

ABSTRACT ALGEBRA: HOMEWORK #5

JOEL SAVITZ

1. CHAPTER 11, EXERCISE A2

Suppose $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 1 & 3 & 4 & 5 & 4 \end{pmatrix}$.

Then, f generates a subgroup of S_6 — denoted $\langle f \rangle$ — like so:

$$(1) \quad f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 1 & 3 & 2 & 5 & 4 \end{pmatrix}$$

$$(2) \quad f^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 6 & 3 & 1 & 5 & 2 \end{pmatrix}$$

$$(3) \quad f^3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 3 & 6 & 5 & 1 \end{pmatrix}$$

$$(4) \quad f^4 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix} = e \in S_6$$

2. CHAPTER 11, EXERCISE B1

Suppose we have some group G such that $\text{ord}(G) = n$.

Theorem 1. G is cyclic $\iff \exists x \in G \ni \text{ord}(x) = n$

Proof. Since G is cyclic, it must be generated by some element $a \in G$, and since $\text{ord}(G) = n$, we can rewrite G as $\{e, a, a^2, a^3, \dots, a^{n-1}\}$. Then, since $a^n \in G$ and all other powers of a are already present, we deduce that $a^n = e$, and therefore we have $\text{ord}(a) = n$ and we have the implication G is cyclic $\implies \exists x \in G \ni \text{ord}(x) = n$.

Conversely, suppose we have some $a \in G$ where $\text{ord}(a) = n$. Then, by definition we have $a^n = e$. Define the following set H : $H = \{x \in G : a^{n-i} \ni 0 \leq i < n\}$. First, note that $x \in H \implies x \in G$ by construction. We can see that $|H| = n$ since every a^{n-i} must be distinct due to the fact that $\text{ord}(a)$ is defined to be the smallest positive integer where $a^n = e$. Then, since $|H| = n$ and every element is a power of a under an operation closed on G , we must have that $x \in G \implies x \in H$ and thus by the Axiom of Extensionality we have $H = G$. Then, G is

Date: Wednesday 24 June 2020.

generated by some element $\mathbf{a} \in G$ so G is cyclic. Thus, we have the implication that $\exists \mathbf{x} \in G \ni \text{ord}(\mathbf{x}) = \mathbf{n} \implies G$ is cyclic.

Finally, since we have the implication in both directions, we must have the bidirectional implication that: G is cyclic $\iff \exists \mathbf{x} \in G \ni \text{ord}(\mathbf{x}) = \mathbf{n}$. This proves theorem 1. \square

3. CHAPTER 11, EXERCISE B3

Suppose G is some group generated by $\mathbf{a} \in G$ and suppose $\mathbf{b} \in G$.

Theorem 2. $\exists k \in \mathbb{Z} \ni k \text{ord}(\mathbf{b}) = \text{ord}(\mathbf{a})$ i.e. the order of \mathbf{b} is a factor of the order of \mathbf{a} .

Proof. Let $\mathbf{n} = \text{ord}(\mathbf{a})$ and let $\mathbf{m} = \text{ord}(\mathbf{b})$. We have $\mathbf{m} = \text{ord}(\mathbf{b}) \iff \mathbf{b}^{\mathbf{m}} = \mathbf{e}$. Since $G = \langle \mathbf{a} \rangle$, we have $G = \{\mathbf{e}, \mathbf{a}, \mathbf{a}^2, \mathbf{a}^3, \dots, \mathbf{a}^{\mathbf{n}-1}\}$. Since $\mathbf{b} \in G$, we must have that $\exists z \in \mathbb{Z} \ni 0 < z \leq \mathbf{n}$ such that $\mathbf{a}^z = \mathbf{b}$. Then if we take both sides to the power of \mathbf{m} we have $\mathbf{a}^{\mathbf{m}z} = \mathbf{b}^{\mathbf{m}} = \mathbf{e} = \mathbf{a}^{\mathbf{n}}$. Then clearly \mathbf{m} is a factor of \mathbf{n} , since $\mathbf{a}^{\mathbf{n}} = \mathbf{a}^{\mathbf{m}z}$ so we conclude that the order of \mathbf{b} is a factor of the order of \mathbf{a} . This proves theorem 2. \square

4. CHAPTER 11, EXERCISE D1

Suppose G is a group and $\mathbf{a}, \mathbf{b} \in G$.

