HW2 Problem 1

- A <u>monoid without identity</u> is a set G with an operation $\times : G \times G \to G$ such that: if $a, b, c \in G$ then $(ab)c = a(bc)$.

  For example, the empty set $\emptyset$ is a monoid without identity. Also, the set $\{x_1, x_2\}$ with
  $$x_1x_1 = x_1x_2 = x_2x_1 = x_2x_2 = x_1$$
  is a monoid without identity.

- A <u>monoid</u> is a set G with an operation $\times : G \times G \to G$ such that:
  (a) if $a, b, c \in G$ then $(ab)c = a(bc)$,
  (b) there exists an element $1 \in G$ such that if $a \in G$ then $1a = a1 = a$.

  For example, the set of natural numbers with addition is a monoid. Also, for a set X, the set of functions
  $$\{f : X \to X\}$$
  with function composition is a monoid.

- A <u>group</u> is a set G with an operation $\times : G \times G \to G$ such that
  (a) if $a, b, c \in G$ then $(ab)c = a(bc)$,
  (b) there exists an identity element $1 \in G$ such that if $a \in G$ then $1a = a1 = a$.
  (c) if $a \in G$ there exists an element $y^{-1} \in G$ such that $yy^{-1} = y^{-1}y = 1$.

  For example, given a set X, the functions
  $$\{f : X \to X \mid f \text{ is bijective}\},$$
  is a group with function composition. Also, the set of integers mod 5 is a group with addition

HW 2 Problem 1 Con't

- A ring without identity is a set R with two operations $\times : R \times R \to R$ and $+ : R \times R \to R$ such that
  - (a) R with $+$ is an abelian group
  - (b) If $r, s \in R$ then $r+s = s+r$
  - (c) If $r, s, t \in R$ then $(rs)t = r(st)$
  - (d) If $r, s, t \in R$ then
$$r(s+t) = rs + rt$$
  and
$$(r+s)t = rt + st.$$

  For example, the set of even integers with addition a multiplication is a ring without identity.

- A ring is a ring without identity such that there is an element $1 \in R$ such that if $r \in R$ then $r1 = 1r = r$.
  For example, the set of $n \times n$ matrices with real entries is a ring.

- A field is a commutative ring $\mathbb{F}$ such that if $y \in \mathbb{F}$ and $y \neq 0$ then there is an element $y^{-1} \in \mathbb{F}$ with $yy^{-1} = y^{-1}y = 1$.
  For example, the set of real numbers, with multiplication and addition, is a field.

- A division ring is a ring $\mathbb{D}$ such that if $y \in \mathbb{D}$ and $y \neq 0$ then there is an element $y^{-1} \in \mathbb{D}$ with $yy^{-1} = y^{-1}y = 1$.
  For example, the quaternions are a division ring. Also, the set of invertible $n \times n$ matrices with real entries is a division ring.

<u>HW 2 Problem 2</u>: Give an example of an operation on $\mathbb{Z}$ that is not associative.

Define $\star : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ by

$$a \star b = ab + b$$

for all $a, b \in \mathbb{Z}$. Then $\star$ is not associative, since

$$(1 \star 2) \star 3 = 4 \star 3 = 15$$

but

$$1 \star (2 \star 3) = 1 \star 9 = 18.$$

<u>HW 2 Problem 3</u>: Let G be a group. Show that the identity element of G is unique.

<u>Proof</u>: Assume: G is a group.
To Show: identity elt of G is unique.
Assume: $x, y \in G$ are identity elements of G.
To Show: $x = y$.
Consider $xy \in G$. Then

$$xy = x$$

since x is an identity element of G.
But

$$xy = y$$

since y is an identity element of G.
Thus $x = y$.
So, if G is a group, then its identity element is unique.

HW 2 Problem 4 Let G be a group. Show that the inverse of g is unique

Proof: Assume: G is a group.
To Show: the inverse of G is unique.
Assume: $g \in G$, and $x, y \in G$ are both inverses of g.
To Show: $x = y$.
Note that

$$gx = gy = 1.$$

Thus

$$x(gx) = x(gy)$$
$$(xg)x = (xg)y$$
$$1x = 1y$$
$$x = y,$$

as desired. So the inverse of G is unique.

HW 2 Problem 5: Why isn't $\{0,1,2,3,4,5\}$ a group?

The above set is not a group since there is no binary operation specified.

HW 2 Problem 6: Show that $-(-5)=5$.

Proof: To Show: $-(-5)=5$.
That is, we wish to show:
(a) $(-5)+5=0$
(b) $5+(-5)=0$.
But (a) and (b) are true since -5 is the additive inverse of 5. Thus $-(-5)=5$.

