0.3 $\mathbb{Z}/n\mathbb{Z}$: The Integers Modulo n

Proposition 4: $(\mathbb{Z}/n\mathbb{Z})^\times = \{\overline{a} \in \mathbb{Z}/n\mathbb{Z} : (a, n) = 1\}$

Proof: Let $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$, then there exists $\overline{b} \in (\mathbb{Z}/n\mathbb{Z})^\times$ with $\overline{a}\overline{b} = \overline{ab} = \overline{1}$. Consequently, there exists $k \in \mathbb{Z}$ where $ab + kn = 1$, and thus by Bezout's lemma, we have that $(a, n) = 1$.

Now, fix $a \in \mathbb{Z}$ with $(a, n) = 1$, then there exist integers b and k where $ab + nk = 1$. Consequently, $\overline{ab} = \overline{a}\overline{b} = \overline{1}$, and thus $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$. ■

11) Let $\overline{a}, \overline{b} \in (\mathbb{Z}/n\mathbb{Z})^\times$. Since a and b are units mod n, we have that $(a, n) = (b, n) = 1$, thus by Bezout's lemma, there exist integers x_1, x_2, y_1, and y_2 where

$$ax_1 + ny_1 = bx_2 + ny_2 = 1,$$

and thus

$$(ax_1 + ny_1)(bx_2 + ny_2) = ab(x_1x_2) + n(ax_1y_2 + bx_2y_1 + ny_1y_2) = (ab)x + (n)y = 1$$

for integers x and y, thus ab is a unit mod n and $\overline{ab} \in (\mathbb{Z}/n\mathbb{Z})^\times$. ■

1.1 Basic Axioms and Examples

1a) $a * b = a - b$ is not associative, as

$$1 - (2 - 3) = 1 - (-1) = 2 \neq (1 - 2) - 3 = -1 - 3 = -4$$

■

1b) Let $a, b, c \in \mathbb{Z}$, then

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

and thus $a * b = a + b + ab$ is associative. ■

5) Fix $n > 1$. For all $\overline{x} \in \mathbb{Z}/n\mathbb{Z}$, we have that $\overline{0}\overline{x} = \overline{0x} = \overline{0}$, and thus $\overline{0}$ has no multiplicative inverse in $\mathbb{Z}/n\mathbb{Z}$. ■

6a) Is a group. *Proof of Closure*

6b) Not a group, isn't closed $\left(\frac{1}{2} + \frac{1}{6} = \frac{2}{3}\right)$.

6c) Not a group, lacks inverses and an identity.

6d) Not a group, lacks inverses.

9) Let $G = \left\{a + b\sqrt{2} : a, b \in \mathbb{Q}\right\}$, and $x_1, x_2, x_3 \in G$ where $x_1 = a_1 + b_1\sqrt{2}$, $x_2 = a_2 + b_2\sqrt{2}$, and $x_3 = a_3 + b_3\sqrt{2}$ for $a_i, b_i \in \mathbb{Q}$.

a) We have that $x_1 + x_2 = a_1 + b_1\sqrt{2} + a_2 + b_2\sqrt{2} = a_1 + a_2 + (b_1 + b_2)\sqrt{2} = a + b\sqrt{2}$ where $a, b \in \mathbb{Q}$, thus $x_1 + x_2 \in G$ and closure is satisfied.

We have that $x_1 + 0 = x_1$, thus an identity element exists.

Fix x_1 and let $y = -a_1 - b_1\sqrt{2}$, then we have that $x_1 + y = a_1 + b_1\sqrt{2} - a_1 - b_1\sqrt{2} = a_1 - a_1 + (b_1 - b_1)\sqrt{2} = 0$, thus $y = (x_1)^{-1} = -x_1$, and inverses are satisfied.

Finally, we can see that

$$\begin{aligned} x_1 + (x_2 + x_3) &= a_1 + b_1\sqrt{2} + \left(a_2 + b_2\sqrt{2} + a_3 + b_3\sqrt{2}\right) \\ &= \left(a_1 + b_1\sqrt{2} + a_2 + b_2\sqrt{2}\right) + a_3 + b_3\sqrt{2} \\ &= (x_1 + x_2) + x_3, \end{aligned}$$

and thus associativity is satisfied, which proves that G is a group under addition. ■

b) Let $G^* = G \setminus \{0\}$, and suppose $x_1, x_2, x_3 \in G^*$.

We have that

$$\begin{aligned} x_1x_2 &= (a_1 + b_1\sqrt{2})(a_2 + b_2\sqrt{2}) \\ &= a_1a_2 + 2b_1b_2 + (a_1b_2 + a_2b_1)\sqrt{2} \\ &= a + b\sqrt{2}, \end{aligned}$$

thus $x_1x_2 \in G^*$ and closure is satisfied.

