1, 2 in your notes

3. Let $A = [0,2]$, $B = [-1,6]$. Show $f: A \to B$ is a bijection where $f(x) = \frac{7}{2}x - 1$. What does this fact tell us about the sets A and B?

f is a bijection

Proof First we will show f is injective.

Let $a_1, a_2 \in A$ so that $f(a_1) = f(a_2)$.

Thus $\frac{7}{2}a_1 - 1 = \frac{7}{2}a_2 - 1$ by def of f

$\frac{7}{2}a_1 = \frac{7}{2}a_2$

$a_1 = a_2$

Therefore, f is injective.

Now we will show f is onto. Let $b \in [-1,6]$.

Thus $-1 \leq b \leq 6$

$0 \leq b+1 \leq 7$

$0 = \frac{2}{7}(0) \leq \frac{2}{7}(b+1) \leq \frac{2}{7}(7) = 2.$

Let $a = \frac{2}{7}(b+1)$. Note $a \in [0,2]$. Also note

$f(a) = \frac{7}{2}a - 1 = \frac{7}{2}\left(\frac{2}{7}(b+1)\right) - 1$

$= (b+1) - 1 = b.$

So f is onto. THEREFORE f is a bijection. ☐

Since $f: A \to B$ is a bijection we have $A \sim B$.

4. (in notes)

5. We will show the set of irrationals is uncountable.

Proof. First recall $\mathbb{R}$ is uncountable. Assume $\mathbb{J} = \mathbb{R} \setminus \mathbb{Q}$ is countable (toward a contradiction). Recall $\mathbb{Q}$ is countable. Also recall a previous proposition

"IF A, B are countable then $A \cup B$ is countable"

For $A = \mathbb{J}$ and $B = \mathbb{Q}$ we have two countable sets, so by the proposition $A \cup B$ is countable.

But $A \cup B = \mathbb{J} \cup \mathbb{Q}$

$= (\mathbb{R} \setminus \mathbb{Q}) \cup \mathbb{Q} = \mathbb{R}$.

So $\mathbb{R}$ is countable, a contradiction to $\mathbb{R}$ being uncountable. Therefore our assumption is false, That is $\mathbb{J} = \mathbb{R} \setminus \mathbb{Q}$ is uncountable. ∎

(6.) Let $a, b, c \in \mathbb{Z}$ with $b \neq 0$.

If $a|b$ AND $b|c$ then $a|c$.

Proof Let $a, b, c \in \mathbb{Z}$ with $b \neq 0$. Assume $a|b$ and $b|c$.

So $\exists\ k, \ell \in \mathbb{Z}$ so that $b = ak$ AND $c = b\ell$.

Thus $c = b\ell$

$= (ak)\ell$ since $b = ak$

$= a(k\ell)$.

Since $k\ell \in \mathbb{Z}$ we have $a|c$. ∎

(7.) Let $a, b, c, x, y \in \mathbb{Z}$

If $a|b$ AND $a|c$ then $a|bx+cy$.

Proof Let $a, b, c, x, y \in \mathbb{Z}$ so that $a|b$ AND $a|c$

Thus $b = ak$ AND $c = a\ell$ for some $k, \ell \in \mathbb{Z}$. Note

$bx + cy = (ak)x + (a\ell)y$

$= a(kx + \ell y)$.

Since $kx + \ell y \in \mathbb{Z}$ we have $a|bx+cy$. ∎

(8.) Let $a, b, c, d \in \mathbb{Z}$.

If $a|b$ and $c|d$ then $ac|ad+bc$.

Proof. Let $a, b, c, d \in \mathbb{Z}$. Assume $a|b$ and $c|d$

So $\exists\ k, \ell \in \mathbb{Z}$ so that $b = ak$ and $d = c\ell$. Note

$ad + bc = a(c\ell) + (ak)c$

$= ac[\ell + k]$.

Since $k + \ell \in \mathbb{Z}$ we have $ac|ad+bc$. ∎

). Let $n \in \mathbb{Z}$. Then $3 \mid n^3 - n$.

Proof. Let $n \in \mathbb{Z}$. By the division algorithm

$$n = 3q + r$$

where $r \in \{0, 1, 2\}$ and $q \in \mathbb{Z}$.

CASE 1. Let $r = 0$. So $n = 3q + 0 = 3q$. Thus

$n^3 - n = (3q)^3 - 3q = 3(9q^3 - q)$. Since $9q^3 - q \in \mathbb{Z}$ we have $3 \mid n^3 - n$.

CASE 2. Let $r = 1$. So $n = 3q + 1$. Thus

$$n^3 - n = (3q+1)^3 - (3q+1)$$
$$= 27q^3 + 27q^2 + 9q + 1 - 3q - 1$$
$$= 27q^3 + 27q^2 + 6q = 3(9q^3 + 9q^2 + 2q)$$

Since $9q^3 + 9q + 2q \in \mathbb{Z}$, $3 \mid n^3 - n$.

