

HW3 Problem 1

An abelian group is a group G such that
if $g_1, g_2 \in G$ then $g_1 g_2 = g_2 g_1$.

The group $\mathbb{Z}/98\mathbb{Z}$ is abelian.

The group S_3 is not abelian since

$$\begin{matrix} X & 1 \\ X & X \end{matrix} = * \quad \text{and} \quad \begin{matrix} X & X \\ X & 1 \end{matrix} = 1X.$$

HW3 Problem 2

An $n \times n$ permutation matrix is an $n \times n$ matrix such that there is exactly one 1 in each row and each column and all other entries are 0.

The symmetric group S_n is the set of $n \times n$ permutation matrices with operation matrix multiplication.

HW3 Problem 3

A cyclic group is a group generated by one element.

The cyclic groups are

$$C_n = \{1, g, g^2, \dots, g^{n-1}\} \text{ with } g^n = 1$$

and

$$C_\infty = \{\dots, g^{-2}, g^{-1}, 1, g, g^2, \dots\}.$$

Note that $C_n \cong \mathbb{Z}/n\mathbb{Z}$ and $C_\infty \cong \mathbb{Z}$.

HW3 Problem 4 Let $n \in \mathbb{Z}_{>0}$.

The dihedral group D_n is the group generated by a and b with operation determined by

$$a^n = 1, b^2 = 1 \text{ and } ba = a^{n-1}b.$$

HW3 Problem 5

The Klein 4 group is the group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

HW3 Problem 6

Let G and H be groups.

The product of G and H is the set

$$G \times H = \{(g, h) \mid g \in G, h \in H\}$$

with operation given by

$$(g_1, h_1)(g_2, h_2) = (g_1 g_2, h_1 h_2).$$

If $H = \{1\}$ then $G \times \{1\} \subseteq G$.

Similarly, if $G = \{1\}$ then $\{1\} \times H \subseteq H$.

So every group G is a product, $G \times \{1\}$.

The smallest example which is not of this form is the

Klein 4 group, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

HW3 Problem 8 See HW3 Problem 2.

HW3 Problem 10

Let G be a group.

A subgroup of G is a subset H of G such that

(a) If $h_1, h_2 \in H$ then $h_1 h_2 \in H$

(b) $1 \in H$

(c) If $h \in H$ then $h^{-1} \in H$.

Some examples are

$$SL_n(\mathbb{C}) \subseteq GL_n(\mathbb{C}), \quad S_n \subseteq O_n(\mathbb{C}), \quad \mathbb{Z} \subseteq \mathbb{Q},$$

$$\mathbb{Z}/2\mathbb{Z} \times \{0\} \subseteq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

Another example is the subgroup

$$\{111, X, X\} \subseteq S_3.$$

Here, $\{111, X, X\} = \mathbb{Z}/3\mathbb{Z}.$

HW3 Problem 11

Let S and T be sets

The sets S and T have equal cardinality if there exists a bijection $\varphi: S \rightarrow T.$

Write $\text{Card}(S) = \text{Card}(T)$ if S and T have equal cardinality.

HW3 Problem 12

Let S be a set.

The set S is finite if $\text{Card}(S) = \text{Card}(\mathbb{Z}/n\mathbb{Z})$ for some $n \in \mathbb{Z}_{>0}.$

The set S is countable if S is finite or $\text{Card}(S) = \text{Card}(\mathbb{Z})$

The set S is infinite if S is not finite.

The set S is uncountable if S is not countable.

HW3 Problem 13

(5)

Show that $\text{Card}(\mathbb{Z}_{70}) = \text{Card}(\mathbb{Z}_{70})$.

Proof

To show: $\text{Card}(\mathbb{Z}_{70}) = \text{Card}(\mathbb{Z}_{70})$

To show: There exists a bijection $\varphi: \mathbb{Z}_{70} \rightarrow \mathbb{Z}_{70}$.

Let $\varphi: \mathbb{Z}_{70} \rightarrow \mathbb{Z}_{70}$ be given by

$$\varphi(i) = i-1.$$

To show: φ is a bijection.

To show: The inverse function to φ exists.

