MATH 546, HOMEWORK, SPRING 2023

(1) Recall the group $S_n = \mathrm{Sym}(\{1,...,n\})$, where S_n is the set of invertible functions from $\{1,\ldots,n\}$ to $\{1,\ldots,n\}$. The operation in S_n is function composition.

(a) Take $n=3$. Let σ and τ be the following elements of S_3:

$$\sigma(1)=2, \quad \sigma(2)=1, \quad \sigma(3)=3, \quad \text{and}$$
$$\tau(1)=2, \quad \tau(2)=3, \quad \tau(3)=1.$$

(i) How many distinct elements[1] of S_3 can be written in the form $\sigma^i \circ \tau^j$?

(ii) Can $\tau\circ\sigma$ be written in the form $\sigma^i \circ \tau^j$?

(iii) Record the multiplication table for the smallest subgroup of S_3 which contains τ and σ. Put your entries in the form $\sigma^i \circ \tau^j$ whenever this makes sense.

(b) Take $n=4$. Let σ and τ be the following elements[2] of S_4:

$$\sigma(1)=3, \quad \sigma(2)=2, \quad \sigma(3)=1, \quad \sigma(4)=4, \quad \text{and}$$
$$\tau(1)=2, \quad \tau(2)=3, \quad \tau(3)=4, \quad \tau(4)=1.$$

(i) How many distinct elements of S_4 can be written in the form $\sigma^i \circ \tau^j$?

(ii) Can $\tau\circ\sigma$ be written in the form $\sigma^i \circ \tau^j$?

(iii) Record the multiplication table for the smallest subgroup of S_4 which contains τ and σ. Put your entries in the form $\sigma^i \circ \tau^j$ whenever this makes sense.

(c) Take $n=4$. Let σ and τ be the following elements of S_4:

$$\sigma(1)=2, \quad \sigma(2)=1, \quad \sigma(3)=3, \quad \sigma(4)=4, \quad \text{and}$$

[1] If f is an element of S_3, then one relatively convenient way to record f is in the form

$$\begin{pmatrix} 1 & 2 & 3 \\ f(1) & f(2) & f(3) \end{pmatrix}.$$

If one uses this notation, then

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \quad \text{and} \quad \tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}.$$

[2] In the notation of footnote 1,

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix} \quad \text{and} \quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}.$$

$$\tau(1) = 2, \quad \tau(2) = 3, \quad \tau(3) = 4, \quad \tau(4) = 1.$$

(i) How many distinct elements of S_4 can be written in the form $\sigma^i \circ \tau^j$?
(ii) Can $\tau \circ \sigma$ be written in the form $\sigma^i \circ \tau^j$?
(iii) Record the multiplication table for the smallest subgroup of S_4 which contains τ and σ. (This part of the problem is unpleasant. You can skip it if you want. Actually, this problem is the very last thing in the class notes. See part 5 of the section "Loose Ends", which is section 7.C.)

(2) Consider the following sets S with binary operation $*$. Which pairs $(S,*)$ form a group? If $(S,*)$ is not a group, which axioms fail?
 (a) Let S be the set of integers $\mathbb{Z}$ and let $a*b = ab$.
 (b) Let S be the set of integers $\mathbb{Z}$ and let $a*b = \max\{a,b\}$.
 (c) Let S be the set of integers $\mathbb{Z}$ and let $a*b = a-b$.
 (d) Let S be the set of integers $\mathbb{Z}$ and $a*b = |ab|$.
 (e) Let S be the set of positive real numbers $\mathbb{R}^+$ and $a*b = ab$.
 (f) Let S be the set of non-zero rational numbers $\mathbb{Q} \setminus \{0\}$ and $a*b = ab$.

(3) Prove that multiplication of 2×2 matrices satisfies the associative law.

(4) Is the group $\mathrm{GL}_n(\mathbb{R})$ an Abelian group? Give a proof or counter example. Recall that $\mathrm{GL}_n(\mathbb{R})$ is the group of invertible $n\times n$ matrices under multiplication.