Theorem 3. $(\exists k \in \mathbb{Z} \ni \mathbf{a} = \mathbf{b}^k) \implies \langle \mathbf{a} \rangle \subseteq \langle \mathbf{b} \rangle$

Proof. Suppose that some integer k exists where $\mathbf{a} = \mathbf{b}^k$. Then, suppose some $\mathbf{x} \in \langle \mathbf{a} \rangle$. We must have some integer \mathbf{n} where $\mathbf{a}^{\mathbf{n}} = \mathbf{x}$, so we substitute the identity defined in our initial antecedent for \mathbf{a} to get $\mathbf{b}^{\mathbf{n}k} = \mathbf{x}$, and we see that necessarily $\mathbf{x} \in \langle \mathbf{b} \rangle$ since it is some power of \mathbf{b} . Thus $\mathbf{x} \in \langle \mathbf{a} \rangle \implies \mathbf{x} \in \langle \mathbf{b} \rangle \iff \langle \mathbf{a} \rangle \subseteq \langle \mathbf{b} \rangle$. We arrive at the implication $(\exists k \in \mathbb{Z} \ni \mathbf{a} = \mathbf{b}^k) \implies \langle \mathbf{a} \rangle \subseteq \langle \mathbf{b} \rangle$ and this proves theorem 3. \square

5. CHAPTER 11, EXERCISE D2

Suppose $\mathbf{a} \in \langle \mathbf{b} \rangle$ for some $\mathbf{a}, \mathbf{b} \in G$ where there exists some integer k such that $\mathbf{a} = \mathbf{b}^k$

Theorem 4. $\exists q \in \mathbb{Z} \ni \mathbf{a}^q = \mathbf{b} \iff \langle \mathbf{a} \rangle = \langle \mathbf{b} \rangle$

Proof. Suppose we have some $q \in \mathbb{Z}$ where $\mathbf{a}^q = \mathbf{b}$. We can rewrite $\langle \mathbf{b} \rangle$ as the equivalent set $\{\mathbf{e}, \mathbf{b}, \mathbf{b}^2, \dots, \mathbf{b}^{\mathbf{n}-1}\}$. If we substitute \mathbf{a}^q for every \mathbf{b} , we have $\langle \mathbf{b} \rangle = \{\mathbf{e}, \mathbf{a}^q, \mathbf{a}^{2q}, \mathbf{a}^{3q}, \dots, \mathbf{a}^{(\mathbf{n}-1)q}\}$ and therefore \mathbf{a} generates $\langle \mathbf{b} \rangle$, or $\langle \mathbf{a} \rangle = \langle \mathbf{b} \rangle$.

Conversely, suppose $\langle a \rangle = \langle b \rangle$. Then, we can rewrite this equation as $\{e, a, a^2, a^3, \dots, a^{n-1}\} = \{e, b, b^2, b^3, \dots, b^{n-1}\}$. Since any $a^q \in \langle a \rangle = \langle b \rangle$, we must have an integer q where $a^q = b \in \langle b \rangle$.

Then, since we have the individual implication in both directions, we have the biconditional implication $\exists q \in \mathbb{Z} \ni a^q = b \iff \langle a \rangle = \langle b \rangle$. This proves theorem 4. \square

6. CHAPTER 12, EXERCISE B1

Suppose some $m, n \in \mathbb{Z}$.

Define a relation \sim as $m \sim n \iff |m| = |n|$

Theorem 5. \sim is an equivalence relation.

Proof. Suppose some $a, b, c \in \mathbb{Z}$.

Trivially $|a| = |a| \iff a \sim a$, i.e. \sim is reflexive.

Suppose $a \sim b$. Then, $|a| = |b| \iff |b| = |a|$ since equality is symmetric, so $a \sim b$ and we have $a \sim b \implies b \sim a$, i.e. \sim is symmetric.

Suppose $a \sim b \wedge b \sim c$. Then, $|a| = |b| \wedge |b| = |c| \iff |a| = |c|$ since equality is transitive, so $a \sim c$ and we have $a \sim b \wedge b \sim c \implies a \sim c$, i.e. \sim is transitive.

Then, \sim is reflexive, symmetric, and transitive, if and only if \sim is an equivalence relation. This proves theorem 5. \square

We can describe the equivalence class of some $a \in \mathbb{Z}$ by $[a] = \{a, -a\}$.

7. CHAPTER 12, EXERCISE B5

Suppose some $m, n \in \mathbb{R}$.

Define a relation \sim as $m \sim n \iff a - b \in \mathbb{Q}$.

Theorem 6. \sim is an equivalence relation.

Proof. Suppose $a, b, c \in \mathbb{R}$.

