Rings and Principal Roots of Unity

a prelude in algebra

rings

Here

$$\mathbb{N} = \{1, 2, \ldots\}$$

Ring $R = (S, +, *, 0, 1)$

- S: set
- $+, * : S \times S \to S$ operations
- $+$ associative and commutative, $*$ associative

  $$(a+b)+c = (a+(b+c)) \quad , \quad a+b = b+a \quad , \quad (a*b)*c = a*(b*c)$$

- distributivity laws from both sides

  $$a*(b+c) = a*b+a*c \quad , \quad (b+c)*a = b*a+c*a$$

- 0 and 1 are neutral elements of $+$ and $*$

  $$r+0 = 0+r = r \quad , \quad r*1 = 1*r = r$$

- elements $r \in S$ have inverse elements $(-r)$ with respec t to $+$

  $$r+(-r) = 0$$

  define

  $$a-b = a+(-b)$$

rings

Here

$$\mathbb{N} = \{1, 2, \ldots\}$$

Ring $R = (S, +, *, 0, 1)$

- S: set
- $+, * : S \times S \to S$ operations
- $+$ associative and commutative, $*$ associative

$$(a+b)+c = (a+(b+c)) \quad , \quad a+b = b+a \quad , \quad (a*b)*c = a*(b*c)$$

- distributivity laws from both sides

$$a*(b+c) = a*b+a*c \quad , \quad (b+c)*a = b*a+c*a$$

- 0 and 1 are neutral elements of $+$ and $*$

$$r+0 = 0+r = r \quad , \quad r*1 = 1*r = r$$

- elements $r \in S$ have inverse elements $(-r)$ with respect t to $+$

$$r+(-r) = 0$$

define

$$a-b = a+(-b)$$

Ring M is *commutative* if $*$ is commutative

$$a*b = b*a$$

Examples of commutative rings

- integers

$$(\mathbb{Z}, +, -, 0, 1)$$

- integers mod m

$$\mathbb{Z}_m = ([0:m-1], + \mod m, \cdot \mod m,\ 0,\ 1)$$

rings

Here

$$\mathbb{N} = \{1, 2, \ldots\}$$

Ring $R = (S, +, *, 0, 1)$

- S: set
- $+, * : S \times S \to S$ operations
- $+$ associative and commutative, $*$ associative

$$(a+b)+c = (a+(b+c)) \quad , \quad a+b = b+a \quad , \quad (a*b)*c = a*(b*c)$$

- distributivity laws from both sides

$$a*(b+c) = a*b + a*c \quad , \quad (b+c)*a = b*a + c*a$$

- 0 and 1 are neutral elements of $+$ and $*$

$$r+0 = 0+r = r \quad , \quad r*1 = 1*r = r$$

- elements $r \in S$ have inverse elements $(-r)$ with respec t to $+$

$$r + (-r) = 0$$

define

$$a - b = a + (-b)$$

Ring M is *commutative* if $*$ is commutative

$$a*b = b*a$$

Examples of commutative rings

- integers

$$(\mathbb{Z}, +, -, 0, 1)$$

- integers mod m

$$\mathbb{Z}_m = ([0 : m-1], + \mod m, \cdot \mod m,\ 0,\ 1)$$

principal root of unity

$\omega \in S$ is an n'th *root of unity* if

$$\omega^n = 1$$

It is a *principal* n'th root of unity if

$$\omega \neq 1 \ \wedge \ \forall p \in [0 : n-1] : \sum_{j=0}^{n-1} \omega^{jp} = 0$$

principal root of unity

$\omega \in S$ is an n'th *root of unity* if

$$\omega^n = 1$$

It is a *principal* n'th root of unity if

$$\omega \neq 1 \ \wedge \ \forall p \in [0 : n-1] : \sum_{j=0}^{n-1} \omega^{jp} = 0$$

Lemma 1. *Let*

$$n = 2^k \quad , \quad k \in \mathbb{N}$$

Then for all $\omega \in \mathbb{Z} \quad , \quad \omega \neq 0$*:*

$$\sum_{i=0}^{n-1} \omega^{ip} = \prod_{i=0}^{k-1} (1 + \omega^{2^i p}) \quad \textit{for} \quad 1 \leq p < n$$

principal root of unity

$\omega \in S$ is an n'th *root of unity* if

$$\omega^n = 1$$

It is a *principal* n'th root of unity if

$$\omega \neq 1 \;\wedge\; \forall p \in [0 : n-1] : \sum_{j=0}^{n-1} \omega^{jp} = 0$$

Lemma 1. *Let*

$$n = 2^k \quad , \quad k \in \mathbb{N}$$

Then for all $\omega \in \mathbb{Z} \quad , \quad \omega \neq 0$*:*

$$\sum_{i=0}^{n-1} \omega^{ip} = \prod_{i=0}^{k-1} (1 + \omega^{2^i p}) \quad \textit{for} \quad 1 \leq p < n$$

Proof. **Computing still in** $\mathbb{Z}$. Induction on k.