CASE 3. Let $r = 2$. So $n = 3q + 2$. Thus

$$n^3 - n = (3q+2)^3 - (3q+2)$$
$$= 27q^3 + 54q^2 + 36q + 8 - 3q - 2$$
$$= 27q^3 + 54q^2 + 33q + 6$$
$$= 3[9q^3 + 18q^2 + 11q + 2].$$

Since $9q^3 + 18q^2 + 11q + 2 \in \mathbb{Z}$, $3 \mid n^3 - n$.

Since in all three cases $3 \mid n^3 - n$, so $3 \mid n^3 - n$ for all $n \in \mathbb{Z}$. ■

12. Let $a,b,c \in \mathbb{Z}$ where $\gcd(a,b)=1$.
If $a|c$ AND $b|c$ then $ab|c^2$.

Proof Let $a,b,c \in \mathbb{Z}$ where $\gcd(a,b)=1$. Also assume $a|c$ AND $b|c$. Since $\gcd(a,b)=1$ by the GCD Theorem $\exists\ x,y \in \mathbb{Z}$ so that

$$ax+by=1 \quad (*)$$

Also since $a|c$, and $b|c$ we have $c=ak$ AND $c=b\ell$ for some $k,\ell \in \mathbb{Z}$.

So note $c = c(1) = c(ax+by)$ by $(*)$

$$= cax + cby$$
$$= (b\ell)ax + (ak)by$$
$$= ab[\ell x + ky].$$

Since $\ell x + ky \in \mathbb{Z}$ we have $ab|c$. ∎

14. Let $n \in \mathbb{Z}$ be odd. Prove $n^2 \equiv 1 \bmod 8$.

Proof Let $n \in \mathbb{Z}$ be odd. By the division algorithm we have $n = 8q+r$ where $r \in \{0,1,2,\cdots,7\}$ and $q \in \mathbb{Z}$. N

Since n is odd AND $8q+0$, $8q+2$, $8q+4$, and $8q+6$ are all even $r \in \{1,3,5,7\}$. So we will show in four cases that $n^2 \equiv 1 \bmod 8$.

CASE 1 Let $r=1$. So $n = 8q+1$. Thus $n^2 \equiv (8q+1)^2 \bmod 8$

$$\equiv 64q^2 + 16q + 1 \bmod 8$$
$$= 0 + 0 + 1 \bmod 8 \quad \text{since } 64 \equiv 0 \bmod 8 \text{ \& } 16 \equiv 0 \bmod 8$$
$$\equiv 1 \bmod 8.$$

(You repeat for cases 2, 3, 4 . . .)

15. Let $a, b, c \in \mathbb{Z}$ so that $a^2 + b^2 = c^2$.

Then $4 \mid ab$.

Proof. By problem 14 we have $n^2 \equiv 1 \bmod 8$ for $n \in \mathbb{Z}$ with n odd. Also it can be shown* if n is even then n^2 is either 0 or $4 \bmod 8$. So we can check all possibilites for $a^2 + b^2 \equiv c^2 \bmod 8$ where $a^2, b^2 \equiv 0, 1$ or $4 \bmod 8$.

a) $0 + 1 \equiv 1 \bmod 8$

b) $1 + 1 \equiv 2 \bmod 8$ X Not possible

(c) $4 + 1 \equiv 5 \bmod 8$ X Not possible

(d) $0 + 0 \equiv 0 \bmod 8$

(e) $1 + 0 \equiv 1 \bmod 8$

(f) $4 + 0 \equiv 4 \bmod 8$

(g) $0 + 4 \equiv 4 \bmod 8$

(h) $1 + 4 \equiv 5 \bmod 8$ X not possible

(i) $4 + 4 \equiv 0 \bmod 8$

CASE I Either $a^2 \equiv 0 \bmod 8$ or $b^2 \equiv 0 \bmod 8$. Assume $a^2 \equiv 0 \bmod 8$, So (cases a, d, e, f, g)

$4 \mid a$. Thus $4 \mid a \cdot b$.

CASE II Assume $a^2 \equiv 4 \bmod 8$ AND $b^2 \equiv 4 \bmod 8$. Thus $2 \mid a$ AND $2 \mid b$ (case i)

∴ so $4 \mid a \cdot b$.

We don't need to check cases b, c, h (why?). Thus

$4 \mid ab$. ∎

(16.) use problem 14.

(17.) from class

(18.) in class

19-23 definitions from class

24 in class

(25.) (a) $(\mathbb{Q}^*, \cdot)$ is a group

Proof: We will show $\mathbb{Q}^*$ satisfies G1, G2, and G3.

G1 Let $a, b, c \in \mathbb{Q}^*$. Then $(ab)c = a(bc)$ since multiplication over $\mathbb{Q}$ is associative.

G2. Note 1, the multiplicative identity, is in $\mathbb{Q}^*$.

G3 Let $q \in \mathbb{Q}^*$. So $q = \frac{a}{b}$ where $b \neq 0$ (since $\frac{a}{b} \in \mathbb{Q}$) and $a \neq 0$ since $\frac{a}{b} \neq 0$. So $\frac{b}{a} \in \mathbb{Q}$ AND $\frac{b}{a} \neq 0$.

