# Warmup Q1)

$R = (\mathbb{Z}/5)[x]$, and $I = (x^2 + x + \overline{2})_{(\mathbb{Z}/5)[x]} \subset R$

- Show that $(\mathbb{Z}/5)[x]/I$ is a field.
- Find (multiplicative) inverse of $(\overline{2}x + \overline{3}) + I$.

# Prime and maximal ideals

$R$ is a commutative ring, $I \subsetneq R$ an ideal.

$I$ is prime if

- $ab \in I$ implies $a \in I$ or $b \in I$.

$I$ is maximal if

- $I \subset J \subset R$ implies $J = I$ or $J = R$.

(If $I \subset J$, can think $I$ is *smaller* than $J$. A maximal ideal is *bigger* than any comparable proper ideal.)

# Quotients by prime or maximal

**Proposition (15.4)**

*Given $R$ a commutative ring, and $I \subset R$ an ideal.*

- *$I$ is prime iff $R/I$ is an integral domain*
- *$I$ is maximal iff $R/I$ is a field*

Since a field is an integral domain, a maximal ideal is prime. (Cf. Lemma 15.3)

# Q1)

$R = (\mathbb{Z}/5)[x]$, and $I = (x^2 + x + \overline{2})_{(\mathbb{Z}/5)[x]} \subset R$

Show $(\mathbb{Z}/5)[x]/I$ is a field.

- Has the form $R/I$, so show $I$ is maximal
- $R = (\mathbb{Z}/5)[x]$ is a PID, so $I$ is maximal if generator is irreducible (See Q3)
- $x^2 + x + \overline{2}$ has no roots, so is irreducible (because it has degree 2)

So $(\mathbb{Z}/5)[x]/I$ is a field.

# Q1 ctd)

$R = (\mathbb{Z}/5)[x]$, and $I = (x^2 + x + \overline{2})_{(\mathbb{Z}/5)[x]} \subset R$

Find (multiplicative) inverse of $(\overline{2}x + \overline{3}) + I$.

- Inverse has form $(ax + b) + I$
  (linear representative by division algorithm)
- Set up and solve system of equations
  (See solutions)
- Remember that $x^2 + I = (-x - \overline{2}) + I$

Or, use Euclidean algorithm and read it backwards...

# Q1 ctd)

In $R = (\mathbb{Z}/5)[x]$

$$\begin{aligned} x^2 + x + \overline{2} &= q(x)(\overline{2}x + \overline{3}) + r(x) \\ &= (\overline{3}x + \overline{1}) \cdot (\overline{2}x + \overline{3}) - \overline{1} \end{aligned}$$

Rearrange to write

$$\overline{1} = -(x^2 + x + \overline{2}) + (\overline{3}x + \overline{1})(\overline{2}x + \overline{3})$$

Modulo $I$

$$\overline{1} + I = ((\overline{3}x + \overline{1}) + I) \cdot ((\overline{2}x + \overline{3}) + I)$$

So $(\overline{3}x + \overline{1}) + I$ is the multiplicative inverse.

(Repeat steps for more complicated examples.)

# First isomorphism theorem

**Theorem (13.2)**

*Given ring homomorphism* $\phi\colon R \to S$. *Define associated map* $\overline{\phi}$ *by*

$$\begin{aligned} \overline{\phi}\colon R/\ker\phi &\to \operatorname{im}\phi \\ r + \ker\phi &\mapsto \phi(r) \end{aligned}$$

*Then* $\overline{\phi}$ *is an isomorphism. So* $R/\ker\phi \cong \operatorname{im}\phi$

If you see an isomorphism involving a quotient ring, think First Isomorphism Theorem