HW2 Problem 7: Show that $1/(1/5)=5$

Proof: To Show: $1/(1/5)=5$
That is, we wish to show:
(a) $(1/5)5=1$
(b) $5(1/5)=1$.
But (a) and (b) are true since $1/5$ is the multiplicative inverse of 5.
Thus $1/(1/5)=5$.

HW 2 Problem 8: Show that $-1\cdot5=-5$.

Proof: To Show: $-1\cdot5=-5$
That is, we wish to show that $-1\cdot5$ is the additive inverse of 5. Since

$$\begin{aligned}-1\cdot5+5 &= -1\cdot5+1\cdot5\\ &= (-1+1)5\\ &= 0\cdot5 \qquad \text{(see problem 9)}\\ &= 0\end{aligned}$$

and similarly,

$$\begin{aligned}5+(-1\cdot5) &= (1\cdot5)+(-1\cdot5)\\ &= (1+(-1))5\\ &= 0\cdot5 \qquad \text{(see problem 9)}\\ &= 0,\end{aligned}$$

it follows that $-1\cdot5=-5$.

HW 2 Problem 9 : Show that $0 \cdot 5 = 0$

Proof : To Show : $0 \cdot 5 = 0$

Note that

$$
\begin{aligned}
0 \cdot 5 + 5 &= 0 \cdot 5 + 1 \cdot 5 \\
&= (0+1) \cdot 5 \\
&= 1 \cdot 5 \\
&= 5
\end{aligned}
$$

so

$$
\begin{aligned}
0 \cdot 5 + 5 &= 5 \\
0 \cdot 5 + 5 + (-5) &= 5 + (-5) \\
0 \cdot 5 + 0 &= 0 \\
0 \cdot 5 &= 0.
\end{aligned}
$$

So, $0 \cdot 5 = 0$.

HW 2 Problem 16 Let C_n be the set of n^{th} roots of unity in $\mathbb{C}$. Show that C_n is a group.

First write

$$C_n = \{ e^{2\pi i k/n} \mid 0 \le k \le n-1 \}$$

$$= \{ \xi^0, \xi^1, \ldots, \xi^{n-1} \}, \text{ where } \xi = e^{2\pi i/n}.$$

To show: C_n is a subgroup of $GL_1(\mathbb{C})$

To show: (a) If $g, h \in C_n$ then $gh \in C_n$.

(b) $1 \in C_n$

(c) If $g \in C_n$ then $g^{-1} \in C_n$.

(a) Assume $g, h \in C_n$

To show: $gh \in C_n$.

To show: gh is an n^{th} root of 1.

To show: $(gh)^n = 1$.

$(gh)^n = g^n h^n = 1 \cdot 1$, since $g, h \in C$ and g and h are n^{th} roots of 1.

So $gh \in C_n$.

(b) To show: 1 is an n^{th} root of 1

To show: $1^n = 1$.

This is clear, since $1 \cdot 1 \cdots 1 = 1$. //

(c) Assume $g \in C_n$.

To show: $g^{-1} \in C_n$.

To show: g^{-1} is a n^{th} root of unity.

To show: $(g^{-1})^n = 1$.

$(g^{-1})^n = g^{-n} = (g^n)^{-1} = 1^{-1} = 1$, since $g \in \mathbb{C}$ and $g^n = 1$.

So $g^{-1} \in C_n$.

So C_n is a subgroup of $GL_1(\mathbb{C})$. //

<u>HW2 Problem 17</u> Define $M_n(\mathbb{C})$ and prove that it is a ring.

$M_n(\mathbb{C})$ is the set of $n \times n$ matrices with entries in $\mathbb{C}$ with operations matrix addition and matrix multiplication.

To show: $M_n(\mathbb{C})$ is a ring.

To show: (a) If $a, b, c \in M_n(\mathbb{C})$ then $(a+b)+c = a+(b+c)$

(b) There exists an element $0 \in M_n(\mathbb{C})$ such that if $a \in M_n(\mathbb{C})$ then $0+a = a+0 = a$.

(c) If $a \in M_n(\mathbb{C})$ there exists an element $-a \in M_n(\mathbb{C})$ such that $a+(-a) = (-a)+a = 0$.

(d) If $a, b \in M_n(\mathbb{C})$ then $a+b=b+a$.

(e) If $a,b,c \in M_n(\mathbb{C})$ then $(ab)c = a(bc)$

(f) There exists an element $1 \in M_n(\mathbb{C})$ such that if $a \in M_n(\mathbb{C})$ then $1 \cdot a = a \cdot 1 = a$.