- $k = 1$:

$$\sum_{i=0}^{2^1-1} \omega^{ip} = 1 + \omega^p = \prod_{i=0}^{0} (1 + \omega^{2^i p})$$

principal root of unity

$\omega \in S$ is an n'th *root of unity* if

$$\omega^n = 1$$

It is a *principal* n'th root of unity if

$$\omega \neq 1 \wedge \forall p \in [0 : n-1] : \sum_{j=0}^{n-1} \omega^{jp} = 0$$

Lemma 1. *Let*

$$n = 2^k \quad , \quad k \in \mathbb{N}$$

Then for all $\omega \in \mathbb{Z} \quad , \quad \omega \neq 0$*:*

$$\sum_{i=0}^{n-1} \omega^{ip} = \prod_{i=0}^{k-1} (1 + \omega^{2^i p}) \quad \textit{for} \quad 1 \leq p < n$$

Proof. **Computing still in** $\mathbb{Z}$. Induction on k.

- $k = 1$:

$$\sum_{i=0}^{2^1-1} \omega^{ip} = 1 + \omega^p = \prod_{i=0}^{0} (1 + \omega^{2^i p})$$

- $k > 1$:

$$\begin{aligned}
\sum_{i=0}^{n-1} \omega^{ip} &= (1+\omega^p) \sum_{i=0}^{n/2-1} (\omega^2)^{ip} \\
&= (1+\omega^p) \prod_{i=0}^{k-2} (1 + (\omega^2)^{2^i p}) \quad (\text{IH and } \omega^2 \neq 0) \\
&= (1+\omega^p) \prod_{i=1}^{k-1} (1 + \omega^{2^i p}) \quad (\text{IH and } \omega^2 \neq 0) \\
&= \prod_{i=0}^{k-1} (1 + \omega^{2^i p})
\end{aligned}$$

principal root of unity

$\omega \in S$ is an n'th *root of unity* if

$$\omega^n = 1$$

It is a *principal* n'th root of unity if

$$\omega \neq 1 \ \wedge \ \forall p \in [0 : n-1] : \sum_{j=0}^{n-1} \omega^{jp} = 0$$

Lemma 1. *Let*

$$n = 2^k \quad , \quad k \in \mathbb{N}$$

Then for all $\omega \in \mathbb{Z} \quad , \quad \omega \neq 0$*:*

$$\sum_{i=0}^{n-1} \omega^{ip} = \prod_{i=0}^{k-1} (1 + \omega^{2^i p}) \quad \textit{for} \quad 1 \leq p < n$$

Lemma 2. *Let*

$$n = 2^k \ , \ k \in \mathbb{N} \quad , \quad 0 \neq \omega \in \mathbb{Z} \quad , \quad m = \omega^{n/2} + 1$$

Then

$$\sum_{i=0}^{n-1} \omega^{ip} \equiv 0 \mod m \quad \textit{for} \quad 1 \leq p < n$$

principal root of unity

$\omega \in S$ is an n'th *root of unity* if

$$\omega^n = 1$$

It is a *principal* n'th root of unity if

$$\omega \neq 1 \wedge \forall p \in [0 : n-1] : \sum_{j=0}^{n-1} \omega^{jp} = 0$$

Lemma 1. *Let*

$$n = 2^k \quad , \quad k \in \mathbb{N}$$

Then for all $\omega \in \mathbb{Z} \quad , \quad \omega \neq 0$*:*

$$\sum_{i=0}^{n-1} \omega^{ip} = \prod_{i=0}^{k-1} (1 + \omega^{2^i p}) \quad \textit{for} \quad 1 \leq p < n$$

Lemma 2. *Let*

$$n = 2^k \, , \, k \in \mathbb{N} \quad , \quad 0 \neq \omega \in \mathbb{Z} \quad , \quad m = \omega^{n/2} + 1$$

