Chapter 2 part 3

$\mathbb{Z}_n$ - the set of equivalence classes with respect to the congruence relation $\equiv$
$n>0,\ n\in\mathbb{Z}$ congruence classes

Operations $\oplus, \odot$ on $\mathbb{Z}_n$ induced from addition and multiplication on $\mathbb{Z}$

Th2.7 The operations $\oplus, \odot$ have all expected properties.

Example $[a]\odot([b]\oplus[c]) = [a]\odot[b] \oplus [a]\odot[c]$

Notations Usually one skips brackets and circles

Example: they write $a\in\mathbb{Z}_n$ meaning $[a]\in\mathbb{Z}_n$

$3\cdot 9 = 3$ in $\mathbb{Z}_6$ meaning $[3]\odot[9]=[3]$ in $\mathbb{Z}_6$

One cannot make cancellations

$[27]=[3]$

$9\neq 1$ in $\mathbb{Z}_6$

$27\equiv 3 \pmod 6$

Moreover, it is convenient to use powers:

for $k>0,\ k\in\mathbb{Z}$, not an element of $\mathbb{Z}_n$

$a^k = [a]^k = \underbrace{a\cdot a\ldots a}_{k \text{ times}} = \underbrace{[a]\odot[a]\odot\ldots\odot[a]}_{k\text{ times}}$ in $\mathbb{Z}_n$

A subtlety

For positive integers a, b, what is $a^b\in\mathbb{Z}_n$?

1^{st} interpretation

$$ab = [a] \odot [b] \in \mathbb{Z}_n$$

2^{nd} interpretation

$$ab = \underbrace{[b] \oplus [b] \oplus \dots \oplus [b]}_{a \text{ times}} \in \mathbb{Z}_n$$

Fortunately, there is no ambiguity:

$$\underbrace{[b] \oplus \dots \oplus [b]}_{a \text{ times}} = [\underbrace{b + \dots + b}_{a \text{ times}}] = [ab] = [a] \odot [b]$$