Let $\varphi^{-1}: \mathbb{Z}_{70} \rightarrow \mathbb{Z}_{70}$ be given by

$$\varphi^{-1}(j) = j+1.$$

To show: (a) $\varphi \circ \varphi^{-1} = \text{id}_{\mathbb{Z}_{70}}$

(b) $\varphi^{-1} \circ \varphi = \text{id}_{\mathbb{Z}_{70}}$.

~~Assume~~
(a) ~~If $j \in \mathbb{Z}_{70}$.~~ To show: If $j \in \mathbb{Z}_{70}$ then

$$(\varphi \circ \varphi^{-1})(j) = \text{id}_{\mathbb{Z}_{70}}(j).$$

Assume $j \in \mathbb{Z}_{70}$.

To show: $(\varphi \circ \varphi^{-1})(j) = \text{id}_{\mathbb{Z}_{70}}(j)$.

$$(\varphi \circ \varphi^{-1})(j) = \varphi(\varphi^{-1}(j)) = \varphi(j+1) = j+1-1 = j = \text{id}_{\mathbb{Z}_{70}}(j).$$

$$\square (\varphi \circ \varphi^{-1})(j) = \text{id}_{\mathbb{Z}_{70}}(j).$$

$\circlearrowleft \varphi \circ \varphi^{-1} = 2_{\mathbb{Z}_{70}}$

(b) To show: $(\varphi^{-1} \circ \varphi) = 2_{\mathbb{Z}_{70}}$.

To show: If $i \in \mathbb{Z}_{70}$ then $(\varphi^{-1} \circ \varphi)(i) = 2_{\mathbb{Z}_{70}}(i)$

Assume $i \in \mathbb{Z}_{70}$.

To show: $(\varphi^{-1} \circ \varphi)(i) = 2_{\mathbb{Z}_{70}}(i)$.

$(\varphi^{-1} \circ \varphi)(i) = \varphi^{-1}(\varphi(i)) = \varphi^{-1}(i-1) = i-1+1 = i = 2_{\mathbb{Z}_{70}}(i)$.

$\circlearrowleft (\varphi^{-1} \circ \varphi)(i) = 2_{\mathbb{Z}_{70}}(i)$

$\circlearrowleft \varphi^{-1} \circ \varphi = 2_{\mathbb{Z}_{70}}$

\circlearrowleft the inverse to φ exists.

$\circlearrowleft \varphi$ is a bijection

$\circlearrowleft \text{Card}(\mathbb{Z}_{70}) = \text{Card}(\mathbb{Z}_{70})$.

HW3 Problem 18 Let G and H be groups

A group homomorphism from G to H is a function $\varphi: G \rightarrow H$ such that

(a) If $g_1, g_2 \in G$ then $\varphi(g_1 g_2) = \varphi(g_1) \varphi(g_2)$

(b) $\varphi(1) = 1$,

(c) If $g \in G$ then $\varphi(g^{-1}) = \varphi(g)^{-1}$.

(7)

An isomorphism between G and H is a homomorphism $\varphi: G \rightarrow H$ such that

- (a) $\varphi^{-1}: H \rightarrow G$ exists
- (b) φ^{-1} is a group homomorphism.

The function

$$\det: GL_n(\mathbb{C}) \rightarrow GL_1(\mathbb{C})$$

is a homomorphism.

The ^{homomorphism} ~~function~~ $\varphi: S_3 \rightarrow D_3$ determined given by

$$\varphi(X) = a \text{ and } \varphi(X1) = b$$

is an isomorphism.

HW3 Problem 21

Let $\varphi: G \rightarrow H$ be a group homomorphism.

The kernel of φ is

$$\ker \varphi = \{g \in G \mid \varphi(g) = 1\}$$

The image of φ is

$$\text{im } \varphi = \{\varphi(g) \mid g \in G\}.$$

To show: (a) $\ker \varphi$ is a subgroup of G

(b) $\text{im } \varphi$ is a subgroup of H .

⑧

(a) To show: (aa) If $g_1, g_2 \in \ker \varphi$ then $g_1 g_2 \in \ker \varphi$

(ab) $1 \in \ker \varphi$

(ac) If $g \in \ker \varphi$ then $g^{-1} \in \ker \varphi$.

