Lecture 5: Rings and fields

An *abelian group* is a set A with a function (addition)

$$A \times A \to A$$
$$(a,b) \mapsto a+b \qquad \text{such that}$$

(a) If $a_1, a_2, a_3 \in A$ then $(a_1+a_2)+a_3 = a_1+(a_2+a_3)$

(b) There exists $0 \in A$ such that
if $a \in A$ then $0+a=a$ and $a+0=a$.

(c) If $a \in A$ then there exists $-a \in A$ such that
$a+(-a)=0$ and $(-a)+a=0$.

Examples: (a) $\mathbb{Z}$ with addition.

(b) $M_{1\times 5}(\mathbb{R}) = \left\{\begin{matrix}\text{column vectors of length} \\ \text{5 with entries in } \mathbb{R}\end{matrix}\right\}$

with
$$\begin{pmatrix} a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \end{pmatrix} + \begin{pmatrix} b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \end{pmatrix} = \begin{pmatrix} a_1+b_1 \\ a_2+b_2 \\ a_3+b_3 \\ a_4+b_4 \\ a_5+b_5 \end{pmatrix}.$$

A *ring* is an abelian group R with a function (multiplication)

$$R \times R \to R$$
$$(a,b) \mapsto ab \qquad \text{such that}$$

(d) If $r_1, r_2, r_3 \in R$ then $(r_1 r_2) r_3 = r_1 (r_2 r_3)$,

(e) There exists $1 \in R$ such that
if $r \in R$ then $r \cdot 1 = r$ and $1 \cdot r = r$.

(f) If $r_1, r_2, r_3 \in R$ then

$$r_1(r_2+r_3) = r_1r_2 + r_1r_3 \quad \text{and} \quad (r_1+r_2)r_3 = r_1r_3 + r_2r_3$$

(the distributive properties).

Examples: (a) $\mathbb{Z}$ with addition and multiplication.

(b) $\mathbb{Z}/m\mathbb{Z}$ with addition and multiplication

(c) $\mathbb{C}[t]$, polynomials, with addition and multiplication

(d) $M_{n\times n}(\mathbb{R})$, square matrices, with addition and multiplication

$$\mathbb{C}[t] = \left\{ a_0 + a_1t + a_2t^2 + \cdots \;\middle|\; \begin{array}{l} a_i \in \mathbb{C} \text{ and all but a finite} \\ \text{number of the } a_i \text{ are } 0 \end{array} \right\}$$

$$\begin{aligned}(5t^2+3t+7)(3t^3+5) &= 15t^5 + 25t^2 + 9t^4 + 15t + 21t^3 + 35 \\ &= 15t^5 + 9t^4 + 21t^3 + 25t^2 + 15t + 35.\end{aligned}$$

A <u>commutative ring</u> is a ring R such that

(g) if $r_1, r_2 \in R$ then $r_1r_2 = r_2r_1$

A <u>field</u> is a commutative ring $\mathbb{F}$ such that

(h) If $r \in \mathbb{F}$ and $r \neq 0$ then there exists $r^{-1} \in \mathbb{F}$ such that $r \cdot r^{-1} = 1$ and $r^{-1} \cdot r = 1$.

Examples: (a) $\mathbb{Q} = \{ \frac{a}{b} \mid a, b \in \mathbb{Z},\ b \neq 0 \}$ with $\frac{a}{b} = \frac{c}{d}$ if $ad = bc$.

(b) $\mathbb{R} = \{\text{decimal expansions}\}$

(c) $\mathbb{C} = \{ a + bi \mid a, b \in \mathbb{R} \}$ with $i^2 = -1$.

Clocks

1	1 2	1 3 2	1 4 2 3	1 5 2 4 3
$\mathbb{Z}/1\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/3\mathbb{Z}$	$\mathbb{Z}/4\mathbb{Z}$	$\mathbb{Z}/5\mathbb{Z}$

Better to write

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

All of these are commutative rings.
Which are fields?

