Section 4
Homework Assignment

#8. We can also consider multiplication in modulo n in $\mathbb{Z}_n$. For example, $5 \cdot_7 6 = 2$ in $\mathbb{Z}_7$ because $5 \cdot 6 = 30 = 4 \cdot 7 + 2$. The set $\{1, 3, 5, 7\}$ with multiplication in modulo 8 is a group. Give the table for this group.

Ans: As usual we write $\bar{1}, \bar{3}, \bar{5}, \bar{7}$ to denote the residue classes modulo 8:

$\cdot$	$\bar{1}$	$\bar{3}$	$\bar{5}$	$\bar{7}$
$\bar{1}$	$\bar{1}$	$\bar{3}$	$\bar{5}$	$\bar{7}$
$\bar{3}$	$\bar{3}$	$\bar{1}$	$\bar{7}$	$\bar{5}$
$\bar{5}$	$\bar{5}$	$\bar{7}$	$\bar{1}$	$\bar{3}$
$\bar{7}$	$\bar{7}$	$\bar{5}$	$\bar{3}$	$\bar{1}$

Note that this is the same table structure as the one of the Klein 4-group V_4, and the same as the one of $\mathbb{Z}_2 \times \mathbb{Z}_2$.

#19. Let S be the set of all real numbers except -1. Define $*$ on S by

$$a * b = a + b + ab$$

(a) Show that $*$ gives a binary operation on S.

(b) Show that $(S, *)$ is a group.

(c) Find the solution of the equation $2 * x * 3 = 7$ in S.

Ans. (a) We must show that S is closed under $*$, that is, that for all $a, b \in S$ one has $a * b \in S$. In other words, $a, b \neq -1$ implies $a * b \neq -1$. Suppose that $a * b = -1$, i.e. $a + b + ab = -1$. Then $a + ab + b + 1 = 0$ or $a(b+1) + b + 1 = 0$ or $(a+1)(b+1) = 0$. This implies that either $a = -1$ or $b = -1$. A contradiction.

(b) For all $a, b, c \in S$ we have

$$\begin{aligned} a * (b * c) &= a * (b + c + bc) \\ &= a + (b + c + bc) + a(b + c + bc) \\ &= a + b + c + bc + ab + ac + abc \\ &= (a + b + ab) + c + (a + b + ab)c \\ &= (a * b) * c \end{aligned}$$

This proves that the operation $*$

is "associative". Notice that we used the fact that "+" is commutative.

$0 \in S$ acts as "identity". Indeed, for all $a \in S$ we have

$$a * 0 = a + 0 + a \cdot 0 = a$$

$$0 * a = 0 + a + 0 \cdot a = a$$

We need to show that every element $a \in S$ has an "inverse". Who is the right candidate?

$a * ? = 0$ i.e. $a + ? + a ? = 0$

Solve for "?": $?(a+1) = -a$ $\therefore ? = \frac{-a}{a+1}$

Indeed we have that for all $a \in S$

$$\frac{-a}{a+1} * a = 0 = a * \frac{-a}{a+1} \quad \blacksquare$$

(c) Observe that "*" is commutative.

So $2 * x * 3 = 2 * 3 * x =$

$= (2 + 3 + 2 \cdot 3) * x = 11 * x$

Now, the inverse of 11 is $-\frac{11}{12}$

So that $2 * x * 3 = 7$ is equivalent to: $x = -\frac{11}{12} * 7 = \ldots = -1/3$.

#28. Let $\varphi: G \longrightarrow G'$ be a group isomorphism. By Theorem 3.14 one has that $\varphi(e) = e'$, where e is the identity of G and e' is the identity of G'. Show that for any $a \in G$ one has $\varphi(a)^{-1} = \varphi(a^{-1})$.

Ans. We recall that a^{-1} is the unique element of G such that

$$a a^{-1} = e = a^{-1} a$$

Thus, if we apply φ we obtain

$$e' = \varphi(e) = \varphi(a a^{-1}) = \varphi(a)\,\varphi(a^{-1})$$

$$e' = \varphi(e) = \varphi(a^{-1} a) = \varphi(a^{-1})\,\varphi(a)$$

Thus $\varphi(a^{-1})$ is an inverse for $\varphi(a)$. But, the inverse is unique so

$$\boxed{\varphi(a)^{-1} = \varphi(a^{-1})} \quad \text{for all } a \in G.$$

#31. If $*$ is a binary operation on a set S, an element x of S is an idempotent for $*$

if $x * x = x$. Prove that a group has exactly one idempotent element.