(aa) Assume $g_1, g_2 \in \ker \varphi$.

To show: $g_1 g_2 \in \ker \varphi$.

We know $\varphi(g_1) = 1$ and $\varphi(g_2) = 1$.

To show: $\varphi(g_1 g_2) = 1$.

$$\begin{aligned}\varphi(g_1 g_2) &= \varphi(g_1) \varphi(g_2), \text{ since } \varphi \text{ is a homomorphism,} \\ &= 1 \cdot 1 = 1.\end{aligned}$$

∴ $g_1 g_2 \in \ker \varphi$.

(ab) To show: $1 \in \ker \varphi$.

To show: $\varphi(1) = 1$.

This follows from condition (b) in the definition of homomorphism.

(ac) To show: If $g \in \ker \varphi$ then $g^{-1} \in \ker \varphi$.

Assume $g \in \ker \varphi$.

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

We know: $\varphi(g) = 1$.

9

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

$$\begin{aligned} \varphi(g^{-1}) &= \varphi(g)^{-1}, \text{ since } \varphi \text{ is a homomorphism} \\ &= 1^{-1}, \text{ since } g \in \ker \varphi, \\ &= 1, \text{ since } 1 \cdot 1 = 1. \end{aligned}$$

So $g^{-1} \in \ker \varphi$.

So $\ker \varphi$ is a subgroup of G .

(b) To show: $\text{im } \varphi$ is a subgroup of H .

To show: (ba) If $h_1, h_2 \in \text{im } \varphi$ then $h_1 h_2 \in \text{im } \varphi$.

(bb) $1 \in \text{im } \varphi$.

(bc) If $h \in \text{im } \varphi$ then $h^{-1} \in \text{im } \varphi$.

(ba) Assume $h_1, h_2 \in \text{im } \varphi$.

To show: $h_1 h_2 \in \text{im } \varphi$.

We know that there exist $g_1, g_2 \in G$ such that $\varphi(g_1) = h_1$ and $\varphi(g_2) = h_2$.

To show: There exists $k \in G$ such that $\varphi(k) = h_1 h_2$.

Let $k = g_1 g_2$.

To show: $\varphi(k) = h_1 h_2$

$$\varphi(k) = \varphi(g_1 g_2) = \varphi(g_1) \varphi(g_2) = h_1 h_2$$

So $h_1 h_2 \in \text{im } \varphi$.

(10)

(bb) To show: $1 \in \text{im } \varphi$.

To show: There exists $k \in G$ such that $\varphi(k) = 1$.

Let $k = 1$.

To show: $\varphi(k) = 1$

$\varphi(k) = \varphi(1) = 1$, since φ is a homomorphism.

So $1 \in \text{im } \varphi$.

(bc) To show: If $h \in \text{im } \varphi$ then $h^{-1} \in \text{im } \varphi$.

Assume $h \in \text{im } \varphi$

To show: $h^{-1} \in \text{im } \varphi$.

We know that there exists $g \in G$ such that

$$\varphi(g) = h.$$

To show: There exists $k \in G$ such that $\varphi(k) = h^{-1}$.

Let $k = g^{-1}$.

To show: $\varphi(k) = h^{-1}$.

$$\begin{aligned} \varphi(k) &= \varphi(g^{-1}) = \varphi(g)^{-1}, \text{ since } \varphi \text{ is a homomorphism,} \\ &= h^{-1}, \text{ since } \varphi(g) = h. \end{aligned}$$

So $h^{-1} \in \text{im } \varphi$.

So $\text{im } \varphi$ is a subgroup of H . //

HW3 Problem 22

Let G and H be groups and let $\varphi: G \rightarrow H$ be a function such that

$$\text{if } g_1, g_2 \in G \text{ then } \varphi(g_1 g_2) = \varphi(g_1) \varphi(g_2).$$

Show that $\varphi(1) = 1$.

Proof Assume G and H are groups and $\varphi: G \rightarrow H$ is a function such that if $g_1, g_2 \in G$

$$\text{then } \varphi(g_1 g_2) = \varphi(g_1) \varphi(g_2).$$

To show: $\varphi(1) = 1$.

