At the end of the previous lecture we mentioned a subring criterion:

Suppose \((A, +, \cdot)\) is a ring. Then \(B \subseteq A\) is a subring if and only if

1. \((B, +)\) is a subgroup,
2. \(B\) is closed under multiplication.

As we combine this with a subgroup criterion we get the following:

**Proposition (Subring criterion)** Suppose \((A, +, \cdot)\) is a ring, and \(B \subseteq A\). Then \(B\) is a subring if and only if \(\forall b_1, b_2 \in B\)

1. \(b_1 - b_2 \in B\) and
2. \(b_1 \cdot b_2 \in B\).

**Ex.** \(n \mathbb{Z}\) is a subring of \(\mathbb{Z}\) which is not unital if \(n > 1\).

**Ex.** \(M_n(\mathbb{Q})\): the set of \(n \times n\) rational matrices with the usual addition and multiplication of matrices.

In fact, for any ring \(R\), \(M_n(R)\) is a ring (Check why.)

**Ex/Def.** Suppose \(R_1, \ldots, R_n\) are rings. Then the **direct product** \(R_1 \times \cdots \times R_n\) is a ring with componentwise operations; that means

\[(a_1, \ldots, a_n) + (b_1, \ldots, b_n) = (a_1 + b_1, \ldots, a_n + b_n)\] and
$(a_1, \ldots, a_n) \cdot (b_1, \ldots, b_n) = (a_1 b_1, \ldots, a_n b_n)$.

Notice if $1_{R_i}$ is the unity of $R_i$ for $1 \leq i \leq n$, then $(1_{R_1}, \ldots, 1_{R_n})$ is the unity of $R_1 \times \cdots \times R_n$.

**Ex.** Compute $(1, 0) \cdot (1, \sqrt{2})$ in $\mathbb{Z} \times \mathbb{R}$;

$$(1, 0) \cdot (1, \sqrt{2}) = (1, 0).$$

**Ex.** Compute $(1, 0) + (1, \sqrt{2})$ in $\mathbb{Z} \times \mathbb{R}$;

$$(1, 0) + (1, \sqrt{2}) = (2, \sqrt{2}).$$

**Ex.** Compute

$$\begin{bmatrix} (1, 0) & (1, \sqrt{2}) \\ (0, 1) & (1, 1) \end{bmatrix}^2 \text{ in } M_2(\mathbb{Z} \times \mathbb{R}).$$

$$\begin{bmatrix} (1, 0) & (1, \sqrt{2}) \\ (0, 1) & (1, 1) \end{bmatrix} \begin{bmatrix} (1, 0) & (1, \sqrt{2}) \\ (0, 1) & (1, 1) \end{bmatrix} =$$

$$\begin{bmatrix} (1, 0)(1, 0) + (1, \sqrt{2})(0, 1) & (1, 0)(1, \sqrt{2}) + (1, \sqrt{2})(1, 1) \\ (0, 1)(1, 0) + (1, 1)(0, 1) & (0, 1)(1, \sqrt{2}) + (1, 1)(1, 1) \end{bmatrix} =$$

$$= \begin{bmatrix} (1, 0) + (0, \sqrt{2}) & (1, 0) + (1, \sqrt{2}) \\ (0, 0) + (0, 1) & (0, \sqrt{2}) + (1, 1) \end{bmatrix} = \begin{bmatrix} (1, \sqrt{2}) & (2, \sqrt{2}) \\ (0, 1) & (1, 1 + \sqrt{2}) \end{bmatrix}$$
Remark. \((0,1) \cdot (1,0) = (0,0)\); so sometimes product of two non-zero elements is zero. Such elements are called zero-divisors.

**Def.** Suppose \(A\) is a commutative ring. \(a \in A \setminus \{0\}\) is called a zero-divisor if \(\exists b \in A \setminus \{0\}\) s.t. \(ab = 0\).

