L2: Integers modulo n and the Quaternion group

Integers modulo n : $\mathbb{Z}/n\mathbb{Z}$

Def Let $a, b \in \mathbb{Z}$. We say a, b have the same residue mod n and write $a \equiv b \pmod{n}$ if $\exists k \in \mathbb{Z}$ s.t.

$$a - b = k \cdot n$$

Given $a \in \mathbb{Z}$ denote by $\bar{a} = \{ b \in \mathbb{Z} \mid b \equiv a \pmod{n} \}$
$= \{ a + kn \in \mathbb{Z} \mid k \in \mathbb{Z} \} \subseteq \mathbb{Z}$

and define $\mathbb{Z}/n\mathbb{Z} = \{ \bar{a} \subseteq \mathbb{Z} \mid a \in \mathbb{Z} \}$

Lemma: i) $a \equiv b \pmod{n} \iff \bar{a} = \bar{b}$

ii) $\mathbb{Z}/n\mathbb{Z} = \{ \bar{0}, \bar{1}, \bar{2}, \dots, \overline{n-1} \}$

Pf Exc. (division with remainder)

Prop The assignment $m(\bar{a}, \bar{b}) = \overline{a+b}$ is well-defined, and $(\mathbb{Z}/n\mathbb{Z}, m)$ is an abelian group.

Pf Exercise: · well-def $a_1 \equiv a_2 \pmod{n}$ $b_1 \equiv b_2 \pmod{n}$ $\Rightarrow a_1 + a_2 \equiv b_1 + b_2 \pmod{n}$

· assoc

· unit : $e = \bar{0}$

inverse : $a^{-1} = \overline{-a}$

· abelian: ✓

Notation: we write $a = \bar{a}$

E.g. in $\mathbb{Z}/5\mathbb{Z}$ we have $2 + 3 = 0$

Lemma $1 \in \mathbb{Z}/n\mathbb{Z}$ has order n.

Pf · $n \cdot 1 = n = 0$

· $k \cdot 1 = k \underset{\text{in } \mathbb{Z}/n\mathbb{Z}}{\neq} 0$ for $0 < k < n$.

Quaternion group

Quaternion group

Let $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$
with $m: Q_8 \times Q_8 \to Q_8$ given by

- $i^2 = j^2 = k^2 = 1$
- $ij = k$, $jk = i$, $ki = j$
- $ji = -k$, $kj = -i$, $ik = -j$

and signs as expected e.g.
- $(-j)(-k) = jk = -k$
- $(-i)j = -k$

Prop (Q_8, m) is a group.
Pf Exc.