

Review of additive cosets

Discuss in your group:

Consider the **additive group** \mathbb{Z} and its subgroup $5\mathbb{Z}$.

(a) Find all distinct cosets of $5\mathbb{Z}$.

Note: They have the form $a + 5\mathbb{Z}$ where $a \in \mathbb{Z}$.

(b) Find the smallest positive integer b such that $378 + 5\mathbb{Z} = b + 5\mathbb{Z}$.

(c) Find the coset sum $(3 + 5\mathbb{Z}) + (4 + 5\mathbb{Z})$.

Recall: We formed the **quotient group**

$$\mathbb{Z}/5\mathbb{Z} = \{0 + 5\mathbb{Z}, 1 + 5\mathbb{Z}, 2 + 5\mathbb{Z}, 3 + 5\mathbb{Z}, 4 + 5\mathbb{Z}\}$$

under the operation of coset addition.

- $a + 5\mathbb{Z} = b + 5\mathbb{Z} \iff a - b \in 5\mathbb{Z}$ (and $b - a \in 5\mathbb{Z}$)

$$378 + 5\mathbb{Z} = 3 + 5\mathbb{Z}, \text{ since } 378 - 3 = 375 \in 5\mathbb{Z}.$$

- $(a + 5\mathbb{Z}) + (b + 5\mathbb{Z}) = (a + b) + 5\mathbb{Z}$ (i.e., the shortcut)

$$(3 + 5\mathbb{Z}) + (4 + 5\mathbb{Z}) = 7 + 5\mathbb{Z} = 2 + 5\mathbb{Z}.$$

We've seen that $\mathbb{Z}/5\mathbb{Z} \cong \mathbb{Z}_5$ as additive groups.

+	$0 + 5\mathbb{Z}$	$1 + 5\mathbb{Z}$	$2 + 5\mathbb{Z}$	$3 + 5\mathbb{Z}$	$4 + 5\mathbb{Z}$
$0 + 5\mathbb{Z}$	$0 + 5\mathbb{Z}$	$1 + 5\mathbb{Z}$	$2 + 5\mathbb{Z}$	$3 + 5\mathbb{Z}$	$4 + 5\mathbb{Z}$
$1 + 5\mathbb{Z}$	$1 + 5\mathbb{Z}$	$2 + 5\mathbb{Z}$	$3 + 5\mathbb{Z}$	$4 + 5\mathbb{Z}$	$0 + 5\mathbb{Z}$
$2 + 5\mathbb{Z}$	$2 + 5\mathbb{Z}$	$3 + 5\mathbb{Z}$	$4 + 5\mathbb{Z}$	$0 + 5\mathbb{Z}$	$1 + 5\mathbb{Z}$
$3 + 5\mathbb{Z}$	$3 + 5\mathbb{Z}$	$4 + 5\mathbb{Z}$	$0 + 5\mathbb{Z}$	$1 + 5\mathbb{Z}$	$2 + 5\mathbb{Z}$
$4 + 5\mathbb{Z}$	$4 + 5\mathbb{Z}$	$0 + 5\mathbb{Z}$	$1 + 5\mathbb{Z}$	$2 + 5\mathbb{Z}$	$3 + 5\mathbb{Z}$

Question: But \mathbb{Z}_5 is also a ring. Can we define multiplication in $\mathbb{Z}/5\mathbb{Z}$ and turn it into a ring, too? How?!

- For instance, what should $(3 + 5\mathbb{Z}) \cdot (4 + 5\mathbb{Z})$ be?

Answer: $(3 + 5\mathbb{Z}) \cdot (4 + 5\mathbb{Z}) = 3 \cdot 4 + 5\mathbb{Z} = 2 + 5\mathbb{Z}$.

Key: Adapt the shortcut for coset multiplication.

Definition: Multiply cosets in $\mathbb{Z}/5\mathbb{Z}$ by $(a + 5\mathbb{Z}) \cdot (b + 5\mathbb{Z}) = a \cdot b + 5\mathbb{Z}$.

$$(2 + 5\mathbb{Z}) \cdot (3 + 5\mathbb{Z}) = 6 + 5\mathbb{Z} = 1 + 5\mathbb{Z}. \quad \leftarrow \text{multiplicative identity}$$

Thus, $2 + 5\mathbb{Z}$ and $3 + 5\mathbb{Z}$ are units with

$$(2 + 5\mathbb{Z})^{-1} = 3 + 5\mathbb{Z} \quad \text{and} \quad (3 + 5\mathbb{Z})^{-1} = 2 + 5\mathbb{Z}.$$

Conclusion: $\mathbb{Z}/5\mathbb{Z}$ is a **quotient ring**, and it's (ring) isomorphic to \mathbb{Z}_5 .