(5) Write a multiplication table for the following set of matrices over $\mathbb{Q}$:

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad A = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, \quad B = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \quad \text{and} \quad C = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}.$$

(6) Let $G = \{x \in \mathbb{R} \mid 0 < x \text{ and } x \neq 1\}$. Define $a*b = a^{\ln b}$, for a and b in G. Prove that $(G,*)$ is an Abelian group.

(7) Let $S = \mathbb{R} \setminus \{-1\}$. Define $*$ by $a*b = a+b+ab$, for a and b in S. Prove that $(S,*)$ is a group.

(8) Prove that a non-Abelian group must have at least five distinct elements.

(9) Let G be a group and let a,b be elements of G. Suppose $(ab)^2 = a^2b^2$. Prove that a and b commute.

(10) Is the group of complex numbers $\{1,-1,i,-i\}$, under multiplication, a Klein 4-group?

(11) Let ρ be rotation counter clockwise by 120° fixing the origin. Let σ be reflection of the xy plane across the x axis. Let D_3 be the smallest subgroup of the group of rigid motions which contains ρ and σ.
 (a) List the elements of D_3.
 (b) Find the multiplication table for D_3.
 (c) Describe the action of each element of D_3.

(d) Show that if $\tau \in D_3$, then $\tau(T) = T$, where T is the triangle with vertices $(1,0)$, $(-\frac{1}{2}, \frac{\sqrt{3}}{2})$, and $(-\frac{1}{2}, -\frac{\sqrt{3}}{2})$.

(12) Suppose H and K are subgroups of the group G. Is the intersection $H \cap K$ a always subgroup of G? If so, prove the statement. If not, give an example.

(13) Suppose H and K are subgroups of the group G. Is the union $H \cup K$ always a subgroup of G? If so, prove the statement. If not, give an example.

(14) Let G be the group of rational numbers, under addition, and let H and K be subgroups of G. Prove that if $H \neq \{0\}$ and $K \neq \{0\}$, then $H \cap K \neq \{0\}$.

(15) Let G be a group, and let $a \in G$. The set $C(a) = \{x \in G \mid xa = ax\}$ of all elements of G that commute with a is called the *centralizer* of a.

(a) Prove that $C(a)$ is a subgroup of G.

(b) Prove that $\langle a \rangle \subseteq C(a)$.

(c) Find the centralizer of ρ in D_4.

(d) Find the centralizer of ρ^2 in D_4.

(e) Find the centralizer in $\mathrm{GL}_2(\mathbb{R})$ of the matrix

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}.$$

(16) Find 6 subgroups of D_4 in addition to D_4 and $\{\mathrm{id}\}$.

(17) Let U_8 be the group of complex numbers which satisfy $x^8 = 1$. Find two subgroups of U_8 in addition to $\{\mathrm{id}\}$ and U_8.

(18) Let G be the group U_9, which consists of all complex numbers z such that $z^9 = 1$.

(a) What is the order of each element of G?

(b) Which elements of G are generators of all of G. (Recall that the element g in the group G *generates* G, if $\langle g \rangle = G$.)

(c) Which elements g of G can be written in the form h^2 for some $h \in G$?

(d) Which elements g of G can be written in the form h^3 for some $h \in G$?

(19) Let H be a subgroup of the integers under addition. Prove that H is a cyclic group.

(20) Find three subgroups of D_4 of order 4. (A subgroup of order 4 is a subgroup with 4 elements.)

(21) Let g be an element of the group G and let

$$S = \{n \in \mathbb{Z} \mid g^n = \mathrm{id}\}. \tag{0.0.1}$$

(In other words, S is the set of integers n such that g^n is equal to the identity of G.) Prove that S is a subgroup of $(\mathbb{Z}, +)$.

(22) Consider $g = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}$ in the group $\mathrm{GL}_2(\mathbb{C})$. What is the set S (as in (0.0.1)) for g?