~~Let~~ ~~let~~ $g \in G$. Then

~~$$\varphi(1) = \varphi(g g^{-1}) = \varphi(g)$$~~

~~$$\varphi(1) = \varphi(1) \cdot \varphi(1)$$~~

$$\varphi(1) = \varphi(1 \cdot 1) = \varphi(1) \cdot \varphi(1).$$

Since H is a group $\varphi(1)^{-1} \in H$. ~~So~~ Multiply on the right by $\varphi(1)^{-1}$ to get

$$\varphi(1) \varphi(1)^{-1} = \varphi(1) \cdot \varphi(1) \varphi(1)^{-1}$$

$$\delta \quad 1 = \varphi(1) \cdot 1 = \varphi(1).$$

$$\delta \quad \varphi(1) = 1.$$

HW3 Problem 23

(12)

Let G and H be groups and let $\varphi: G \rightarrow H$ be a function such that

$$\text{if } g_1, g_2 \in G \text{ then } \varphi(g_1 g_2) = \varphi(g_1) \varphi(g_2).$$

Show that if $g \in G$ then $\varphi(g^{-1}) = \varphi(g)^{-1}$.

Proof Assume G and H are groups and $\varphi: G \rightarrow H$ is a function such that if $g_1, g_2 \in G$ then

$$\varphi(g_1 g_2) = \varphi(g_1) \varphi(g_2).$$

To show: If $g \in G$ then $\varphi(g^{-1}) = \varphi(g)^{-1}$.

Assume $g \in G$

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

To show: $\varphi(g^{-1})$ is the inverse of $\varphi(g)$.

To show: (a) $\varphi(g^{-1}) \varphi(g) = 1$

(b) $\varphi(g) \varphi(g^{-1}) = 1$.

(a) $\varphi(g^{-1}) \varphi(g) = \varphi(g^{-1} g) = \varphi(1) = 1$, by Problem 22

(b) $\varphi(g) \varphi(g^{-1}) = \varphi(g g^{-1}) = \varphi(1) = 1$, by Problem 22.

So $\varphi(g^{-1})$ is the inverse of $\varphi(g)$.

So $\varphi(g^{-1}) = \varphi(g)^{-1}$. \square

HW3 Problem 24 Let φ be a field homomorphism.

Show that φ is injective.

Proof:

Assume F and K are fields and $\varphi: F \rightarrow K$ is a field homomorphism.

To show: $\varphi: F \rightarrow K$ is injective.

To show: If $c_1, c_2 \in F$ and $\varphi(c_1) = \varphi(c_2)$ then $c_1 = c_2$.

Assume $c_1, c_2 \in F$ and $\varphi(c_1) = \varphi(c_2)$

To show: $c_1 = c_2$.

Proof by contradiction.

Assume $c_1 \neq c_2$.

Then $c_1 - c_2 \neq 0$ and $(c_1 - c_2)^{-1} \in F$.

$$\begin{aligned} \text{So } 1 &= \varphi(1) = \varphi((c_1 - c_2)(c_1 - c_2)^{-1}) \\ &= \varphi(c_1 - c_2) \varphi((c_1 - c_2)^{-1}) \\ &= 0 \cdot \varphi((c_1 - c_2)^{-1}) = 0. \end{aligned}$$

So $1 = 0$ in K .

So, if $k \in K$ then

$$k = k \cdot 1 = k \cdot 0 = 0.$$

So $K = \{0\}$.

At this point we see that the problem is not

stated quite right. It should say:

Let $\varphi: \mathbb{F} \rightarrow \mathbb{K}$ be a field homomorphism such that \mathbb{K} is not the zero field. Then φ is injective.

Proof

Assume \mathbb{F} and \mathbb{K} are fields, $\mathbb{K} \neq \{0\}$ and $\varphi: \mathbb{F} \rightarrow \mathbb{K}$ is a field homomorphism.

To show: $\varphi: \mathbb{F} \rightarrow \mathbb{K}$ is injective.

