Lecture 2: (1)

Repetition:
- $a \equiv b \pmod n$ if $n \mid b-a$
- Congruence classes $[a] = \{ b \in \mathbb{Z} \mid b \equiv a \pmod n \}$

  The congruence classes constitutes a partition of $\mathbb{Z}$.
- $\mathbb{Z}_n = \{[0],[1],[2],\ldots,[n-1]\}$

  operations $[a] \oplus [b] = [a+b]$

  $[a] \odot [b] = [ab]$

Convention: We write $+$ and $\cdot$ instead of $\oplus$ and $\odot$, if context is clear.
Sometimes we write a instead of $[a]$.

Properties of $\mathbb{Z}$ and $\mathbb{Z}_n$ are the same (page 34), with a few exceptions:

In $\mathbb{Z}_6$:
- i) $[3]\cdot[2] = [6] = [0]$
- ii) eq. $[2]\cdot x = [2]$ has more than one solution
- iii) eq. $[2]\cdot x = [1]$ has no solution

Theorem: Let $p \in \mathbb{Z}$. The following are equivalent:

1. p is prime
2. eq. $ax = 1$ has solution in $\mathbb{Z}_p$ for all $a \neq 0$ in $\mathbb{Z}_p$
3. $ab = 0$ in $\mathbb{Z}_p \Rightarrow a=0$ or $b=0$ in $\mathbb{Z}_p$

Proof: (1) $\Rightarrow$ (2): Assume $[a] \neq [0]$. This means that $p \nmid a \Rightarrow (p,a) = 1 \Rightarrow$ there exist u,v such that (2)

$au + pv = 1 \Rightarrow au \equiv 1 \pmod p$

$\Rightarrow [a]\cdot[u] = [1] \Rightarrow [u]$ is a solution the equation.

(2) $\Rightarrow$ (3): Assume $a \neq 0$ in $\mathbb{Z}_p$. Then there exists x in $\mathbb{Z}_p$ such that $ax = 1$. We get

In $\mathbb{Z}_p$: $ab = 0 \Rightarrow xab = x \cdot 0 \Leftrightarrow \underbrace{(ax)}_{=1}b = 0 \Leftrightarrow b = 0$

(3) $\Rightarrow$ (1): Suppose p not prime. Then $p = ab$ where $1 < a,b < p \Rightarrow \underset{\neq [0]}{[a]}\cdot\underset{\neq [0]}{[b]} = [ab] = [p] = [0]$.

Contradicts assumption. □

Note: Proof (1) $\Rightarrow$ (2) provides a method for finding solution of $ax = 1$ in $\mathbb{Z}_p$: Find u and v by applying Euclid's alg. "backwards".

Exercise: Prove that
$[a]x = [1]$ has solution in $\mathbb{Z}_n \Leftrightarrow (a,n) = 1$.

Corollary: p prime, $a \neq 0$ in $\mathbb{Z}_p \Rightarrow$ For any b, the eq. $ax = b$ has unique solution in $\mathbb{Z}_p$.

Proof: Existence: There exists x such that $ax = 1$ in $\mathbb{Z}_p$
$\overset{}{\underset{(2)}{\Rightarrow}} a(xb) = b$ in $\mathbb{Z}_p$.

Uniqueness: Assume $ax = b$ and $ay = b$ in $\mathbb{Z}_p$. (3)

Then $a(x-y) = ax - ay = b - b = 0$.

$\overset{(3)}{\Rightarrow} (a=0)$ or $x - y = 0 \Rightarrow x = y$. □

Rings

Def (Ring): The set $R \neq \emptyset$, equipped with the op. $+$ and $\cdot$, is called a ring if, for all $a,b,c \in R$:

addition:
1. $a,b \in R \Rightarrow a+b \in R$ (closure)
2. $a+(b+c) = (a+b)+c$ (associativity)
3. $a+b = b+a$ (commutativity)
4. there exists element $0_R \in R$, s.t. $a + 0_R = 0_R + a = a$ (zero element)
5. For every $a \in R$, ~~there exists~~ the eq. $a + x = 0_R$ has a solution in R. (add. inverse)

multiplic.:

6. $a,b \in R \Rightarrow ab \in R$ (closure)
7. $a(bc) = (ab)c$ (assoc.)

add. + mult.:

8. $a(b+c) = ab + ac$, $(a+b)c = ac + bc$ (distributivity)

Def: The ring R is commutative if
$ab = ba$ for all $a,b \in R$.