(23) Consider $g = \cos\frac{2\pi}{10} + i \sin\frac{2\pi}{10}$ in the unit circle group U. What is the set S (as in (0.0.1)) for g?

(24) Let $(G,*)$ be a group and let $H = \{g \in G \mid g*g*g = \mathrm{id}\}$. Calculate H for $G = D_4$, $G = D_3$, and $G = U_6$. (Recall that U_6 is the set of complex numbers which are sixth roots of 1.)

(25) Let G be a group. Suppose that g^2 is equal to the identity element of G for all g in G. Prove that G is an Abelian group.

(26) Let G be a finite group with an even number of elements. Prove that there must exist an element g of G with g not the identity element, but g^2 equal to the identity element.

(27) Find an example of a group G and elements a and b in G such that a and b each have finite order, but ab does not. (The element a of the group G has *finite order* if there exists a positive integer n with a^n equal to the identity element. If a does not have finite order, then a has *infinite order*.)

(28) Let $G = D_4$ and let H be the subgroup of G which is generated by σ. List the left cosets of H in G.

(29) Let $G = U_9$ and let H be the subgroup of G which is generated by u^3, where $u = \cos\frac{2\pi}{9} + i\sin\frac{2\pi}{9}$. List the left cosets of H in G.

(30) Let G be the group $(\mathbb{R}^2, +)$, which consists of all column vectors with two real entries, under the operation of addition, and let H be the subgroup of G which consists of all elements of the form $\begin{bmatrix} a \\ a \end{bmatrix}$, for some real number a. Notice that each element of G corresponds in a natural way to a point in the xy-plane. Describe the left cosets of H in G.

(31) Let G be a group. The set $Z(G) = \{x \in G \mid xg = gx \text{ for all } g \in G\}$ of all elements that commute with every other element of G is called the *center* of G.
   (a) Prove that $Z(G)$ is a subgroup of G.
   (b) Show that $Z(G) = \bigcap_{a \in G} C(a)$.
   (c) Find the center of D_3.
   (d) Find the center of D_4.
   (e) Find the center of $\mathrm{GL}_2(\mathbb{R})$.

(32) Let G be a cyclic group. Let a and b be elements of G such that $a \neq g^2$ for any $g \in G$ and $b \neq g^2$ for any $g \in G$. Prove that ab is equal to g^2 for some $g \in G$. What happens if the hypothesis that G is a cyclic group is removed? Is the statement still true? If so, prove it. If not, find a counterexample. Recall that the group G is *cyclic* if there is an element h in G such that every element of G has the form h^n for some integer n.

(33) Let a and b be elements of a group G. Suppose that a and b both have finite order that the orders of a and b are relatively prime. Suppose further that $ab = ba$. Prove that the order of ab is equal to the order of a times the order of b. Recall that the *order* of a group element a is the least positive integer n with a^n equal to the identity element.

(34) True or False. If true, prove it. If false, give a counterexample. Let G be a group and let H be the subset $H = \{g \in G \mid g^2 = \mathrm{id}\}$. Then H is a subgroup of G.

(35) (a) Compute the left and right cosets of $H = \langle \sigma \rangle$ in $G = D_3$.
(b) Is ghg^{-1} in H for all $g \in G$ and h in H, where H and G are as given in (a)?
(c) Compute the left and right cosets of $H = \langle \rho \rangle$ in $G = D_3$.
(d) Is ghg^{-1} in H for all $g \in G$ and h in H, where H and G are as given in (c)?

(36) (a) Suppose that H is a subgroup of the group G with the property that ghg^{-1} in H for all $g \in G$ and h in H. Let a, b, and c be elements of G with $aH = bH$, prove that $acH = bcH$.
(b) Suppose that H is a subgroup of the group G and that a, b, and c be elements of G with $aH = bH$. Must $acH = bcH$? Prove or give a counterexample.