Thus $q^{-1} = \frac{b}{a} \in \mathbb{Q}^*$

Since $(\mathbb{Q}^*, \cdot)$ satisfies G1, G2 AND G3 we have $(\mathbb{Q}^*, \cdot)$ is a group. ∎

25.(b) $(\mathbb{Z}, \odot)$ where $a \odot b = a+b-2$. is a group

Proof We will show $(\mathbb{Z}, \odot)$ satisfies G1, G2 AND G3.

G1 Let $a, b, c \in \mathbb{Z}$ and note

$$(a \odot b) \odot c = (a+b-2) \odot c$$

$$= (a+b-2) + c - 2 = a+b+c-4$$

Also note

$$a \odot (b \odot c) = a \odot (b+c-2) = a + (b+c-2) - 2$$

$$= a+b+c-4$$

Thus $(a \odot b) \odot c = a \odot (b \odot c)$. So $(\mathbb{Z}, \odot)$ satisfies G1.

G2 Notice $e = 2$ since for all $a \in \mathbb{Z}$ we have

$$2 \odot a = 2+a-2 = a$$

and $$a \odot 2 = a+2-2 = a.$$

Thus $e = 2$ is the identity of $(\mathbb{Z}, \odot)$.

G3 Let $a \in \mathbb{Z}$. Note $b = 4-a \in \mathbb{Z}$. Also note

$$a \odot b = a + b - 2 = a + (4-a) - 2 = 2 = e$$

and $$b \odot a = b + a - 2 = (4-a) + a - 2 = 2 = e.$$

Thus b is the inverse of a and therefore $(\mathbb{Z}, \odot)$ satisfies G3.

Since $(\mathbb{Z}, \odot)$ satisfies G1, G2 AND G3 we have $(\mathbb{Z}, \odot)$ is a group. ∎

(25) (c) NOT a group

Note $e = 0$ but $1 \in \mathbb{Z}$ AND

$1 * a = e$ has no solution in $\mathbb{Z}$

$1 * a = e$

$1 \cdot a + 1 + a = 0$

$2a = -1 \Rightarrow a = \frac{-1}{2}$. Thus 1 has no inverse in $\mathbb{Z}$.

Therefore, $(\mathbb{Z}, *)$ is NOT a group.

(25) (d) is a group

You can prove this. Again $e = 0$

AND the inverse of a is $\frac{-a}{1+a}$.

(27) (a) Show $\mathbb{Z}_4 \cong \mathbb{Z}_5^*$

$\mathbb{Z}_4 = \{0, 1, 2, 3\}$ AND $\mathbb{Z}_5^* = \{1, 2, 3, 4\}$

$0 \xrightarrow{f} 1$

$1 \longrightarrow 2$

$2 \nearrow 3$

$3 \searrow 4$

This f is an isomorphism, How did I find it?

Verify a few possibilities

$f(2+3) = f(5) = f(1) = 2$ | $f(2) \cdot f(3) = 4 \cdot 3 \equiv 12 \equiv 2 \pmod 5$ ✓

(27) (b) $(\mathbb{Z}_2, +)$ $(M, \cdot)$

$0 \xrightarrow{f} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

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

verify yourself.

(27) (c) $(\mathbb{Z}_{12}^*, \cdot) \cong (\mathbb{Z}_2 \times \mathbb{Z}_2, +)$

$\mathbb{Z}_{12}^* = \{1, 5, 7, 11\}$

$\mathbb{Z}_2 \times \mathbb{Z}_2 = \{(0,0), (0,1), (1,0), (1,1)\}$

f

$1 \to (0,0)$

$5 \to (1,0)$

$7 \to (0,1)$

$11 \to (1,1)$

Verify (a) $f(5 \cdot 7) = f(5) + f(7)$

(b) $f(11 \cdot 11) = f(11) + f(11)$

(c) $f(11 \cdot 5) = f(11) + f(5)$

(28) a, b, d in class

(c) Let $a \in G$, a group. Then $(a^{-1})^{-1} = a$.

Proof Let $a \in G$. Then $b = (a^{-1})^{-1}$ satisfies

$b(a^{-1}) = e$

and $(a^{-1})b = e$.

Note $b = a$ satisfies the above equations.

$b = (a^{-1})^{-1} = a$.

(29) Let G be a group. Let $a, b \in G$.

If $ab = ba$ then $a^{-1}b^{-1} = b^{-1}a^{-1}$.

Pf: Let G be group and let $a, b \in G$ so that

$$ab = ba.$$

Thus $(ab)^{-1} = (ba)^{-1}$ so $b^{-1}a^{-1} = a^{-1}b^{-1}$. ☑

By prop $((AB)^{-1} = B^{-1}A^{-1})$

30, 31 very easy

(32.) in class

(33.) Same as showing $(E, +)$ was a subgroup from class.

(35, 36) we did in class