Obviously $a - a = 0 \in \mathbb{Q}$, so $a \sim a$ and \sim is reflexive.

Suppose that $a \sim b$. Then, $a - b \in \mathbb{Q} \iff b - a \in \mathbb{Q}$, so $b \sim a$. This demonstrates that $a \sim b \implies b \sim a$ so we see that \sim is symmetric.

Suppose that $a \sim b \wedge b \sim c$. Then, $a - b \in \mathbb{Q} \wedge b - c \in \mathbb{Q} \iff a - b + b - c = a - c \in \mathbb{Q}$, so $a \sim c$. This demonstrates that $a \sim b \wedge b \sim c \implies a \sim c$ so we see that \sim is transitive.

Then, \sim is reflexive, symmetric, and transitive if and only if \sim is an equivalence relation. This proves theorem 6. \square

If we let $\text{floor}(x)$ denote the $n \in \mathbb{Q} \ni n \leq x \wedge (\forall m \in \mathbb{Z})(m \geq n \implies m = n)$, we can describe the equivalence class of an $x \in \mathbb{R}$

with respect to \sim by $[x] = \{y : y = n + \text{floor}(x) \ni n \in \mathbb{Q}\}$. We see from this description of $[x]$ that $[0] = \mathbb{Q}$.

8. CHAPTER 12, EXERCISE D3

Suppose G is some group with elements $a, b \in G$.

Define a relation \sim as $a \sim b \iff \exists x \in G \ni a = xbx^{-1}$.

Theorem 7. *\sim is an equivalence relation.*

Proof. Let $a \in G$. We observe that $ea e^{-1} = a \iff a \sim a$, so we see that \sim is reflexive.

Let $a, b, x \in G \ni a \sim b$ such that $a = xbx^{-1}$. Then, we must have $b = x^{-1}ax$, by multiplication of the left side by x^{-1} and the right side by x . We see that $b = yay^{-1}$ for $y = x^{-1} \in G$, so $b \sim a$ and $a \sim b \implies b \sim a$, therefore \sim is symmetric.

Let $a, b, c, x, y \in G \ni a \sim b \wedge b \sim c$ such that $a = xbx^{-1} \wedge b = ycy^{-1}$. By substitution, we find that $a = x(ycy^{-1})x^{-1} = xyc(xy)^{-1}$, and since $xy \in G$, it is evident that $a \sim c$ and $a \sim b \wedge b \sim c \implies a \sim c$, therefore \sim is transitive.

Then, \sim is reflexive, symmetric, and transitive if and only if \sim is an equivalence relation. This proves theorem 7. \square

9. THE CYCLIC SUBGROUPS OF Z_{12}

The following are the cyclic subgroups of Z_{12} .

- (5) $\langle 0 \rangle = \{0\}$ (trivial)
- (6) $\langle 1 \rangle = Z_{12}$ (trivial)
- (7) $\langle 2 \rangle = \{0, 2, 4, 6, 8, 10\}$
- (8) $\langle 3 \rangle = \{0, 3, 6, 9\}$
- (9) $\langle 4 \rangle = \{0, 4, 8\}$
- (10) $\langle 6 \rangle = \{0, 6\}$
- (11)

Then, the following are the orders of the generator of each cyclic subgroup:

- (12) $\text{ord}(0) = 1$
- (13) $\text{ord}(1) = 12$
- (14) $\text{ord}(2) = 6$
- (15) $\text{ord}(3) = 4$
- (16) $\text{ord}(4) = 3$
- (17) $\text{ord}(6) = 2$

By inspection, we see that the orders of each generator element divide 12, where $12 = \text{ord}(Z_{12})$.

10. THE PERMUTATION KNOWN AS $x + 1$

Suppose that $f(x) = x + 1 \in S_{\mathbb{R}}$.

Semi-formally, we can describe the elements of $\langle f \rangle$ as $\{\dots, x - 2, x - 1, x, x + 1, x + 2, x + 3, x + 4, \dots\}$. In general, $\forall x \in \mathbb{Z}$ we have $f^n(x) = x + n$, the proof of which is trivial and hence omitted.

Theorem 8. $\mathbb{Z} \cong \langle f \rangle$

Proof. Define $\phi : \mathbb{Z} \rightarrow \langle f \rangle$ by $\phi(n) = f^n$. Suppose some $x, y \in \mathbb{Z}$.

Furthermore, suppose that $\phi(x) = \phi(y)$. Then since in general $f^n(x) = x + n$, we have in particular that $f^x(z) = x + z = y + z = f^y(z) \iff x = y$, so ϕ is injective.