To show: If $a, b \in \mathbb{F}$ and $\varphi(a) = \varphi(b)$ then $a = b$.

Assume $a, b \in \mathbb{F}$ and $\varphi(a) = \varphi(b)$.

To show: $a = b$.

Proof by contradiction.

Assume $a \neq b$.

Then $a - b \neq 0$ and $(a - b)^{-1} \in \mathbb{F}$.

$$\begin{aligned} \text{So } 1 &= \varphi(1) = \varphi((a - b)(a - b)^{-1}) \\ &= \varphi(a - b) \varphi((a - b)^{-1}) \\ &= 0 \cdot \varphi((a - b)^{-1}) = 0. \end{aligned}$$

So $1 = 0$ in \mathbb{K} .

So, if $k \in \mathbb{K}$ then $k = k \cdot 1 = k \cdot 0 = 0$.

So $\mathbb{K} = \{0\}$.

Contradiction to $\mathbb{K} \neq \{0\}$.

So $a = b$. So φ is injective.

HW3 Problem 7

Let $M_n(\mathbb{C})$ be the set of $n \times n$ matrices with entries in \mathbb{C} .

The general linear group is the set

$$GL_n(\mathbb{C}) = \{ g \in M_n(\mathbb{C}) \mid g \text{ is invertible} \}$$

with operation matrix multiplication

The special linear group is the subgroup

$$SL_n(\mathbb{C}) = \{ g \in GL_n(\mathbb{C}) \mid \det(g) = 1 \}$$

of $GL_n(\mathbb{C})$.

The orthogonal group is the subgroup,

$$O_n(\mathbb{C}) = \{ g \in GL_n(\mathbb{C}) \mid gg^t = I \},$$

of $GL_n(\mathbb{C})$.

The special orthogonal group is

$$SO_n(\mathbb{C}) = O_n(\mathbb{C}) \cap SL_n(\mathbb{C})$$

If $g = (g_{ij})$ is an $n \times n$ matrix

$$\bar{g} = (\bar{g}_{ij}) \text{ where } \bar{g}_{ij} \text{ is the complex}$$

conjugate of g_{ij} (If $a+bi \in \mathbb{C}$ then $\overline{a+bi} = a-bi$).

HW3 Problem 9

The General linear group $GL_n(\mathbb{C})$ acts on the n -dimensional vector space $\mathbb{C}^n = M_{n \times 1}(\mathbb{C})$ of $n \times 1$ matrices by matrix multiplication.

The Symmetric group S_n , of $n \times n$ permutation matrices acts on the ~~set~~ n -element set

$$\left\{ \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix}, \dots, \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix} \right\}$$

by matrix multiplication.

The dihedral group D_n , generated by a and b with $a^n = 1$, $b^2 = 1$ and $ba = a^{n-1}b$, acts on a regular n -gon by having

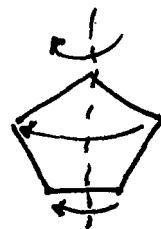
a act by rotation by $\frac{2\pi}{n}$

and b act by reflection in the axis determined by the center and a vertex.

For example D_5 acts on a pentagon by



and



Since the cyclic group

$$C_n = \{1, a, a^2, \dots, a^{n-1}\}$$

is a subgroup of D_n , it also acts on the n -gon.

HW3 Problem 19

Let R and S be rings

A ring homomorphism from R to S is a function

$\varphi: R \rightarrow S$ such that

- (a) If $r_1, r_2 \in R$ then $\varphi(r_1 + r_2) = \varphi(r_1) + \varphi(r_2)$,
- (b) $\varphi(0) = 0$,
- (c) If $r \in R$ then $\varphi(-r) = -\varphi(r)$,
- (d) If $r_1, r_2 \in R$ then $\varphi(r_1 r_2) = \varphi(r_1) \varphi(r_2)$,
- (e) $\varphi(1) = 1$.

An isomorphism between R and S is a function $\varphi: R \rightarrow S$ such that

- (a) $\varphi^{-1}: S \rightarrow R$ exists,
- (b) φ is a ring homomorphism,
- (c) φ^{-1} is a ring homomorphism.