**Ex.** \((1,0)\) is a zero-divisor in \(\mathbb{Z} \times \mathbb{R}\).

**Pr.** \((1,0) \cdot (0,1) = (0,0)\).

**Ex.** The ring \(\mathbb{Z}_n\) of integers modulo \(n\). I am going to follow your book and use a bit non-standard way of defining \(\mathbb{Z}_n\).

\[\mathbb{Z}_n = \{0, 1, \ldots, n-1\} \text{ as set.}\]

**Division algorithm** \(m \in \mathbb{Z}, n \in \mathbb{Z}^+, \exists! (q, r) \in \mathbb{Z} \times \mathbb{Z}, m = nq + r, 0 \leq r < n.\)

\(q\) is called the quotient of \(m\) divided by \(n\) and \(r\) is called the remainder.

For \(a, b \in \mathbb{Z}_n\), \(a \oplus b := \text{the remainder of } a + b \text{ divided by } n.\)
and \( a \text{ } \circ \text{ } b := \text{ the remainder of } a \cdot b \text{ divided by } n \).

To see why \( \mathbb{Z}_n \) is a ring, let us recall basic properties of congruence arithmetic from your previous courses:

**Def.** For \( a, b \in \mathbb{Z} \), we say \( a \equiv b \text{ (mod n) if } n \mid a - b \). (We say \( a \) is congruent to \( b \) modulo \( n \))

**Basic Properties of Congruence Arithmetic**

1. \( a \equiv a \text{ (mod n) ; } a_1 \equiv a_2 \text{ (mod n)} \iff a_1 - a_2 \equiv 0 \text{ (mod n)}. \)

2. \( a_1 \equiv a_2 \text{ (mod n)} \iff a_1 + b_1 \equiv a_2 + b_2 \text{ (mod n)} \)

3. \( a_1 \equiv a_2 \text{ (mod n)} \iff a_1 \cdot b_1 \equiv a_2 \cdot b_2 \text{ (mod n)} \)

4. \( r \) is the remainder of \( a \) divided by \( n \) if and only if

\[ a \equiv r \text{ (mod n) and } r \in \{0, 1, \ldots, n-1\} \]
**Lecture 02: Basic properties of congruence arithmetic**

Monday, April 2, 2018 11:06 AM

1. \(\text{If } a \equiv 0 \pmod{n}, \text{ then } n \mid a-a; \text{ and so } a \equiv a \pmod{n}.\)

2. \(a_1 \equiv a_2 \pmod{n} \Rightarrow n \mid a_1-a_2 \Rightarrow a_1-a_2 = nk \text{ for some } k \in \mathbb{Z} \)

3. \(a_2 \equiv a_3 \pmod{n} \Rightarrow n \mid a_2-a_3 \Rightarrow a_2-a_3 = nl \text{ for some } l \in \mathbb{Z} \)

\[ \Rightarrow (a_1-a_2) + (a_2-a_3) = nk + nl = n(k+l) \in \mathbb{Z} \]

\[ \Rightarrow n \mid a_1-a_3 \Rightarrow a_1 \equiv a_3 \pmod{n}. \]

2. \(a_1 \equiv a_2 \pmod{n} \Rightarrow n \mid a_1-a_2 \Rightarrow a_1-a_2 = nk \text{ for some } k \in \mathbb{Z}.

b_1 \equiv b_2 \pmod{n} \Rightarrow n \mid b_1-b_2 \Rightarrow b_1-b_2 = nl \text{ for some } l \in \mathbb{Z}.

\[ \Rightarrow (a_1-a_2) + (b_1-b_2) = n(k+l) \Rightarrow a_1+b_1 \equiv a_2+b_2 \pmod{n}. \]

3. As in part (2), \(a_1-a_2 = nk \) and \(b_1-b_2 = nl \) for some \(k, l\) in \(\mathbb{Z}\). Then

\[ a_1b_1-a_2b_2 = a_1b_1 - a_2b_1 + a_2b_1 - a_2b_2 \]

\[ = (a_1-a_2)b_1 + a_2(b_1-b_2) \]

We will continue next time.