

Part 1.

(i) we show that $[R', \oplus]$ is an abelian group.

(a) closure: it holds from defn of \oplus ,

$$a \oplus b = a + b + 1, \quad \forall a, b \in R' \quad (A1)$$

(b) Associativity: Let $a, b, c \in R'$.

$$(a \oplus b) \oplus c = (a + b + 1) \oplus c = (a + b + 1) + c + 1$$

$$a \oplus (b \oplus c) = a \oplus (b + c + 1) = a + b + c + 2$$
$$= a + (b + c + 1) + 1 \quad (A2)$$
$$= a + b + c + 2$$

$$\therefore (a \oplus b) \oplus c = a \oplus (b \oplus c), \quad \forall a, b, c \in R'$$

(c) Existence of Identity:

Let $e \in R'$ be the additive identity in R' w.r. to. \oplus .

$$\text{Then, } e \oplus a = a \oplus e = a, \quad \forall a \in R' \quad (A3)$$

$$\therefore e \oplus a = a$$

$$\Rightarrow e + a + 1 = a \Rightarrow e + 1 = 0 \Rightarrow e = -1$$

$\therefore e = -1 \in R'$ is the additive identity.

(d) Existence of Inverse:

Let $i \in R'$ be the additive inverse of $a \in R'$ w.r. to. \oplus .

$$\text{Then, } i \oplus a = a \oplus i = e = -1$$

$$\therefore i \oplus a = -1 \Rightarrow i + a + 1 = -1$$

$$\Rightarrow i = -a - 2 = -(a + 2)$$

is the additive inverse of $a \in R'$. (A4)

(e) Commutativity:

$$\text{Let } a, b \in R' \quad (A5)$$

$$\text{Then, } a \oplus b = a + b + 1 = b + a + 1 = b \oplus a$$

$\therefore [R', \oplus]$ is an abelian group.

(ii) we show that $\langle R', \oplus \rangle$ is a group.

(a) [M1] closure: holds from defⁿ of \oplus
where $a \oplus b = axb + a + b, \forall a, b \in R'$.

(b) [M2] Associativity: Let $a, b, c \in R'$

$$\begin{aligned}\text{Then, } (a \oplus b) \oplus c &= (ab + a + b) \oplus c \\ &= (ab + b + c)c + (ab + a + b) \\ &\quad + c \\ &= abc + ac + bc + ab + a + bc\end{aligned}$$

$$\begin{aligned}a \oplus (b \oplus c) &= a \oplus (bc + b + c) \\ &= a(bc + b + c) + a + (bc + b + c) \\ &= abc + ab + ac + bc + a + b + c\end{aligned}$$

$$\therefore (a \oplus b) \oplus c = a \oplus (b \oplus c).$$

(iii) [M3] \oplus distributes over \odot

$$\begin{aligned}\text{ie, } a \oplus (b \odot c) &= (a \oplus b) \odot (a \oplus c) \\ (b \odot c) \oplus a &= (b \oplus a) \odot (c \oplus a)\end{aligned}$$

$\therefore \langle R', \odot, \oplus \rangle$ forms a ring.

PART 2: If $\langle R', \odot, \oplus \rangle$ is a ring with
identity, then there exists an identity e
in $\langle R', \oplus \rangle$ such that

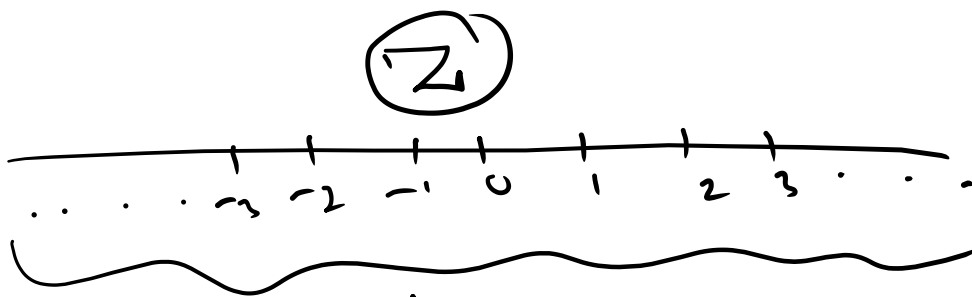
$$e \oplus x = x \oplus e = x, \forall x \in R'$$

$$\text{Now, } e \oplus x = x$$

$$\Rightarrow ex + e + x = x \Rightarrow e(x+1) = 0$$

$$\Rightarrow e = 0, \text{ since } x+1 \neq 0.$$

$e = 0$ is the identity in (R', \oplus) .



$$\boxed{\mathbb{Z}_n} = \{0, 1, 2, \dots, n-1\}$$

$$\boxed{0, 1, 2, 3, \dots, n-1}$$

Galois $\boxed{\mathbb{Z}_n}$

Given a_1, a_2, \dots, a_n :

$$\gcd(a_1, a_2, a_3, \dots, a_n)$$

$$= \gcd(\gcd(a_1, a_2, \dots, a_{n-1}), a_n)$$

$$= \vdots$$

$$= \gcd[\gcd(a_1, \gcd(a_2, a_3) \dots a_{n-1}), a_n]$$