(g) If $a,b,c \in M_n(\mathbb{C})$ then $(a+b)c = ac+bc$ and
$a(b+c) = ab+ac$.

(a) Assume $a,b,c \in M_n(\mathbb{C})$.

To show: $(a+b)+c = a+(b+c)$.

To show: $((a+b)+c)_{ij} = (a+(b+c))_{ij}$.

$$((a+b)+c)_{ij} = (a+b)_{ij} + c_{ij} = (a_{ij}+b_{ij})+c_{ij}$$
$$= a_{ij}+(b_{ij}+c_{ij}) = a_{ij}+(b+c)_{ij} = (a+(b+c))_{ij}.$$

So $(a+b)+c = a+(b+c)$.

(e) Assume $a,b,c \in M_n(\mathbb{C})$.

To show: $(ab)c = a(bc)$.

To show: $((ab)c)_{ij} = (a(bc))_{ij}$.

$$((ab)c)_{ij} = \sum_{l=1}^{n} (ab)_{il} c_{lj} = \sum_{l=1}^{n} \left(\sum_{k=1}^{n} a_{ik} b_{kl} \right) c_{lj}$$

$$= \sum_{\ell=1}^{n} \sum_{k=1}^{n} a_{ik} b_{k\ell} c_{\ell j} = \sum_{k=1}^{n} \sum_{\ell=1}^{n} a_{ik} b_{k\ell} c_{\ell j}$$

$$= \sum_{k=1}^{n} a_{ik} \left(\sum_{\ell=1}^{n} b_{k\ell} c_{\ell j} \right) = \sum_{k=1}^{n} a_{ik} (bc)_{kj} = (a(bc))_{ij}.$$

(f) To show: There exists an element $1 \in M_n(\mathbb{C})$ such that if $a \in M_n(\mathbb{C})$ then $1 \cdot a = a \cdot 1 = a$.

Let 1 be the matrix with entries

$$1_{ij} = \begin{cases} 0, & \text{if } i \neq j \\ 1, & \text{if } i = j. \end{cases}$$

~~Then~~ To show: If $a \in M_n(\mathbb{C})$ then $1 \cdot a = a$ and $a \cdot 1 = a$.

Assume $a \in M_n(\mathbb{C})$

To show: (fa) $1 \cdot a = a$

(fb) $a \cdot 1 = a$.

(fa) To show: $(1 \cdot a)_{ij} = a_{ij}$.

$$(1 \cdot a)_{ij} = \sum_{k=1}^{n} 1_{ik} a_{kj} = 1_{i1} a_{1j} + 1_{i2} a_{2j} + \cdots + 1_{ii} a_{ij} + \cdots + 1_{in} a_{nj}$$

$$= 0 + 0 + \cdots + 1 \cdot a_{ij} + 0 + \cdots + 0 = a_{ij}.$$

(fb) To show: $(a \cdot 1)_{ij} = a_{ij}$.

$$(a \cdot 1)_{ij} = \sum_{k=1}^{n} a_{ik} 1_{kj} = a_{ij} \cdot 1_{jj} = a_{ij} \cdot 1 = a_{ij}.$$

HW2 Problem 12

Let $n \in \mathbb{Z}_{>0}$ and let $k \in \mathbb{Z}$.

<u>$k \bmod n$</u> is the integer $\bar{k}$ such that

$$k = \ell n + \bar{k}, \text{ with } \ell \in \mathbb{Z} \text{ and } 0 \le \bar{k} \le n-1.$$

$\mathbb{Z}/n\mathbb{Z} = \{0, 1, 2, \ldots, n-1\}$ with the operations determined by

$$\bar{a} + \bar{b} = \overline{a+b} \quad \text{and} \quad \bar{a}\bar{b} = \overline{ab}$$

for $a, b \in \mathbb{Z}$.

To show: $\mathbb{Z}/n\mathbb{Z}$ is a ring.

To show: (a) $+ : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ is well defined.

(b) $\cdot : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ is well defined

(c) If $\bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}/n\mathbb{Z}$ then
$(\bar{a}+\bar{b}) + \bar{c} = \bar{a} + (\bar{b}+\bar{c})$.

(d) There is an element $z \in \mathbb{Z}/n\mathbb{Z}$ such that if $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$ then $z + \bar{a} = \bar{a} + z = \bar{a}$.

(e) If $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$ then there exists an element $b \in \mathbb{Z}/n\mathbb{Z}$ such that $b + \bar{a} = \bar{a} + b = z$.