Consider the polynomial ring $\mathbb{Z}_3[x]$ and a subset

$$\langle x^2 \rangle = \{x^2 \cdot q(x) \mid q(x) \in \mathbb{Z}_3[x]\},$$

i.e., the **principal ideal** generated by x^2 (or the set of all multiples of x^2).


The **quotient ring** $\mathbb{Z}_3[x]/\langle x^2 \rangle$ contains cosets of the form

$$a(x) + \langle x^2 \rangle \quad \text{where } a(x) \in \mathbb{Z}_3[x].$$

Compare this with $\mathbb{Z}/5\mathbb{Z}$ which contains cosets of the form

$$a + 5\mathbb{Z} \quad \text{where } a \in \mathbb{Z}.$$

Key: $\langle x^2 \rangle$ will play the role of $5\mathbb{Z}$. (Both are *ideals*.)

 Also, $5\mathbb{Z} = \{5 \cdot q \mid q \in \mathbb{Z}\} = \langle 5 \rangle$.

Problem #2: Let $\alpha(x), \beta(x) \in \mathbb{Z}_3[x]$ where

$$\alpha(x) = 2x^7 + x^5 + 2x^4 + 2x + 1 \text{ and } \beta(x) = 2x + 1.$$

- $\alpha(x) \neq \beta(x)$ in $\mathbb{Z}_3[x]$, they're different polynomials.
- But in $\mathbb{Z}_3[x]/\langle x^2 \rangle$, their cosets are the same, i.e.,

$$\alpha(x) + \langle x^2 \rangle = \beta(x) + \langle x^2 \rangle, \text{ because } \alpha(x) - \beta(x) \in \langle x^2 \rangle.$$

Key: Compare this with how $378 \neq 3$ in \mathbb{Z} ,

but $378 + 5\mathbb{Z} = 3 + 5\mathbb{Z}$ in $\mathbb{Z}/5\mathbb{Z}$, because $378 - 3 \in 5\mathbb{Z}$.

Problem #4: The distinct elements of $\mathbb{Z}_3[x]/\langle x^2 \rangle$ are

$$\begin{aligned}\mathbb{Z}_3[x]/\langle x^2 \rangle &= \{(ax + b) + \langle x^2 \rangle \mid a, b \in \mathbb{Z}_3\} \\ &= \{(0x + 0) + \langle x^2 \rangle, (0x + 1) + \langle x^2 \rangle, (0x + 2) + \langle x^2 \rangle, \\ &\quad (1x + 0) + \langle x^2 \rangle, (1x + 1) + \langle x^2 \rangle, (1x + 2) + \langle x^2 \rangle, \\ &\quad (2x + 0) + \langle x^2 \rangle, (2x + 1) + \langle x^2 \rangle, (2x + 2) + \langle x^2 \rangle\}\end{aligned}$$

(Watch Proof of the Day for why these are actually distinct.)


Units in $\mathbb{Z}_3[x]/\langle x^2 \rangle$

$$((x + 1) + \langle x^2 \rangle) \cdot ((2x + 1) + \langle x^2 \rangle) = \underline{(x + 1)(2x + 1) + \langle x^2 \rangle}$$

$$= \underline{(2x^2 + \overset{0}{\cancel{3}x} + 1) + \langle x^2 \rangle}$$

$$= (2x^2 + 1) + \langle x^2 \rangle$$

$$= 1 + \langle x^2 \rangle$$

 since $(2x^2 + 1) - 1 = 2x^2 \in \langle x^2 \rangle$.

$\implies (x + 1) + \langle x^2 \rangle$ and $(2x + 1) + \langle x^2 \rangle$ are units.

Zero divisors in $\mathbb{Z}_3[x]/\langle x^2 \rangle$

$$(x + \langle x^2 \rangle) \cdot (x + \langle x^2 \rangle) = x^2 + \langle x^2 \rangle = 0 + \langle x^2 \rangle.$$

$\neq 0 + \langle x^2 \rangle.$

just like $5 + 5\mathbb{Z} = 0 + 5\mathbb{Z}.$

$\implies x + \langle x^2 \rangle$ is a zero divisor, hence not a unit.

$\implies \mathbb{Z}_3[x]/\langle x^2 \rangle$ is *not* a field.