(ax) = -0 = 0$, we see that I_a contains 0 and additive inverses of each of its elements x, so I_a is a subring of $\mathcal{R}$. (Note that thus far, we have not used commutativity in $\mathcal{R}$.) Let $r \in \mathcal{R}$. Then

$$a(xr) = (ax)r = 0r = 0 \Longrightarrow xr \in I_a,$$

and because $\mathcal{R}$ is commutative, we see that $a(rx) = r(ax) = r0 = 0$, so $rx \in I_a$. Thus I_a is an ideal of $\mathcal{R}$. □

m) Let $\mathcal{R}$ be a ring with at least two elements. Suppose that for each nonzero element $a \in \mathcal{R}$ there is a unique element $b \in \mathcal{R}$ (that depends on a), with $aba = a$. Show then that $\mathcal{R}$ is a division ring.

Proof. Let a be a nonzero element of $\mathcal{R}$ and assume that $aba = a$ for some unique $b \in \mathcal{R}$. In order to show that $\mathcal{R}$ is a division ring, we need to show that every nonzero element is a unit. We are going to show this in a series of steps:

Step 1 (Show that $\mathcal{R}$ has no zero divisors): For some $x \in \mathcal{R}$, suppose $ax = 0$ or $xa = 0$ with $a \neq 0$. We want to show that $x = 0$:

$$a(b + x)a = aba + axa = a + 0 = a.$$

But then by uniqueness of b, we have that $b + x = b$, from which follows that $x = 0$. Hence $\mathcal{R}$ has no zero divisors.

Step 2 (Show that $bab = b$): From $aba = a$, we know that $b \neq 0$ also. Multiplying on the left by b, we obtain $baba = ba$. Since –according to our work in *Step 1*– $\mathcal{R}$ has no zero divisors, by a previous theorem we know that the cancellation laws hold and thus we have that $bab = b$.

Step 3 (Show that $\mathcal{R}$ has unity): We claim that ab is unity for nonzero a and b given in the statement of the exercise. Let $x \in \mathcal{R}$ and observe that

$$\begin{aligned} & aba = a \\ \Longrightarrow\ & xa = xaba \\ \Longrightarrow\ & x = x(ab) \end{aligned} \tag{♡}$$

Notice that in (♡) we were able to cancel a on both sides because we already showed that $\mathcal{R}$ has no zero divisors and therefore the cancellation law holds. Now from *Step 2*, we have $bx = babx$, and canceling b yields $x = (ab)x$. Thus ab satisfies $(ab)x = x(ab)$ for all $x \in \mathcal{R}$, which shows that ab is unity.

Final Step (Show that $\mathcal{R}$ is a division ring): By *Step 3*, $ab = 1$ so b is a right inverse of a. Because the elements a and b behave in a symmetric fashion by *Step 2*, an argument symmetric to that in *Step 3*, starting with the equation $ax = abax$, shows that $ba = 1$ also. Thus b is also a left inverse of a, so a is a unit. This shows that $\mathcal{R}$ is a division ring. □