Def: The ring R is a ring with identity if there exists element $1_R \in R$ s.t. $a \cdot 1_R = 1_R \cdot a = a$ for all $a \in R$. (4)

Exercises:
- 0_R and 1_R are unique
- $0_R = 1_R \Rightarrow R = \{0_R\}$ (zero ring)

Note: 0_R and 1_R are written 0 and 1 if the context is clear.

Ex:
- $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ and $\mathbb{Z}_n$ commutative rings with identity (usual operations)
- even integers $2\mathbb{Z} = \{2k \mid k \in \mathbb{Z}\}$ comm. ring but no identity
- odd integers $\{2k+1 \mid k \in \mathbb{Z}\}$ no ring. E.g not closed under addition.
- $M_n(\mathbb{R}) = \{n \times n\text{-matrices with real elements}\}$ (usual operations) is a (noncommutative) ring with identity.
- R ring $\Rightarrow M_n(R)$ ring
- R_1, R_2 rings $\Rightarrow R_1 \times R_2 = \{(a,b) \mid a \in R_1, b \in R_2\}$

  with op. $(a,b) + (c,d) = (a+c, b+d)$

  $(a,b)\cdot(c,d) = (ac, bd)$

  is a ring
- $\mathbb{R}[x] = \{\text{polynomials in } x \text{ with real coeff.}\}$ (usual op.) is a commutative ring with identity.

(5)

Def: The subset $S \subseteq R$, R ring, is a <u>subring</u> of R if S is a ring w.r.t same operations.

Ex: $\mathbb{Z}$ subring of $\mathbb{Q}$
$\mathbb{Q}$ subring of $\mathbb{R}$
$2\mathbb{Z}$ subring of $\mathbb{Z}$

Note:
- $0_S = 0_R$ (exercise)
- in general not $1_S = 1_R$ (exercise, hint: consider $\mathbb{Z}\times\mathbb{Z}$)

Def: Let R be a comm. ring with identity. If R has no <u>zero-divisors</u>, i.e.

$$ab = 0_R \Rightarrow a = 0_R \text{ or } b = 0_R \quad \text{for all } a,b \in R,$$

it is called an <u>integral domain</u>.

Ex: $\mathbb{Z}, \mathbb{R}, \mathbb{Q}, \mathbb{C}$ integral domains
$\mathbb{Z}_4$ not integral domain; $2\cdot 2 = 0$.

> **Theorem:** $\mathbb{Z}_n$ int. domain $\Leftrightarrow$ n prime
> **Proof:** From previous th.

Def: Let R be a commutative ring with identity s.t. $ax = 1_R$ has a solution for all $a \neq 0$. Then R is called a <u>field</u> (swedish: <u>kropp</u>).

Ex: $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ fields, $\mathbb{Z}_n$ field $\Leftrightarrow$ n prime (prev. th.),
$\mathbb{Z}$ not a field: e.g. $2x = 1$ no solution in $\mathbb{Z}$.

(6)

Note: "noncommutative field" = <u>division ring</u>
($ax = 1_R$ <u>and</u> $xa = 1_R$ has solution)
Note that $M_n(\mathbb{R})$ is <u>not</u> a division ring since not every matrix is invertible:
$AX = I$ and $XA = I$ sol. $\Leftrightarrow$ A invertible

Ex: $K = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \,\middle|\, a,b \in \mathbb{R} \right\} \subseteq M_2(\mathbb{R})$

<u>K ring:</u> (1): $\begin{pmatrix} a & b \\ -b & a \end{pmatrix} + \begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \begin{pmatrix} a+c & b+d \\ -(b+d) & a+c \end{pmatrix} \in K$

(2), (3): follows from $M_2(\mathbb{R})$

(4): $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \in K$

solution!

(5): $\begin{pmatrix} a & b \\ -b & a \end{pmatrix} + \begin{pmatrix} -a & -b \\ b & -a \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

(6): $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}\begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \begin{pmatrix} ac-bd & ad+bc \\ -(ad+bc) & ac-bd \end{pmatrix}$

(7), (8): follows from $M_2(\mathbb{R})$

<u>K commutative:</u> $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}\begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \begin{pmatrix} ac-bd & ad+bc \\ -(ad+bc) & ac-bd \end{pmatrix} = \begin{pmatrix} c & d \\ -d & c \end{pmatrix}\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$

<u>K has identity:</u> $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in K$

Moreover, $A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ invertible, since $\begin{vmatrix} a & b \\ -b & a \end{vmatrix} = a^2 + b^2 \neq 0$,
i.e. A^{-1} exists.

Conclusion, K is a <u>field</u>.