(37) Let G be $(\mathbb{C} \setminus \{0\}, \times)$. Describe the left cosets of the subgroup H in G where
(a) $H = U_4$
(b) $H = \{ru \mid \ r \text{ is a positive real number and } u \in U_4\}$.

(38) Suppose that H is a subgroup of the group G and ghg^{-1} is in H for all $g \in G$ and $h \in H$.
(a) Let h_1 be an arbitrary element of H and g be an arbitrary element of G. Prove that there exists an element h of H with $h_1 = ghg^{-1}$. (It is possible to give a proof which works for infinite groups as well as finite groups.)
(b) Let a, b, c, and d be elements of G with $aH = bH$ and $cH = dH$. Prove that $acH = bdH$.
(c) Let S be the set of cosets $S = \{aH \mid a \in G\}$ of H in G. Problem 38b shows that the operation on S given by $(aH) * (bH) = abH$ is a well-defined function. Prove that S is a group. (If you are looking for this somewhere, S is usually written as $\frac{G}{H}$ and S is called the "quotient group of G mod H", or the "factor group of G mod H". BY THE WAY: S is not a subset of anything; we have to verify all of the axioms for group. Fortunately, this is very easy.)

(39) (a) If G is an Abelian group and H is a subgroup of G, then prove that ghg^{-1} is in H for all $g \in G$ and $h \in H$.
(b) If G is a finite group with $2n$ elements and H is a subgroup of G with n elements, then prove that ghg^{-1} is in H for all $g \in G$ and $h \in H$.
(c) If G is a group and H is a subgroup of the center of G, then prove that ghg^{-1} is in H for all $g \in G$ and $h \in H$. (The word center is defined in Problem 31.)

For future reference, a subgroup H of a group G is called a *normal* subgroup if ghg^{-1} is in H for all $g \in G$ and $h \in H$.

(40) Work out some examples of $\frac{G}{H}$ as described in problem 38c.

(a) Let $G = D_4$ and $H = \langle \rho \rangle$. Problem 39c tells us that it is legal to create $\frac{G}{H}$. What is this group? How many elements does it have? What is the multiplication table? Do you believe that this multiplication makes sense?

(b) Let $G = D_4$ and $H = \langle \rho^2 \rangle$. Problem 39b tells us that it is legal to create $\frac{G}{H}$. What is this group? How many elements does it have? What is the multiplication table? Do you believe that this multiplication makes sense?

(c) Let $G = \mathbb{Z}$ and $H = 5\mathbb{Z}$. Problem 39a tells us that it is legal to create $\frac{G}{H}$. What is this group? How many elements does it have? What is the addition table? Do you believe that this addition makes sense? (Notice that the elements of this $\frac{G}{H}$ look like $a+H$ because the operation in G is called $+$. Furthermore, the operation in $\frac{G}{H}$ is also called $+$; that is, $(a+H)+(b+H) = a+b+H$.)

(41) Prove that if N is a normal subgroup of the group G, and H is any subgroup of G, then $H \cap N$ is a normal subgroup of H. The word normal is defined in problem 39.

(42) Let G be a finite group, and let n be a divisor of $|G|$. Prove that if H is the only subgroup of G of order n , then H must be normal in G . (The symbol $|G|$ means the number of elements in the group G. It is often read as the *order* of G.)

(43) Let H and K be normal subgroups of of the group G such that $H \cap K = \langle \mathrm{id} \rangle$ Prove that $hk = kh$ for all $h \in H$ and $k \in K$.

(44) Prove that $\frac{\mathbb{Z}\times\mathbb{Z}}{\langle(0,1)\rangle}$ is an infinite cyclic group. Recall that the direct product of $\mathbb{Z}$ with $\mathbb{Z}$ is the group of ordered pairs (a,b), where a and b are integers. The operation is coordinate wise addition: $(a,b)+(c,d) = (a+c, b+d)$, for integers a, b, c, and d. (For a more sophisticated solution to this problem than you are able to give now, see problem 67.)