Ans. We denote the group with $(G, \cdot)$ rather than using $(G, *)$.

Notice that the identity $e \in G$ is such that:

$$e^2 = e \cdot e = e$$

so that G has at least one idempotent element.

Let x be another idempotent element: $x^2 = xx = x$.
But then, if we multiply the above equation by x^{-1} we obtain:

$$\begin{aligned} x^{-1}(xx) &= x^{-1}(x) \\ (x^{-1}x)\,x &= e \\ e\,x &= e \\ x &= e. \end{aligned}$$

This establishes the uniqueness of the idempotent.

#32. Show that every group G with identity e and such that $x * x = e$ for all $x \in G$ is abelian.

Ans. If we use "$\cdot$" instead of "$*$" we can rewrite the statement as:

"If $g^2 = e$ for all $g \in G$, then G is an abelian group"

Let $g_1, g_2 \in G$. Hence $g_1^2 = e$ and $g_2^2 = e$. But $g_1 g_2 \in G$ as well, so $(g_1 g_2)^2 = e$. Thus:

$$g_1^2 = e \qquad g_2^2 = e \qquad (g_1 g_2)^2 = e$$

We conclude that

$$g_1^2 g_2^2 = e \quad \text{and} \quad (g_1 g_2)(g_1 g_2) = e,$$

where $(g_1 g_2)(g_1 g_2) = (g_1 g_2)^2$!!

If we equate the above identities we obtain

$$g_1^2 g_2^2 = g_1 g_2 g_1 g_2 \qquad \text{or}$$

$$g_1 g_1 g_2 g_2 = g_1 g_2 g_1 g_2$$

Multiply on the left by g_1^{-1} and on the right by g_2^{-1} and obtain

$$g_1 g_2 = g_2 g_1$$

#34. Let G be a group with a finite number of elements. Show that for any $a \in G$, there exists an $n \in \mathbb{Z}^+$ such that $a^n = e$.

Ans. Note that a^n means $\underbrace{a \cdot a \cdot a \cdot \dots \cdot a}_{n\text{-times}}$.

Also, G has a finite number of elements.

The elements $e, a, a^2, a^3, \dots, a^n, \dots$ are all elements of G. They cannot be all different since G has a finite number, say m, of elements.

Thus we must have $a^i = a^j$ for some i, j with $i < j$.

Repeated cancellation (i times) of a, leads to

$$e = a^{j-i} \quad \text{so} \quad n = j - i .$$

#41. Let G be a group and let g be one fixed element of G. Show that the map i_g, such that $i_g(x) = gxg^{-1}$ for all $x \in G$ is an isomorphism of G with itself.

Ans. We need to show that the map

$$i_g : G \longrightarrow G, \quad \underset{\uparrow G}{x} \longmapsto i_g(x) = \underset{\uparrow G}{gxg^{-1}}$$

is: one-one; onto; morphism.

One-one: suppose $i_g(x_1) = i_g(x_2)$. I.e., $gx_1g^{-1} = gx_2g^{-1}$. But if we multiply on the left by g^{-1} and on the right by g^{-1}, we obtain

$$x_1 = x_2 .$$

onto: For any $y \in G$ we need to find an element $? \in G$ such that $i_g(?) = y$. Choose $?$ to be

$$g(?)g^{-1} = y \quad \text{or} \quad ? = \underline{g^{-1}yg} .$$

That is, $i_g(g^{-1}yg) = y$.

morphism : for all $x_1, x_2 \in G$ we have that :

$$i_g(x_1 x_2) = g(x_1 x_2) g^{-1} =$$

$$= g x_1 e x_2 g^{-1} =$$

$$= g x_1 (g^{-1} g) x_2 g^{-1} =$$

$$= (g x_1 g^{-1})(g x_2 g^{-1}) =$$

$$= i_g(x_1)\, i_g(x_2)$$

as desired.

i_g is called an "inner automorphism" or "conjugation by g".