Last time: Defined a ring \( R \), with two binary operations

\[ + : \text{addition} \]

\[ \cdot : \text{multiplication} \]

with the following properties

1. \((R, +)\) makes an abelian gp
   - in particular, \( \exists 0 \in R \), (\( \exists \): there exists)
     - additive identity
   - \( \exists \) additive inverses: \( \forall b \in R \exists -b \in R \) so that
     \[ b + (-b) = 0 \]
   - addition is commutative, i.e. \( a + b = b + a \)
   - addition is associative, i.e. \( a + (b + c) = (a + b) + c \).

2. the binary operation of multiplication interacts with addition in a precise way:
   - distributive property:
     \[ a(b+c) = ab + ac \text{ and } (b+c)a = ba + ca \]
   - mult. is associative: \( a(bc) = (ab)c \).

More examples
More examples

- \( \mathbb{Z}/n\mathbb{Z} \) (in your textbook, this is denoted \( \mathbb{Z}_n \))
- Elements of \( \mathbb{Z}/n\mathbb{Z} \) are by definition cosets
  - \( a + n\mathbb{Z} \)
  - Addition is
    \[
    (a + n\mathbb{Z}) + (b + n\mathbb{Z}) = a + b + n\mathbb{Z}
    \]
  - Multiplication is
    \[
    (a + n\mathbb{Z}) \cdot (b + n\mathbb{Z}) = ab + n\mathbb{Z}
    \]

Ex \( \quad n = 9 \)
- \( 3 + 12 \equiv 15 \equiv 6 \mod 9 \)
- \( 4 \cdot 5 \equiv 20 \equiv 2 \mod 9 \)

Question: What is \( 50 \cdot 2 + 59 \cdot 7 \equiv ? \mod 9 ? \)

\[

text{III} \quad 50 \equiv 5 \mod 9 \\
59 \equiv 5 \mod 9 \\
5 \cdot 2 + 5 \cdot 7 \\
5 \cdot (2 + 7) \\
50 \equiv 59 \mod 9 \\
50 \cdot 2 + 59 \cdot 7 \equiv 50 \cdot 2 + 50 \cdot 7 \\
\equiv 50 \cdot (2 + 2) \\
\equiv 50 \cdot 0 \equiv 0 \mod 9
\]
Example $\mathbb{Z}[x]$: polynomials in $x$ with integer coefficients is a ring.

- Addition is the usual addition of polynomials.
  \[
  \exists: (x^2 + 4x - 3) + (x^3 + 2x + 5) = x^3 + x^2 + 6x + 2
  \]

  I.e. \[
  \left( \sum_{j=0}^{\infty} a_j x^j \right) + \left( \sum_{j=0}^{\infty} b_j x^j \right) = \sum_{j=0}^{\infty} (a_j + b_j) x^j
  \]
  \[a_j, b_j \in \mathbb{Z}\]

- Multiplication is usual multiplication of polynomials.
  \[
  \exists: (x+1) \cdot (x-3) = x^2 - 2x - 3
  \]
  \[
  \left( \sum_{j=0}^{\infty} a_j x^j \right) \left( \sum_{k=0}^{\infty} b_k x^k \right) = \sum_{j,k} a_j b_k x^{j+k}
  \]

**Question:** Does this ring have a multiplicative identity?

**Answer:** Yes, it does: $1 = x^0$.

Example

- $\mathbb{Z}/n\mathbb{Z}[x]$: the polynomials in $x$ with coefficients in $\mathbb{Z}/n\mathbb{Z}$ is a ring.

Example $n = 6$

\[
(2x) \cdot (3x + 2) = 6x^2 + 4x
\]
\((2x) \cdot (3x+2) = \frac{6x^2 + 4x}{4x} \opleft[ \frac{2x}{x} \right] = \frac{1}{x}\) in \(\mathbb{Z}_2[x]\)

Example: \((x+1)(x^2+3) = x^3 + x^2 + 3x + 3\) in \(\mathbb{Z}_2[x]\)

• In fact, if \(R\) is a commutative ring with 1, then \(R[x]\) is again a commutative ring with 1.

• By def., \(R[x]\) is the polynomials in \(x\) with coefficients in \(R\).

• If \(1 \in R\) is the unit identity, \(1 \cdot x^n \in R[x]\) is the multiplicative identity in \(R[x]\).

• Suppose \(R_1, R_2, \ldots, R_n\) rings

\(R_1 \times R_2 \times \ldots \times R_n = \\{ (a_1, a_2, \ldots, a_n) : a_i \in R_i \} \)

• Is a ring with addition defined as:

\[- (a_1, a_2, \ldots, a_n) + (b_1, b_2, \ldots, b_n) = (a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n) \]

\[- (a_1, \ldots, a_n) \cdot (b_1, \ldots, b_n) = (a_1 b_1, \ldots, a_n b_n) \]

Properties of Rings

• Recall that \(-b\) denotes the additive inverse of \(b \in R\), so that \(b + (-b) = 0\).
If \( b, c \in R \), we'll write \( b - c = b + (-c) \)

**Thm** Suppose \( a, b, c \in R \), ring:

1. \( a0 = 0a = 0 \)
2. \( a(-b) = (-a)b = -(ab) \)
3. \( (-a)(-b) = ab \)
4. \( a(b - c) = ab - ac \) and \( (b - c)a = ba - ca \)

Furthermore, if \( R \) has a identity \( 1 \), then:

5. \( (-1)a = -a \)
6. \( (-1)(-1) = 1 \)

**Pf:** \( O + O = 0 \) by \( c \) additive identity

\( \rightarrow \) distributive property \( a \cdot O = a(0+0) = aO + aO \)

\( \Rightarrow O = a \cdot O \) by cancelling

same argument: \( O = O \cdot a \)

\( a(-b) + ab = a(-b+b) = aO = 0 \)

\( \Rightarrow a(-b) = -(ab) \)

same argument: \( (-a)b = -(ab) \)

\( \Rightarrow a(-b) = (-a)b = -(ab) \).

\( (-a)(-b) = -(a)(-b) = --(ab) = ab \)
next time: finish proof