HW3 Problem 20

(19)

Let F and K be fields

A field homomorphism from F to K is a function $\varphi: F \rightarrow K$ such that

- (a) If $r_1, r_2 \in F$ then $\varphi(r_1 + r_2) = \varphi(r_1) + \varphi(r_2)$,
- (b) $\varphi(0) = 0$,
- (c) If $r \in F$ then $\varphi(-r) = -\varphi(r)$,
- (d) If $r_1, r_2 \in F$ then $\varphi(r_1 r_2) = \varphi(r_1) \varphi(r_2)$
- (e) $\varphi(1) = 1$
- (f) If $r \in F$ and $r \neq 0$ then $\varphi(r^{-1}) = \varphi(r)^{-1}$.

An isomorphism between F and K is a function $\varphi: F \rightarrow K$ such that

- (a) $\varphi^{-1}: K \rightarrow F$ exists,
- (b) φ is a field homomorphism,
- (c) φ^{-1} is a field homomorphism.

HW3 Problem 17 Show that $\text{Card}(\mathbb{R}) = \text{Card}(\mathbb{C})$.

Proof To show: $\text{Card}(\mathbb{C}) = \text{Card}(\mathbb{R})$.

To show: There exists a bijection $\varphi: \mathbb{C} \rightarrow \mathbb{R}$

Let

$$\varphi(a+bi) = d_2 a_2 \dots d_2 a_2 b_1 a_1 b_0 a_0 a_1 b_1 a_2 b_2 \dots$$

if the decimal expansions of a and b are

$$a_1 \dots a_1 a_0 a_{-1} a_{-2} \dots \text{ and } b_1 \dots b_1 b_0 b_{-1} b_{-2} \dots$$

To show: φ is bijective

To show: $\varphi^{-1}: \mathbb{R} \rightarrow \mathbb{C}$ exists.

Let

$$\varphi^{-1}(c_{2k-1} \dots c_1 c_0 c_{-1} c_{-2} \dots) = \frac{c_{2k-1} \dots c_1 c_0 c_{-1} c_{-2} \dots}{2}$$

$$= c_{2k-2} \dots c_2 c_0 c_{-1} c_{-3} \dots + c_{2k-1} \dots c_3 c_1 c_{-2} c_{-4} \dots i$$

To show: φ^{-1} is the inverse of φ .

To show: (a) $\varphi \circ \varphi^{-1} = \text{id}_{\mathbb{R}}$

(b) $\varphi^{-1} \circ \varphi = \text{id}_{\mathbb{C}}$.

(a) To show: If $x \in \mathbb{R}$ then $(\varphi \circ \varphi^{-1})(x) = \text{id}_{\mathbb{R}}(x)$.

Assume $x \in \mathbb{R}$, $x = x_{2k-1} \dots x_1 x_0 x_{-1} x_{-2} \dots$

Then

$$(\varphi \circ \varphi^{-1})(x) = \varphi(\varphi^{-1}(x)) = \varphi\left(x_{2k-2} \dots x_2 x_0 x_{-1} x_{-3} \dots + x_{2k-1} \dots x_3 x_1 x_{-2} x_{-4} \dots i\right)$$

(21)

$$= x_{2l-1} x_{2l-2} \dots x_3 x_2 x_1 x_0 \cdot x_{-1} x_{-2} x_{-3} \dots = x = z_{\mathbb{R}}(x).$$

(b) To show: If $a+bi \in \mathbb{C}$ then $(\varphi^{-1} \circ \varphi)(a+bi) = z_{\mathbb{C}}(a+bi)$.

Assume $a+bi \in \mathbb{C}$,

$$a = a_l \dots a_1 a_0 \cdot a_{-1} a_{-2} \dots \text{ and}$$

$$b = b_l \dots b_1 b_0 \cdot b_{-1} b_{-2} \dots$$

Then

$$(\varphi^{-1} \circ \varphi)(a+bi) = \varphi^{-1}(\varphi(a+bi))$$

$$= \varphi^{-1}(b_l a_l \dots b_1 a_1 b_0 a_0 \cdot a_{-1} b_{-1} a_{-2} b_{-2} \dots)$$

$$= a_l \dots a_1 a_0 \cdot a_{-1} a_{-2} \dots + b_l b_{l-1} \dots b_1 b_0 \cdot b_{-1} b_{-2} \dots \cdot i$$

$$= a+bi = z_{\mathbb{C}}(a+bi).$$

So φ is invertible.