(45) Prove that $\frac{\mathbb{Z}\times\mathbb{Z}}{\langle(1,1)\rangle}$ is an infinite cyclic group. (For a more sophisticated solution to this problem than you are able to give now, see problem 68.)

(46) Prove that $\frac{\mathbb{Z}\times\mathbb{Z}}{\langle(2,2)\rangle}$ is not a cyclic group.

(47) Compute the group

$$\frac{\frac{Z}{\langle 6\rangle} \times \frac{\mathbb{Z}}{\langle 4\rangle}}{\langle(\bar{2},\bar{2})\rangle}.$$

(For a more sophisticated solution to this problem than you are able to give now, see problem 69.)

(48) Compute the group

$$\frac{\frac{\mathbb{Z}}{\langle 6\rangle}\times\frac{\mathbb{Z}}{\langle 4\rangle}}{\langle(\bar{3},\bar{2})\rangle}.$$

(49) Find all cyclic subgroups of $\frac{\mathbb{Z}}{\langle 8\rangle}$.

(50) Give a subgroup diagram of $\frac{\mathbb{Z}}{\langle 60\rangle}$.

(51) Find the cyclic subgroup of $(\mathbb{C}\setminus\{0\},\times)$ generated by $\frac{\sqrt{2}+i\sqrt{2}}{2}$.

(52) Find the order of the cyclic subgroup of $(\mathbb{C}\setminus\{0\},\times)$ generated by i.

(53) Find all cyclic subgroups of $\frac{\mathbb{Z}}{\langle 4\rangle}\times\frac{\mathbb{Z}}{\langle 2\rangle}$.

(54) Define $\varphi:(\mathbb{C}\setminus\{0\},\times)\to(\mathbb{R}\setminus\{0\},\times)$ by $\varphi(a+bi)=a^2+b^2$. Prove that φ is a homomorphism.

(55) Which of the following are homomorphisms?
   (a) $\varphi:(\mathbb{R}\setminus\{0\},\times)\to \mathrm{GL}_2(\mathbb{R})$ defined by $\phi(a)=\begin{bmatrix}a&0\\0&1\end{bmatrix}$,
   (b) $\varphi:(\mathbb{R},+)\to \mathrm{GL}_2(\mathbb{R})$ defined by $\phi(a)=\begin{bmatrix}1&a\\0&1\end{bmatrix}$,
   (c) $\varphi:\mathrm{Mat}_{2\times 2}(\mathbb{R})\to(\mathbb{R},+)$ defined by $\phi\left(\begin{bmatrix}a&b\\c&d\end{bmatrix}\right)=a$,
   Recall that $\mathrm{Mat}_{2\times 2}(\mathbb{R})$ is the Abelian group of 2×2 matrices with real number entries. The operation in $\mathrm{Mat}_{2\times 2}(\mathbb{R})$ is matrix addition.
   (d) $\varphi:\mathrm{GL}_2(\mathbb{R})\to(\mathbb{R}\setminus\{0\},\times)$ defined by $\phi\left(\begin{bmatrix}a&b\\c&d\end{bmatrix}\right)=ab$,
   (e) $\varphi:\mathrm{GL}_2(\mathbb{R})\to(\mathbb{R},+)$ defined by $\phi\left(\begin{bmatrix}a&b\\c&d\end{bmatrix}\right)=a+d$, and
   (f) $\varphi:\mathrm{GL}_2(\mathbb{R})\to(\mathbb{R}\setminus\{0\},\times)$ defined by $\phi\left(\begin{bmatrix}a&b\\c&d\end{bmatrix}\right)=ad-bc$.

(56) Let $\varphi:G_1\to G_2$ and $\theta:G_2\to G_3$ be group homomorphisms. Prove that $\theta\circ\varphi:G_1\to G_3$ is a group homomorphism. Prove that $\ker(\varphi)\subseteq\ker(\theta\circ\varphi)$.

(57) Prove that the intersection of two normal subgroups of a group G is a normal subgroup of G.