(f) If $\bar{a}, \bar{b} \in \mathbb{Z}/n\mathbb{Z}$ then $\bar{a} + \bar{b} = \bar{b} + \bar{a}$.

(g) If $\bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}/n\mathbb{Z}$ then $(\bar{a}\bar{b})\bar{c} = \bar{a}(\bar{b}\bar{c})$

(h) There exists an element $e \in \mathbb{Z}/n\mathbb{Z}$ such that if $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$ then $e\bar{a} = \bar{a}e = \bar{a}$

(i) If $\bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}/n\mathbb{Z}$ then

$(\bar{a}+\bar{b})\bar{c} = \bar{a}\bar{c} + \bar{b}\bar{c}$ and $\bar{c}(\bar{a}+\bar{b}) = \bar{c}\bar{a} + \bar{c}\bar{b}$.

(a) To show: $+ : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ is well defined.

Let $a_1, a_2, b_1, b_2 \in \mathbb{Z}$ such that $\bar{a}_1 = \bar{a}_2$ and $\bar{b}_1 = \bar{b}_2$.

To show: $\bar{a}_1 + \bar{b}_1 = \bar{a}_2 + \bar{b}_2$

We know: $a_1 = l_1 n + r$ and $a_2 = l_2 n + r$

$b_1 = k_1 n + s$ and $b_2 = k_2 n + s$

with $l_1, l_2, k_1, k_2 \in \mathbb{Z}$ and $0 \le r, s \le n-1$.

Then $\bar{a}_1 + \bar{b}_1 = \overline{a_1 + b_1} = \overline{l_1 n + r + k_1 n + s} = \bar{t}$,

if $r + s = ln + t$ with $l \in \mathbb{Z}$, $0 \le t \le n-1$.

Then $\bar{a}_2 + \bar{b}_2 = \overline{a_2 + b_2} = \overline{l_2 n + r + k_2 n + s} = \bar{t}$.

So $\bar{a}_1 + \bar{b}_1 = \bar{a}_2 + \bar{b}_2$.

(b) To show: $\cdot : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ is well defined.

Let $a_1, a_2, b_1, b_2 \in \mathbb{Z}$ such that $\bar{a}_1 = \bar{a}_2$ and $\bar{b}_1 = \bar{b}_2$.

To show: $\bar{a}_1 \bar{b}_1 = \bar{a}_2 \bar{b}_2$

We know: $a_1 = l_1 n + r$ and $a_2 = l_2 n + r$
$b_1 = k_1 n + s$ and $b_2 = k_2 n + s$

with $l_1, l_2, k_1, k_2 \in \mathbb{Z}$ and $0 \le r, s \le n-1$.

Then
$$\bar{a}_1 \bar{b}_1 = \overline{a_1 b_1} = \overline{(l_1 n + r)(l_2 n + s)} = t,$$

if $rs = ln + t$ with $l \in \mathbb{Z}$, $0 \le t \le n-1$.

Then $$\bar{a}_2 \bar{b}_2 = \overline{a_2 b_2} = \overline{(k_1 n + r)(k_2 n + s)} = t$$

So $\bar{a}_1 \bar{b}_1 = \bar{a}_2 \bar{b}_2$.

(c) To show: If $\bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}/n\mathbb{Z}$ then $(\bar{a} + \bar{b}) + \bar{c} = \bar{a} + (\bar{b} + \bar{c})$.

Assume $\bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}/n\mathbb{Z}$.

To show: $(\bar{a} + \bar{b}) + \bar{c} = \bar{a} + (\bar{b} + \bar{c})$

$$(\bar{a} + \bar{b}) + \bar{c} = \overline{a+b} + \bar{c} = \overline{(a+b)+c}, \text{ and}$$

$$\bar{a} + (\bar{b} + \bar{c}) = \bar{a} + (\overline{b+c}) = \overline{a+(b+c)}$$

and so, by associativity of + on $\mathbb{Z}$,

$$(\bar{a} + \bar{b}) + \bar{c} = \bar{a} + (\bar{b} + \bar{c}).$$

(d) To show: There exists an element $z \in \mathbb{Z}/n\mathbb{Z}$ such that if $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$ then $z + \bar{a} = \bar{a} + z = \bar{a}$.

Let $z = \bar{0}$.

To show: If $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$ then $z + \bar{a} = \bar{a} + z = \bar{a}$.

Assume $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$

To show: (da) $z + \bar{a} = \bar{a}$

(db) $\bar{a} + z = \bar{a}$.