(7)

Note: To check that K is a <u>sub</u>ring of $M_n(\mathbb{R})$, we only need to check prop. (1), (4), (5), (6). The rest is inherited

---

<u>Ring properties:</u>

> **Theorem:** The solution x of eq. $a + x = 0_R$ in (5) is <u>unique</u>

Proof: Assume $a + x = a + y = 0_R$. Then
$$x = x + 0_R = x + (a+y) = (x+a)+y = (a+x)+y = 0_R + y = y$$
$\square$

Note: The unique solution is denoted $-a$.

Def (subtraction): $b - a \overset{\text{def.}}{=} b + (-a)$.

> **Theorem:**
> - $a + b = a + c \Rightarrow b = c$
> - $a\cdot 0_R = 0_R\cdot a = 0_R$
> - $a(-b) = (-a)b = -(ab)$
> - $-(-a) = a$
> - $-(a+b) = (-a) + (-b)$
> - $-(a-b) = -a + b$
> - $(-a)(-b) = ab$
> - $(-1_R)a = -a$ if R has identity

~~Proof: Exercise For example~~

(8)

Proof: • <u>$a + b = a + c \Rightarrow b = c$:</u>

$a + b = a + c \Rightarrow (-a) + (a+b) = (-a) + (a+c)$
$\Rightarrow ((-a)+a) + b = ((-a)+a) + c \Rightarrow 0_R + b = 0_R + c$
$\Rightarrow b = c$

• <u>$a\cdot 0_R = 0_R$:</u> $a\cdot 0_R + 0_R = a\cdot 0_R = a\cdot(0_R + 0_R) = a\cdot 0_R + a\cdot 0_R$

By the above law we now get $0_R = a\cdot 0_R$

The rest is exercise. $\square$

> **Theorem:** To check that $S \subseteq R$ ($S \neq \emptyset$) is a subring of R, we only need
> (I): $a,b \in S \Rightarrow a - b \in S$
> (II): $a,b \in S \Rightarrow ab \in S$

Proof: Enough to check property (1), (4), (5), (6) (see note above)

(6): Identical to (II)
(4): Take any $a \in S$ ($S \neq \emptyset$). By (I), $a - a = 0_R \in S$
(5): If $a \in S$, then by (I) we get $0_R - a = -a \in S$
(1): $a,b \in S \underset{(5)}{\Rightarrow} a, -b \in S \underset{(I)}{\Rightarrow} a - (-b) = a + b \in S$ $\square$

Def: Let $a \in R$. The element $x \in R$ is called a (multiplicative) <u>inverse</u> of a if
$$ax = xa = 1_R$$

Theorem: The multiplicative inverse is unique.

Proof: Assume $ax = xa = 1_R$ and $ay = ya = 1_R$.

Then $x = 1_R \cdot x = (ya)x = y(ax) = y \cdot 1_R = y$. □

Note: The unique solution x is denoted a^{-1}. An element a which has an inverse is called a unit.

Ex: In a field F, every element $a \neq 0_F$ is a unit.

Ex: In $\mathbb{Z}_n$: $[a]$ unit $\Leftrightarrow$ $(a,n) = 1$

(see exercise on page ②)

Theorem: F field $\Rightarrow$ F integral domain.

Proof: Check that F has no zero-divisors:

$$ab = 0_F,\ a \neq 0_F \underset{F \text{ field}}{\Rightarrow} a^{-1}(ab) = a^{-1} \cdot 0_F$$

$$\Rightarrow (a^{-1}a)b = 0_F \Rightarrow 1_F \cdot b = 0_F \Rightarrow b = 0_F. \quad \square$$

Theorem: R finite int. domain $\Rightarrow$ R field.

Proof: Check that every $a \neq 0_R$ has an inverse:

Assume $R = \{a_1, a_2, \ldots, a_n\}$ and construct elements

(*) $aa_1, aa_2, aa_3, \ldots, aa_n$ (n elements)

They are all different since, if $aa_i = aa_j$, then

$$aa_i - aa_j = 0_R \Rightarrow \underset{\neq 0_R}{a}(a_i - a_j) = 0_R \underset{\text{int. domain}}{\Rightarrow} a_i - a_j = 0_R$$

$$\Rightarrow a_i = a_j$$

Thus (*) is a permutation of elements of R.
In particular $aa_i = 1_R$ for some $i \Rightarrow a_i = a^{-1}$
$\Rightarrow R$ field. □

Ex: $\mathbb{Z}_n$ int. domain $\Leftrightarrow$ $\mathbb{Z}_n$ field

An example of an int. domain which is not a field is $\mathbb{Z}$. Only units are ± 1.