Then

$$\sum_{i=0}^{n-1} \omega^{ip} \equiv 0 \mod m \quad \textit{for} \quad 1 \leq p < n$$

Proof. Lemma 1 $\rightarrow$ show:

$$\exists j \in [0 : k-1]. \; 1 + \omega^{2^j p} \equiv 0 \mod m$$

Decompose

$$p = 2^s p' \; , \; p' \text{ odd} \quad , \; 0 \leq s < k$$

Choose

$$j = k - 1 - s$$

Then

$$\begin{aligned} 1 + \omega^{2^j p} &= 1 + \omega^{2^{k-1-s} 2^s p'} \\ &= 1 + \omega^{2^{k-1} p'} \\ &= 1 + \omega^{n/2} p' \\ &\equiv 1 + (-1)^{p'} \mod m \quad (\text{def. of } m) \\ &= 1 - 1 \quad (p' \quad \text{odd}) \end{aligned}$$

principal root of unity

$\omega \in S$ is an n'th *root of unity* if

$$\omega^n = 1$$

It is a *principal* n'th root of unity if

$$\omega \neq 1 \wedge \forall p \in [0:n-1] : \sum_{j=0}^{n-1} \omega^{jp} = 0$$

Lemma 1. *Let*

$$n = 2^k \quad , \quad k \in \mathbb{N}$$

Then for all $\omega \in \mathbb{Z} \quad , \quad \omega \neq 0$*:*

$$\sum_{i=0}^{n-1} \omega^{ip} = \prod_{i=0}^{k-1} (1 + \omega^{2^i p}) \quad \textit{for} \quad 1 \leq p < n$$

Lemma 2. *Let*

$$n = 2^k \,,\, k \in \mathbb{N} \quad , \quad 0 \neq \omega \in \mathbb{Z} \quad , \quad m = \omega^{n/2} + 1$$

Then

$$\sum_{i=0}^{n-1} \omega^{ip} \equiv 0 \mod m \quad \textit{for} \quad 1 \leq p < n$$

From now on:

$$\boxed{n = 2^k \quad , \quad \omega = 2^e \quad , \quad m = \omega^{n/2} + 1 \quad , \quad k, e \in \mathbb{N}}$$

Lemma 3. *In* $\mathbb{Z}_m$ *holds*

- ω *and* n *have multiplicative inverses, which are powers of* 2.
- ω *is* n*'th principal root of unity.*

principal root of unity

$\omega \in S$ is an n'th *root of unity* if

$$\omega^n = 1$$

It is a *principal* n'th root of unity if

$$\omega \neq 1 \wedge \forall p \in [0 : n-1] : \sum_{j=0}^{n-1} \omega^{jp} = 0$$

Lemma 1. *Let*

$$n = 2^k \quad , \quad k \in \mathbb{N}$$

Then for all $\omega \in \mathbb{Z} \quad , \quad \omega \neq 0$*:*

$$\sum_{i=0}^{n-1} \omega^{ip} = \prod_{i=0}^{k-1} (1 + \omega^{2^i p}) \quad \textit{for} \quad 1 \leq p < n$$

Lemma 2. *Let*

$$n = 2^k \, , \, k \in \mathbb{N} \quad , \quad 0 \neq \omega \in \mathbb{Z} \quad , \quad m = \omega^{n/2} + 1$$

Then

$$\sum_{i=0}^{n-1} \omega^{ip} \equiv 0 \mod m \quad \textit{for} \quad 1 \leq p < n$$

From now on:

$$\boxed{n = 2^k \quad , \quad \omega = 2^e \quad , \quad m = \omega^{n/2} + 1 \quad , \quad k, e \in \mathbb{N}}$$

Lemma 3. *In* $\mathbb{Z}_m$ *holds*

- *ω and n have multiplicative inverses, which are powers of* 2.
- *ω is n'th principal root of unity.*

Proof.

$$\begin{aligned} \omega \cdot \omega^{n-1} &= \omega^{n/2} \cdot \omega^{n/2} \\ &\equiv (-1)^2 \mod m \\ n \cdot 2^{kne-k} &= 2^{kne} \\ &= \omega^{kn} \\ &= (\omega^n)^k \\ &\equiv 1 \mod m \end{aligned}$$

$$\omega^{n/2} \equiv -1 \mod m \quad \rightarrow \quad \omega \not\equiv 1 \mod m$$

Now apply lemma 2.