(da) $z + \bar{a} = \bar{0} + \bar{a} = \overline{0+a} = \bar{a}$,

since 0 is the identity in $\mathbb{Z}$.

(db) $\bar{a} + z = \bar{a} + \bar{0} = \overline{a+0} = \bar{a}$,

since 0 is the identity in $\mathbb{Z}$.

(e) To show: If $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$ then there exists an element $b \in \mathbb{Z}/n\mathbb{Z}$ such that $b + \bar{a} = \bar{a} + b = z$.

Assume $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$

To show: There exists $b \in \mathbb{Z}/n\mathbb{Z}$ such that $b + \bar{a} = \bar{a} + b = z$.

Let $b = \overline{-a}$.

To show: (ea) $b + \bar{a} = z$

(eb) $\bar{a} + b = z$

(ea) $b + \bar{a} = \overline{-a} + \bar{a} = \overline{(-a)+a} = \bar{0} = z$,

since $-a$ is the inverse of a in $\mathbb{Z}$.

(eb) $\bar{a} + \bar{b} = \bar{a} + \overline{(-a)} = \overline{a + (-a)} = \bar{0} = z$

since $-a$ is the inverse of a in $\mathbb{Z}$.

(f) To show: If $\bar{a}, \bar{b} \in \mathbb{Z}/n\mathbb{Z}$ then $\bar{a} + \bar{b} = \bar{b} + \bar{a}$.

Assume $\bar{a}, \bar{b} \in \mathbb{Z}/n\mathbb{Z}$.

To show: $\bar{a} + \bar{b} = \bar{b} + \bar{a}$.

$\bar{a} + \bar{b} = \overline{a+b} = \overline{b+a} = \bar{b} + \bar{a}$,

by commutativity in $\mathbb{Z}$.

(g) To show: If $\bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}/n\mathbb{Z}$ then $(\bar{a}\bar{b})\bar{c} = \bar{a}(\bar{b}\bar{c})$

Assume $\bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}/n\mathbb{Z}$

To show: $(\bar{a}\bar{b})\bar{c} = \bar{a}(\bar{b}\bar{c})$

$(\bar{a}\bar{b})\bar{c} = \overline{ab} \cdot \bar{c} = \overline{(ab)c} = \overline{a(bc)} = \bar{a}\,\overline{bc} = \bar{a}(\bar{b}\bar{c})$,

by associativity of multiplication in $\mathbb{Z}$.

(h) To show: There exists an element $e \in \mathbb{Z}/n\mathbb{Z}$ such that if $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$ then $e\bar{a} = \bar{a}e = \bar{a}$.

Let $e = \bar{1}$.

To show: If $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$ then $e\bar{a} = \bar{a}e = \bar{a}$.

Assume $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$

To show: (ha) $e\bar{a} = \bar{a}$

(hb) $\bar{a}e = \bar{a}$.

(Ma) $e\bar{a} = \bar{1}\bar{a} = \overline{1 \cdot a} = \bar{a}$,

since 1 is the identity in $\mathbb{Z}$

(Mb) $\bar{a}e = \bar{a}\bar{1} = \overline{a \cdot 1} = \bar{a}$,

since 1 is the identity in $\mathbb{Z}$.

(i) To show: If $\bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}/n\mathbb{Z}$ then

$(\bar{a}+\bar{b})\bar{c} = \bar{a}\bar{c} + \bar{b}\bar{c}$ and $\bar{c}(\bar{a}+\bar{b}) = \bar{c}\bar{a} + \bar{c}\bar{b}$.

Assume $\bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}/n\mathbb{Z}$.

To show: (ia) $(\bar{a}+\bar{b})\bar{c} = \bar{a}\bar{c} + \bar{b}\bar{c}$

(ib) $\bar{c}(\bar{a}+\bar{b}) = \bar{c}\bar{a} + \bar{c}\bar{b}$.

(ia) $(\bar{a}+\bar{b})\bar{c} = (\overline{a+b})\bar{c} = \overline{(a+b)c}$

$= \overline{ac+bc} = \overline{ac} + \overline{bc} = \bar{a}\bar{c} + \bar{b}\bar{c}$,

by distributivity in $\mathbb{Z}$.

(ib) $\bar{c}(\bar{a}+\bar{b}) = \bar{c}(\overline{a+b}) = \overline{c(a+b)} = \overline{ca+cb}$

$= \overline{ca} + \overline{cb} = \bar{c}\bar{a} + \bar{c}\bar{b}$.

So $\mathbb{Z}/n\mathbb{Z}$ is a ring.