(58) Let $\varphi:G\to G'$ be a group homomorphism.
   (a) Let id be the identity element of G and id$'$ be the identity element of G'. Prove that $\varphi(\mathrm{id})=\mathrm{id}'$.
   (b) Let g be an element of G. Prove that φ of the inverse of g is equal to the inverse of $\varphi(g)$.
   (c) The image of φ is the subset $\mathrm{im}\,\varphi=\{\varphi(g)\mid g\in G\}$ of G'. Prove that $\mathrm{im}\,\varphi$ is a subgroup of G'.
   (d) The kernel of φ is the subset $\ker\varphi=\{g\in G\mid\varphi(g)=\mathrm{id}'\}$, where id$'$ is the identity element of G'. Prove that the kernel of φ is a subgroup of G.
   (e) Prove that $\ker\varphi$ is a normal subgroup of G.

(f) Consider $\bar{\varphi} : \frac{G}{\ker\varphi} \to \operatorname{im}\varphi$, which is given by $\bar{\varphi}(g\ker\varphi) = \varphi(g)$. Prove that $\bar{\varphi}$ is a **FUNCTION**. That is, if $g_1\ker\varphi$ and $g_2\ker\varphi$ are equal cosets, then prove that $\bar{\varphi}(g_1\ker\varphi) = \bar{\varphi}(g_2\ker\varphi)$.

(g) Prove that $\bar{\varphi}$ is a group homomorphism.

(h) Prove that $\bar{\varphi}$ is onto.

(i) Prove that $\bar{\varphi}$ is one-to-one.

In problem 58, you have proven the following very important Theorem.

The First Isomorphism Theorem *If $\varphi : G \to G'$ is a group homomorphism, then $\bar{\varphi} : \frac{G}{\ker\varphi} \to \operatorname{im}\varphi$, which is given by $\bar{\varphi}(g\ker\varphi) = \varphi(g)$, is a group isomorphism.*

(59) Let G be a cyclic group with generator g. Consider the function $\varphi : \mathbb{Z} \to G$ which is given by $\varphi(m) = g^m$ for all integers m.

(a) Prove that φ is a group homomorphism.

(b) Prove that φ is onto.

(c) If G is infinite, then prove that φ is an isomorphism.

(d) If G has finite order n, then prove that G is isomorphic to $\frac{\mathbb{Z}}{n\mathbb{Z}}$. (I strongly encourage you to use the First Isomorphism Theorem.)

(60) Let S and T be sets and let $\varphi : S \to T$ be a function. Suppose that φ is one-to-one and onto.

(a) Prove that there exists a FUNCTION $\theta : T \to S$ with $\varphi \circ \theta$ equal to the identity function on T and $\theta \circ \varphi$ equal to the identity function on S. (The function θ is usually called the inverse of φ.)

(b) Prove that the function θ of part (a) is one-to-one and onto.

(c) If S and T happen to be groups and φ happens to be a group homomorphism, then prove that θ is also a group homomorphism.

(61) Let $\varphi : G \to G'$ and $\varphi' : G' \to G''$ be group homomorphisms. Prove that $\varphi' \circ \varphi : G \to G''$ is a group homomorphism.

(62) Prove that the relationship "is isomorphic to" is an equivalence relation on the class of all groups. Recall that a relation $\sim$ on a class C is an *equivalence relation* if

(a) The relation $\sim$ is *reflexive*. If $c \in C$, then $c \sim c$.

(b) The relation $\sim$ is *symmetric*. If $c \sim c'$ for some c and c' in C, then $c' \sim c$.

(c) The relation $\sim$ is *transitive*. If $c \sim c'$ and $c' \sim c''$ for some c, c', c'' in C, then $c \sim c''$.

In problems 59 and 62, you have proven the following Theorem.

Theorem

(a) *If G and G' are infinite cyclic groups, then G and G' are isomorphic.*

(b) *If G and G' are cyclic groups of finite order n, then G and G' are isomorphic.*

(63) Let $\varphi : G \to G'$ be a group homomorphism. Prove that φ is one-to-one if and only if $\ker\varphi = \{\text{id}\}$.