Suppose that we have some $f^n \in \langle f \rangle$, where $n \in \mathbb{Z}$. Since $f^n(x) = x + n$, we see that $\phi(n) = f^n$, so ϕ is surjective.

At this point, we observe that ϕ is injective and ϕ is surjective if and only if ϕ is bijective.

Removing the previously imposed constraint that $\phi(x) = \phi(y)$, we see that $\phi(x + y) = f^{x+y} = f^x f^y = \phi(x) \phi(y)$, so we conclude that the bijection ϕ is an isomorphism from \mathbb{Z} to $\langle f \rangle$, therefore $\mathbb{Z} \cong \langle f \rangle$. This proves theorem 8. \square

11. THE REAL-VALUED FUNCTION KNOWN AS $x + 1$

Suppose that $f(x) = x + 1 \in \mathcal{F}(\mathbb{R})$.

We can describe the elements of $\langle f \rangle$ as $\langle f \rangle = \{n(x + 1) : n \in \mathbb{Z}\}$, the proof of which is trivial and hence omitted.

Theorem 9. $\mathbb{Z} \cong \langle f \rangle$

Note: I use multiplicative notation to denote vector addition of real-valued functions.

Proof. Define $\phi : \mathbb{Z} \rightarrow \langle f \rangle$ by $\phi(n) = f^n$. Suppose some $x, y \in \mathbb{Z}$.

Furthermore, suppose that $\phi(x) = \phi(y)$. Then since in general $f^n(x) = n(x+1)$, we have $f^x(z) = x(z+1) = y(z+1) = f^y(z) \iff x = y$, so ϕ is injective.

Suppose that we have some $f^n \in \langle f \rangle$, where $n \in \mathbb{Z}$. Since in general we have $f^n(x) = n(x+1)$, we see that $\phi(n) = f^n$, so ϕ is surjective.

At this point, we observe that ϕ is injective and ϕ is surjective if and only if ϕ is bijective.

Removing the previously imposed constraint that $\phi(x) = \phi(y)$, we see that $\phi(x+y) = f^{x+y} = f^x f^y = \phi(x)\phi(y)$, so we conclude that the bijection ϕ is an isomorphism from \mathbb{Z} to $\langle f \rangle$, therefore $\mathbb{Z} \cong \langle f \rangle$. This proves theorem 9. \square

12. A FURTHER LOOK AT $GL_2(\mathbb{R})$

Let $A \in GL_2(\mathbb{R})$ such that $A = \begin{bmatrix} a & (b-a) \\ 0 & b \end{bmatrix} \wedge b \neq 0 \neq a$

Theorem 10. *For any integer n , we have $\begin{bmatrix} a & (b-a) \\ 0 & b \end{bmatrix}^n = \begin{bmatrix} a^n & (b^n - a^n) \\ 0 & b^n \end{bmatrix}$*

Proof. First, note that $A^1 = A \iff \begin{bmatrix} a & (b-a) \\ 0 & b \end{bmatrix}^1 = \begin{bmatrix} a^1 & (b^1 - a^1) \\ 0 & b^1 \end{bmatrix}$.

If we assume that theorem 10 holds for some $n \in \mathbb{Z} \ni n > 0$, we find

$$\text{that } \left(\begin{bmatrix} a & (b-a) \\ 0 & b \end{bmatrix}^n = \begin{bmatrix} a^n & (b^n - a^n) \\ 0 & b^n \end{bmatrix} \right) \implies \left(\begin{bmatrix} a & (b-a) \\ 0 & b \end{bmatrix}^{n+1} = \begin{bmatrix} a^{n+1} & (b^{n+1} - a^{n+1}) \\ 0 & b^{n+1} \end{bmatrix} \right) \text{ since } \begin{bmatrix} a^n & (b^n - a^n) \\ 0 & b^n \end{bmatrix} \begin{bmatrix} a & (b-a) \\ 0 & b \end{bmatrix} = \begin{bmatrix} a^{n+1} & (b^{n+1} - a^{n+1}) \\ 0 & b^{n+1} \end{bmatrix},$$

so we see that theorem 10 holds when n is restricted to be greater than 0.

