Proposition 6.10. *Addition $\oplus$ and multiplication $\odot$ on $\mathbb{Z}_n$ are commutative, associative, and distributive. $\mathbb{Z}_n$ has an additive identity and a multiplicative identity.*

Proof. Commutativity of $\oplus$ follows with Axiom 2.1(i):

$$[a] \oplus [b] \overset{\text{definition}}{=} [a+b] \overset{\text{Axiom 2.1(i)}}{=} [b+a] \overset{\text{definition}}{=} [b] \oplus [a] \ ,$$

commutativity of $\odot$ with Axiom 2.1(iv):

$$[a] \odot [b] = [ab] = [ba] = [b] \odot [a] \ ,$$

associativity of $\oplus$ with Axiom 2.1(ii):

$$([a] \oplus [b]) \oplus [c] = [a+b] \oplus [c] = [(a+b)+c] = [a+(b+c)] = [a] \oplus [b+c] = [a] \oplus ([b] \oplus [c]) \, ,$$

associativity of $\odot$ with Axiom 2.1(v):

$$([a] \odot [b]) \odot [c] = [ab] \odot [c] = [(ab)c] = [a(bc)] = [a] \odot [bc] = [a] \odot ([b] \odot [c]) \, ,$$

and distributivity with Axiom Axiom 2.1(iii):

$$[a] \odot ([b] \oplus [c]) = [a] \odot [b+c] = [a(b+c)] = [ab+ac] = [ab] \oplus [ac] = ([a] \odot [b]) \oplus ([a] \odot [c]) \, .$$

Finally, $[0] \in \mathbb{Z}_n$ is the additive inverse, as for any $[a] \in \mathbb{Z}$ by Axiom 2.2

$$[0] \oplus [a] = [0+a] = [a] = [a+0] = [a] \oplus [0] \ ,$$

and $[1] \in \mathbb{Z}_n$ is the multiplicative inverse, as for any $[a] \in \mathbb{Z}$ by Axiom 2.3

$$[1] \odot [a] = [1 \cdot a] = [a] = [a \cdot 1] = [a] \odot [1] \ . \qquad \square$$