(64) Let m and n be non-zero integers and let H be the subset

$$H = \{am + bn \mid a, b \in \mathbb{Z}\}$$

of $\mathbb{Z}$.

(a) Prove that H is a subgroup of $\mathbb{Z}$.

(b) We have shown that every subgroup of $\mathbb{Z}$ is cyclic. So H is cyclic. Let h_0 be a generator of H. (We can insist that h_0 is positive.) Prove that h_0 is a common divisor of m and n.

(c) Suppose that ℓ is an integer which happens to divide m and n. Prove that ℓ must also divide h_0.

(d) Notice that you have proven that h_0 is the greatest common divisor of m and n.

In problem 64, you have proven the following result.

Lemma from Number Theory. *If d is the greatest common divisor of the non-zero integers m and n, then there exist integers r and s so that*

$$d = rn + sm.$$

(65) Suppose m and n are relatively prime non-zero integers. Prove that the groups $\frac{\mathbb{Z}}{mn\mathbb{Z}}$ and $\frac{\mathbb{Z}}{m\mathbb{Z}} \times \frac{\mathbb{Z}}{n\mathbb{Z}}$ are isomorphic. (An algebraist calls this result the Chinese Remainder Theorem.)

(66) Let G be a cyclic group of order n; let g be a generator of G; and let H be a subgroup of G of order m. Lagrange's Theorem tells us that $m|n$. Let d equal the integer $\frac{n}{m}$. I want you to prove that H is the subgroup of G which is generated by g^d. I propose a couple of steps. First of all, we know that H is cyclic, so $H = \langle g^r \rangle$ for some integer r.

(a) Prove that $d|r$.

(b) Now you know that $H = \langle g^r \rangle \subseteq \langle g^d \rangle$. Finish the proof that $H = \langle g^d \rangle$.

(67) Define a group homomorphism from $\mathbb{Z} \times \mathbb{Z}$ onto $\mathbb{Z}$ whose kernel is the subgroup of $\mathbb{Z} \times \mathbb{Z}$ generated by $(0,1)$. Apply the First Isomorphism Theorem. (This problem gives a more sophisticated solution to problem 44 than you were able to give when you first did problem 44.)

(68) Define a group homomorphism from $\mathbb{Z} \times \mathbb{Z}$ onto $\mathbb{Z}$ whose kernel is the subgroup of $\mathbb{Z} \times \mathbb{Z}$ generated by $(1,1)$. Apply the First Isomorphism Theorem. (This problem gives a more sophisticated solution to problem 45 than you were able to give when you first did problem 45.)

(69) Consider $\varphi : \frac{\mathbb{Z}}{6\mathbb{Z}} \times \frac{\mathbb{Z}}{4\mathbb{Z}} \to \frac{\mathbb{Z}}{3\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}}$, given by

$$\varphi(a + 6\mathbb{Z}, b + 4\mathbb{Z}) = (a + 3\mathbb{Z}, b + 2\mathbb{Z}).$$

(a) Prove that φ is a function.

(b) Prove that φ is a group homomorphism.

(c) What are the image and kernel of φ?

(d) What does the First Isomorphism Theorem tell you?

Problem 69 gives a more sophisticated solution to problem 47 than you were able to give when you first did problem 47.

(70) Find a group homomorphism from $\mathbb{Z}\times\mathbb{Z}$ onto $\mathbb{Z}\times\frac{\mathbb{Z}}{2\mathbb{Z}}$, whose kernel is the subgroup of $\mathbb{Z}\times\mathbb{Z}$ which is generated by $(2,2)$. Apply the First Isomorphism Theorem.

(71) Exhibit an isomorphism $\phi : U \to G$, where U is the unit circle group and G is a subgroup of $\mathrm{GL}_2(\mathbb{R})$. Tell me what G is. Tell me what ϕ is. Prove that ϕ is an isomorphism.