So $\text{Card}(\mathbb{R}) = \text{Card}(\mathbb{C})$.

HW3 Problem 14 Show that $\text{Card}(\mathbb{Z}_{70}) = \text{Card}(\mathbb{Z})$

To show: $\text{Card}(\mathbb{Z}) = \text{Card}(\mathbb{Z}_{70})$

To show: There ^{exists} a bijection $\varphi: \mathbb{Z} \rightarrow \mathbb{Z}_{70}$.

Let $\varphi: \mathbb{Z} \rightarrow \mathbb{Z}_{70}$ be given by

$$\varphi(i) = \begin{cases} 0, & \text{if } i=0, \\ 2i, & \text{if } i \in \mathbb{Z}_{70}, \\ -2i-1, & \text{if } -i \in \mathbb{Z}_{70}. \end{cases}$$

To show: φ is bijective.

To show: $\varphi^{-1}: \mathbb{Z}_{70} \rightarrow \mathbb{Z}$ exists.

Let $\varphi^{-1}: \mathbb{Z}_{70} \rightarrow \mathbb{Z}$ be given by

$$\varphi^{-1}(j) = \begin{cases} j/2, & \text{if } j \text{ is even,} \\ -\frac{j+1}{2}, & \text{if } j \text{ is odd.} \end{cases}$$

To show: (a) $\varphi \circ \varphi^{-1} = \text{id}_{\mathbb{Z}_{70}}$

(b) $\varphi^{-1} \circ \varphi = \text{id}_{\mathbb{Z}}$.

(a) To show: If $j \in \mathbb{Z}_{70}$ then $(\varphi \circ \varphi^{-1})(j) = \text{id}_{\mathbb{Z}_{70}}(j)$.

Assume $j \in \mathbb{Z}_{70}$

To show: $(\varphi \circ \varphi^{-1})(j) = \text{id}_{\mathbb{Z}_{70}}(j)$

Case 1 j is even.

$$(\varphi \circ \varphi^{-1})(j) = \varphi(j/2) = 2 \cdot j/2 = j = \text{id}_{\mathbb{Z}_{70}}(j).$$

Case 2 j is odd.

$$\begin{aligned} (\varphi \circ \varphi^{-1})(j) &= \varphi(\varphi^{-1}(j)) = \varphi\left(-\frac{j+1}{2}\right) = -2\left(-\frac{j+1}{2} - 1\right) \\ &= j - 1 + 1 = j. \end{aligned}$$

(b) To show: $\varphi^{-1} \circ \varphi = \text{id}_{\mathbb{Z}}$

To show: If $i \in \mathbb{Z}$ then $(\varphi^{-1} \circ \varphi)(i) = \text{id}_{\mathbb{Z}}(i)$

Assume $i \in \mathbb{Z}$.

To show $(\varphi^{-1} \circ \varphi)(i) = \text{id}_{\mathbb{Z}}(i)$.

Case 1: $i \in \mathbb{Z}_{>0}$.

$$(\varphi^{-1} \circ \varphi)(i) = \varphi^{-1}(\varphi(i)) = \varphi^{-1}(2i) = \frac{2i}{2} = i.$$

Case 2: $i \in \mathbb{Z}_{<0}$

$$\begin{aligned} (\varphi^{-1} \circ \varphi)(i) &= \varphi^{-1}(\varphi(i)) = \varphi^{-1}(-2i-1) \\ &= -\frac{-2i-1+1}{2} = i. \end{aligned}$$

Case 3: $i = 0$

$$(\varphi^{-1} \circ \varphi)(0) = \varphi^{-1}(\varphi(0)) = \varphi^{-1}(0) = 0/2.$$

So φ is invertible

So φ is a bijection

So $\text{Card}(\mathbb{Z}) = \text{Card}(\mathbb{Z}_{>0})$.