Then since A is a two by two matrix, we have $A^{-1} = \frac{1}{ab-(b-a)0} \begin{bmatrix} b & -(b-a) \\ -0 & a \end{bmatrix} = \begin{bmatrix} a^{-1} & (b^{-1} - a^{-1}) \\ 0 & b^{-1} \end{bmatrix}$ If we assume that

theorem 10 holds for some $n \in \mathbb{Z} \ni n < 0$, we find that $\left(\begin{bmatrix} a & (b-a) \\ 0 & b \end{bmatrix}^n = \begin{bmatrix} a^n & (b^n - a^n) \\ 0 & b^n \end{bmatrix} \right) \implies \left(\begin{bmatrix} a & (b-a) \\ 0 & b \end{bmatrix}^{n-1} = \begin{bmatrix} a^{n-1} & (b^{n-1} - a^{n-1}) \\ 0 & b^{n-1} \end{bmatrix} \right)$

since $\begin{bmatrix} a^n & (b^n - a^n) \\ 0 & b^n \end{bmatrix} \begin{bmatrix} a & (b-a) \\ 0 & b \end{bmatrix}^{-1} = \begin{bmatrix} a^{n-1} & (b^{n-1} - a^{n-1}) \\ 0 & b^{n-1} \end{bmatrix}$, so we see that theorem 10 holds when n is restricted to be greater than 0.

Thus we have covered every integer but the additive identity, $0 \in \mathbb{Z}$. We see that $A^0 = AA^{-1} = \begin{bmatrix} a^n & (b^n - a^n) \\ 0 & b^n \end{bmatrix} \begin{bmatrix} a^{-1} & (b^{-1} - a^{-1}) \\ 0 & b^{-1} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} a^0 & (b^0 - a^0) \\ 0 & b^0 \end{bmatrix}$ and conclude that 10 holds for any integer n . \square

By theorem 10 we have the following:

$$(18) \quad A^{-3} = \begin{bmatrix} a^{-3} & (b^{-3} - a^{-3}) \\ 0 & b^{-3} \end{bmatrix}$$

$$(19) \quad A^{-2} = \begin{bmatrix} a^{-2} & (b^{-2} - a^{-2}) \\ 0 & b^{-2} \end{bmatrix}$$

$$(20) \quad A^{-1} = \begin{bmatrix} a^{-1} & (b^{-1} - a^{-1}) \\ 0 & b^{-1} \end{bmatrix}$$

$$(21) \quad A^0 = \begin{bmatrix} a^0 & (b^0 - a^0) \\ 0 & b^0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I$$

$$(22) \quad A^1 = \begin{bmatrix} a & (b - a) \\ 0 & b \end{bmatrix}$$

$$(23) \quad A^2 = \begin{bmatrix} a^2 & (b^2 - a^2) \\ 0 & b^2 \end{bmatrix}$$

$$(24) \quad A^3 = \begin{bmatrix} a^3 & (b^3 - a^3) \\ 0 & b^3 \end{bmatrix}$$

13. PROOF OF AN EQUIVALENCE RELATION

Suppose $f, g, h \in \mathcal{F}(\mathbb{R})$.

Define the relation \sim as:

$$(25) \quad f \sim g \iff (\forall x \in \mathbb{R})(f(x) - g(x) = c \text{ for some } c \in \mathbb{R})$$

Theorem 11. \sim , as described in (25), is an equivalence relation

Proof. Obviously $f(x) - f(x) = 0 \in \mathbb{R}$ for all real x , so we have that $f \sim f$ i.e. \sim is reflexive.

Then, if we suppose that $f(x) - g(x) = c \in \mathbb{R}$ for all real x , we must then have that $g(x) - f(x) = -c \in \mathbb{R}$, so $f \sim g \implies g \sim f$ i.e. \sim is symmetric.

Alternatively, if we suppose that both $f(x) - g(x) = c \in \mathbb{R} \wedge g(x) - h(x) = d \in \mathbb{R}$ for all real x , we can add the two equations together to

(1) CLAIM: $\begin{bmatrix} a & (b-a) \\ 0 & b \end{bmatrix}^n = \begin{bmatrix} a^n & (b-a)^n \\ 0 & b^n \end{bmatrix}$ for any $n \in \mathbb{N}$

PROOF:

(2) $\angle 1 \leq n = 1$

(3) $\begin{bmatrix} a & (b-a) \\ 0 & b \end{bmatrix}^1 = \begin{bmatrix} a^1 & (b-a)^1 \\ 0 & b^1 \end{bmatrix}$

(4) Suppose (1) held for some $n \in \mathbb{N}$

(5) Then, (4) $\Rightarrow \left(\begin{bmatrix} a & (b-a) \\ 0 & b \end{bmatrix}^n = \begin{bmatrix} a^n & (b^n - a^n) \\ 0 & b^n \end{bmatrix} \right)$