We have that $1 \times x_1 = x_1$, thus an identity exists.

Fix x_1 and let $y = \frac{1}{a_1^2 - 2b_1^2}(a_1 - b_1\sqrt{2})$. We know that $a_1^2 - 2b_1^2 \neq 0$ since if it did we would have that $\sqrt{2} \in \mathbb{Q}$. Consequently,

$$\begin{aligned} x_1y &= \frac{(a_1 + b_1\sqrt{2})(a_1 - b_1\sqrt{2})}{a_1^2 - 2b_1^2} \\ &= \frac{a_1^2 - 2b_1^2}{a_1^2 - 2b_1^2} = 1, \end{aligned}$$

thus $y = (x_1)^{-1} = 1/x_1$, and thus inverses are satisfied.

Finally, we have that

$$\begin{aligned} x_1(x_2x_3) &= (a_1 + b_1\sqrt{2})\left((a_2 + b_2\sqrt{2})(a_3 + b_3\sqrt{2})\right) \\ &= \left((a_1 + b_1\sqrt{2})(a_2 + b_2\sqrt{2})\right)(a_3 + b_3\sqrt{2}) = (x_1x_2)x_3, \end{aligned}$$

thus associativity is satisfied, and thus G^* is a group under multiplication. ■

11) In $(\mathbb{Z}/12\mathbb{Z}, +)$, we have

$\left|\overline{1}\right| = \left|\overline{5}\right| = \left|\overline{7}\right| = \left|\overline{11}\right| = 12$

$\left|\overline{2}\right| = \left|\overline{10}\right| = 6$

$\left|\overline{3}\right| = \left|\overline{9}\right| = 4$

$\left|\overline{4}\right| = \left|\overline{8}\right| = 3$

$\left|\overline{6}\right| = 2$

$\left|\overline{0}\right| = 1$

12) In $((\mathbb{Z}/12\mathbb{Z})^\times, \times)$, we have

$\left|\overline{1}\right| = 1$

$\left|\overline{-1}\right| = \left|\overline{5}\right| = \left|\overline{7}\right| = \left|\overline{-7}\right| = \left|\overline{13}\right| = 2$

17) Fix $x \in G$ with $|x| = n$, then we have that $x(x^{n-1}) = x^{n-1+1} = x^n = e$, and thus $x^{-1} = x^{n-1}$. ■

20) Let $x \in G$ with $|x| = n$, then $x^n = e$, and so $(x^n)^{-1} = x^{-n} = (x^{-1})^n = e^{-1} = e$. Let $|x^{-1}| = k$ and, to establish a contradiction, suppose $k < n$. Then we would have that $(x^{-1})^k = e$, and thus $\left((x^{-1})^k\right)^{-1} = \left(x^{-k}\right)^{-1} = x^k = e^{-1} = e$, but this implies $|x| \leq k < n$, which is a contradiction, thus we must have that $|x^{-1}| = n$. ■

23) Fix $x \in G$ with finite order $|x| = n$ and suppose that $n = st$ for positive integers s and t, then we have that $x^n = x^{st} = (x^s)^t = e$. To establish a contradiction, suppose that $|x^s| = k < t$, then we have that $(x^s)^k = x^{sk} = e$ with $sk < st = n$, which is a contradiction. Thus, $|x^s| = t$. ■

25) Let $a, b \in G$. We have that $(aa)(bb) = e$, as well as $(ab)(ab) = e$, and thus $aabb = abab$. Multiplying by a on the left and b on the right, we maintain equality and obtain $ab = ba$. ■

29) Let $(A, *_A)$ and $(B, *_B)$ be groups.

First, assume that A and B are abelian. Let $(a_1, b_1), (a_2, b_2) \in A \times B$, then we have that

$$(a_1, b_1) * (a_2, b_2) = (a_1 *_A a_2, b_1 *_B b_2) = (a_2 *_A a_1, b_2 *_B b_1) = (a_2, b_2) * (a_1, b_1),$$

and thus $A \times B$ is abelian.