In $\mathbb{Z}/5\mathbb{Z}$: $1\cdot 1=1$, $2\cdot 3=1$, $3\cdot 2=1$, $4\cdot 4=1$

In $\mathbb{Z}/4\mathbb{Z}$: $1\cdot 1=1$, $3\cdot 3=1$ but $2\cdot x$ is never 1.

So 2 is not invertible in $\mathbb{Z}/4\mathbb{Z}$, and $\mathbb{Z}/4\mathbb{Z}$ is not a field.

<u>Example</u> $M_{2\times 2}(\mathbb{C})$ is <u>not</u> a commutative ring since

$$\begin{pmatrix}0&1\\0&0\end{pmatrix}, \begin{pmatrix}0&0\\1&0\end{pmatrix} \in M_{2\times 2}(\mathbb{C}) \quad \text{and}$$

$$\begin{pmatrix}0&1\\0&0\end{pmatrix}\begin{pmatrix}0&0\\1&0\end{pmatrix} = \begin{pmatrix}1&0\\0&0\end{pmatrix} \quad \text{and} \quad \begin{pmatrix}0&0\\1&0\end{pmatrix}\begin{pmatrix}0&1\\0&0\end{pmatrix} = \begin{pmatrix}0&0\\0&1\end{pmatrix}$$

so that

$$\begin{pmatrix}0&1\\0&0\end{pmatrix}\begin{pmatrix}0&0\\1&0\end{pmatrix} \neq \begin{pmatrix}0&0\\1&0\end{pmatrix}\begin{pmatrix}0&1\\0&0\end{pmatrix}.$$

<u>Example</u> Let A be an abelian group. Let $a \in A$.
Show that $-(-a) = a$.

<u>Proof</u> Assume $a \in A$.

To show: $-(-a) = a$.

We know: $-a$ is an element (call it b) such that

(1) $b + a = 0$ and $a + b = 0$.

We know: $-(-a) = -b$ is an element (call it c) such that

(2) $c + b = 0$ and $b + c = 0$.

To show: $c = a$.

$$c = c + 0 = c + (b + a) = (c + b) + a = 0 + a = a,$$

by properties (b), (1), (a), (2), (b), respectively.

<u>Example</u> Let A be an abelian group. Show that $0 \in A$ is unique.

<u>Proof</u> To show: $0 \in A$ is unique.

0 is an element (call it a) such that

(3) if $x \in A$ then $a + x = x$ and $x + a = x$.

Let b be another element such that

(4) if $x \in A$ then $b + x = x$ and $x + b = x$.

To show: $a = b$

$$a = a + b = b,$$ by (4) and (3), respectively.

<u>Example</u> Let R be a ring. Let $a \in R$.
Show that $0 \cdot a = 0$.

<u>Proof</u> Assume $a \in R$.

To show: $0 \cdot a = 0$.

$0 \cdot a = (0+0) \cdot a = 0 \cdot a + 0 \cdot a$. (by (b) and the distributive law)

Add $-(0 \cdot a)$ to each side to get

$0 = 0 \cdot a$ (because $0 \cdot a + (-(0 \cdot a)) = 0$)

//.

<u>Example</u> Let R be a ring. Let $a \in R$. Show that $(-1) \cdot a = -a$.

<u>Proof</u> Assume $a \in R$.

To show: $(-1) \cdot a = -a$.

We know: $-a$ is an element (call it b) such that

$b + a = 0$ and $a + b = 0$.

We know: -1 is an element (call it c) such that

$c + 1 = 0$ and $1 + c = 0$.

To show: $\cancel{(-1) \cdot a =}$ $c \cdot a = b$.

$c \cdot a + a = (c+1)a = 0 \cdot a = 0$, and

$a + c \cdot a = (1+c)a = 0 \cdot a = 0$.

Then $b = b + 0 = b + a + c \cdot a = 0 + c \cdot a = c \cdot a$. //.