(6) $\left(\begin{bmatrix} a & (b-a) \\ 0 & b \end{bmatrix}^{n+1} = \begin{bmatrix} a^n & (b^n - a^n) \\ 0 & b^n \end{bmatrix} \begin{bmatrix} a & (b-a) \\ 0 & b \end{bmatrix} \right)$

(7) $\begin{bmatrix} a^{n+1} & a^n(b-a) + b(b^n - a^n) \\ 0 & b^{n+1} \end{bmatrix}$

(8) $\begin{bmatrix} a^{n+1} & b^{n+1} - a^{n+1} \\ 0 & b^{n+1} \end{bmatrix}$

(9) $\left(\exists n \in \mathbb{N} \Rightarrow \left(\begin{bmatrix} a & (b-a) \\ 0 & b \end{bmatrix}^n = \begin{bmatrix} a^n & b^n - a^n \\ 0 & b^n \end{bmatrix} \right) \Rightarrow \left(\begin{bmatrix} a & (b-a) \\ 0 & b \end{bmatrix}^{n+1} = \begin{bmatrix} a^{n+1} & b^{n+1} - a^{n+1} \\ 0 & b^{n+1} \end{bmatrix} \right) \right)$

(10) $\left((3) \wedge (9) \right) \Leftrightarrow (1) \quad \blacksquare \quad \text{by induction on } n$

FIGURE 1. An early sketch for the proof of theorem 10

get $f(x) - h(x) = c + d \in \mathbb{R}$, so we must have $f \sim g \wedge g \sim h \Rightarrow f \sim h$, i.e. \sim is transitive.

Finally, \sim is reflexive, symmetric, and transitive if and only if \sim is an equivalence relation. This proves theorem 11. \square

14. PROOF OF ANOTHER EQUIVALENCE RELATION

Suppose X is a set, and define the bijection $f: X \rightarrow X$.

Define the following relation for some $\mathbf{a}, \mathbf{b} \in X$:

$$(26) \quad \mathbf{a} \sim \mathbf{b} \iff \exists \mathbf{n} \in \mathbb{Z} \ni f^{\mathbf{n}}(\mathbf{a}) = \mathbf{b}$$

Theorem 12. \sim , as described in (26), is an equivalence relation

Proof. Suppose $\mathbf{a}, \mathbf{b}, \mathbf{c} \in X$.

Obviously $\exists \mathbf{n} \in \mathbb{Z} \ni f^{\mathbf{n}}(\mathbf{a}) = \mathbf{a}$ since $f^0(\mathbf{a}) = \mathbf{a}$ so we have that $\mathbf{a} \sim \mathbf{a}$ i.e. \sim is reflexive.

Then, if we suppose that $\mathbf{a} \sim \mathbf{b}$, we have that some integer \mathbf{n} must exist such that $f^{\mathbf{n}}(\mathbf{a}) = \mathbf{b}$, but since f is bijective, we can apply f^{-1} to both sides of the last equation \mathbf{n} times to get $f^{-\mathbf{n}}(\mathbf{b}) = \mathbf{a}$ and since $-\mathbf{n} \in \mathbb{Z}$ we then have $\mathbf{b} \sim \mathbf{a}$ and so we have the implication that $\mathbf{a} \sim \mathbf{b} \implies \mathbf{b} \sim \mathbf{a}$, i.e. \sim is symmetric.

Alternatively, if we suppose that $\mathbf{a} \sim \mathbf{b} \wedge \mathbf{b} \sim \mathbf{c}$ hold, we have integers \mathbf{n} and \mathbf{m} such that $f^{\mathbf{n}}(\mathbf{a}) = \mathbf{b} \wedge f^{\mathbf{m}}(\mathbf{b}) = \mathbf{c}$, so we can construct the composition $(f^{\mathbf{n}} \circ f^{\mathbf{m}})(\mathbf{a}) = f^{\mathbf{n}+\mathbf{m}}(\mathbf{a}) = \mathbf{c}$, and since $\mathbf{n} + \mathbf{m} \in \mathbb{Z}$, we have $\mathbf{a} \sim \mathbf{c}$ and so we have the implication that $\mathbf{a} \sim \mathbf{b} \wedge \mathbf{b} \sim \mathbf{c} \implies \mathbf{a} \sim \mathbf{c}$, i.e. \sim is symmetric.

Finally, \sim is reflexive, symmetric, and transitive if and only if \sim is an equivalence relation. This proves theorem 12. \square