Now, assume that $A \times B$ is abelian and let $(a_1, b_1), (a_2, b_2) \in A \times B$, then we have that

$$(a_1, b_1) * (a_2, b_2) = (a_2, b_2) * (a_1, b_1),$$

and thus

$$(a_1 *_A a_2, b_1 *_B b_2) = (a_2 *_A a_1, b_2 *_B b_1),$$

which implies that $a_1 *_A a_2 = a_2 *_A a_1$ and $b_1 *_B b_2 = b_2 *_B b_1$, thus A and B are abelian. ■

31) For a group G with even order, fix $x \in G$ such that $|x| = n$ is maximal. Such an x exists because $|x| \leq |G|$ and $|G|$ is finite. If n is odd, then G has an odd number of distinct elements, and thus cannot have even order, thus n must be even. From this, we have that $x^n = (x^{n/2})^2 = e$. Clearly $x^{n/2} \neq e$, and thus $\left|x^{n/2}\right| = 2$, thus an element of order 2 exists in G. ■

32) Let $x \in G$ with $|x| = n$. To establish a contradiction, suppose there exist integers a and b such that $0 \leq a < b < n$ and $x^a = x^b$. Then we have that $x^a x^{-a} = e = x^b x^{-a} = x^{b-a}$, which implies that $|x| \leq b - a < n$, which is a contradiction. Thus we must have that $x^a \neq x^b$ when $0 \leq a < b < n$, thus the elements $e, x, x^2, \ldots, x^{n-1}$ are distinct. ■

Let G be a group with $|G| = n$. To establish a contradiction, suppose there exists an element $x \in G$ where $|x| = k > n$. This implies that the elements $e, x, x^2, \ldots, x^{k-1}$ are distinct, but then G would have k distinct elements, and thus $|G| = k > n$, which is a contradiction. Thus, for all $x \in G$, we must have that $|x| \leq |G|$. ■

1.2 Dihedral Groups

1b) In D_8 we have that

$|e| = 1$

$|r^2| = |s| = |sr| = |sr^2| = |sr^3| = 2$

$|r| = |r^3| = 4$

2) Let $x \in D_{2n}$ and suppose x is not a power of r, then $x = sr^i$ for some integer i. Since $rs = sr^{-1}$ by the given presentation of D_{2n}, we have that $rx = rsr^i = sr^{-1}r^i = sr^{i-1} = sr^i r^{-1} = xr^{-1}$. ■

3) Let $x \in D_{2n}$ where $x = sr^i$ for some integer i. By induction we will show that $x^2 = e$ for all i. For the base case $i = 0$, we have that $x^2 = (sr^0)(sr^0) = s^2 = e$. Now, assume the induction hypothesis holds for $n = i-1$. Since $x^2 = (sr^i)(sr^i) = sr^{i-1}(rr^{-1})sr^{i-1} = (sr^{i-1})(sr^{i-1}) = e$, the hypothesis holds for $n = i$. Since $x \neq e$, we have that $|x| = 2$. ■

11) We can define an equivalence relation on the rigid rotational symmetries G of an octahedron where two rotations are equivalent if their uppermost vertices are the same. Since an octahedron has six vertices, we can see that there are six equivalence classes. Now, fix the uppermost vertex, and consider the rotations in the corresponding equivalence class. The only rotations that can be in this equivalence class are rotations about the vertical axis and whose angle is a multiple of 90°, which restricts us to four rotations. Thus, we have six equivalence classes with each class having four elements. Since each possible rotation of an octahedron is contained in one of the equivalence classes, we have that $|G| = 6 \times 4 = 24$. ■

15) $\mathbb{Z}/n\mathbb{Z} = \langle \overline{1} : \underbrace{\overline{1} + \overline{1} + \cdots + \overline{1}}_{n \text{ times}} = \overline{0} \rangle$.

Extra Proofs

The set $G = \left\{ \frac{a}{m} \in \mathbb{Q} : a, m \in \mathbb{Z}, (a, m) = 1, \text{ and } m \text{ is odd} \right\}$ is closed under addition.

Proof: Let $x, y \in G$ with $x = \frac{a_2}{m_2}$ and $y = \frac{a_2}{m_2}$, then we have

$$x + y = \frac{a_1}{m_1} + \frac{a_2}{m_2} = \frac{a_1 m_2 + a_2 m_1}{m_1 m_2}.$$

We can see that $m_1 m_2$ is odd. Now let $d = (a_1 m_2 + a_2 m_1, m_1 m_2)$. If $d = 1$ we are finished, else d must be odd since $2 \nmid m_1 m_2$. Consequently, $m_1 m_2 / d$ is odd. In addition, we have that $((a_1 m_2 + a_2 m_1)/d, m_1 m_2/d) = 1$, thus

$$x + y = \frac{a_1 m_2 + a_2 m_1}{m_1 m_2} = \frac{\frac{a_1 m_2 + a_2 m_1}{d}}{\frac{m_1 m_2}{d}} = \frac{a}{m}$$

for integers a and m where $(a, m) = 1$ and m is odd, thus $x + y \in G$. ■