(72) Exhibit an isomorphism $\phi : (\mathbb{R}\setminus\{0\},\times)\to(\mathbb{R}\setminus\{-2\},*)$, where $a*b = ab+2a+2b+2$. Tell me what ϕ is and prove that ϕ is an isomorphism.

(73) Let $H=\{\mathrm{id},a,b,c\}$ be a Klein 4-group with $a^2=b^2=c^2=\mathrm{id}$, $ab=ba=c$, $ac=ca=b$, and $bc=cb=a$. The group H has exactly 4 elements. Consider the function $\varphi : \mathbb{Z}\times\mathbb{Z}\to H$ which is given by $\varphi(m,n)=a^mb^n$. Prove that φ is a group homomorphism. Prove that φ is onto. What is the kernel of φ? What does the First Isomorphism Theorem tell you?

(74) Is the additive group $\mathbb{C}$ isomorphic to the multiplicative group $(\mathbb{C}\setminus\{0\},\times)$?

(75) Prove that every group with three elements is isomorphic to $\frac{\mathbb{Z}}{\langle 3\rangle}$.

(76) Find two Abelian groups of order 8 that are not isomorphic.

(77) Let C_2 be the subgroup $\{1,-1\}$ of $(\mathbb{R}\setminus\{0\},\times)$. Prove that $(\mathbb{R}\setminus\{0\},\times)$ is isomorphic to $(\mathbb{R}^{\mathrm{pos}},\times)\times C_2$, where $\mathbb{R}^{\mathrm{pos}}$ is the set of positive real numbers.

(78) Recall the group $(S,*)$ of problem (7). Prove that $(S,*)$ is isomorphic to $(\mathbb{R}\setminus\{0\},\times)$.

(79) Let G be a group, and let a be a fixed element of G. Define a function $\varphi_a : G\to G$ by $\varphi_a(x)=axa^{-1}$, for all $x\in G$. Prove that φ_a is an isomorphism.

(80) Let G be a group. Define $\varphi : G\to G$ by $\varphi(x)=x^{-1}$, for all $x\in G$.

(a) Prove that φ is one-to-one and onto.

(b) Prove that φ is an isomorphism if and only if G is Abelian.

(81) Define $\varphi : (\mathbb{C}\setminus\{0\},\times)\to(\mathbb{C}\setminus\{0\},\times)$ by $\varphi(a+bi)=a-bi$. Prove that φ is an isomorphism.

(82) Prove that $(\mathbb{C}\setminus\{0\},\times)$ is isomorphic to the subgroup of $\mathrm{GL}_2(\mathbb{R})$ which consists of all matrices of the form

$$\begin{bmatrix} a & b \\ -b & a \end{bmatrix}$$

with $a^2+b^2\neq 0$.

(83) Recall the group G of problem (6). Prove that G is isomorphic to the group $(\mathbb{R}\setminus\{0\},\times)$.

(84) Consider the following permutations in S_7:

$$\sigma=\begin{pmatrix}1&2&3&4&5&6&7\\3&2&5&4&6&1&7\end{pmatrix}\quad\text{and}\quad\tau=\begin{pmatrix}1&2&3&4&5&6&7\\2&1&5&7&4&6&3\end{pmatrix}.$$

(a) Compute $\sigma\circ\tau$.
(b) Write $\sigma\circ\tau$ as a product of disjoint cycles.
(c) Write σ and τ each as a product of transpositions.

(85) List all of the elements of S_4. Use cycle notation.

(86) Find the number of cycles of each possible length in S_5. Find all possible orders of elements in S_5. (Try to do this problem without listing all of the elements of S_5.)

(87) Let S be a set and let a be an element of S. Prove that

$$\{\sigma\in\mathrm{Sym}(S)\mid\sigma(a)=a\}$$

is a subgroup of $\mathrm{Sym}(S)$. Recall that $\mathrm{Sym}(S)$ is the group of permutations of S.