Lecture 19, Oct. 17

Midterm today 7:00-8:50

RCH 207 Sec 2

RCH 211 Sec 1 A-O

RCH 309 Sec 1 P-Z

19.1 Definition. A **ring** (with identity) is a set R with two distinct elements $0, 1 \in R$ and two binary operations $+ : R^2 \to R$ and $\times : R^2 \to R$ where for $a, b \in R$ we write $+(a, b)$ as $a + b$, $\times(a, b)$ as $a \times b$ or $a \cdot b$ or ab, such that

1. $+$ is associative
$$\forall a, b, c \in R \ (a + b) + c = a + (b + c)$$
2. $+$ is commutative
$$\forall a, b \in R \ a + b = b + a$$
3. 0 is an identity under $+$
$$\forall a \in R \ a + 0 = a$$
4. every $a \in R$ has an inverse under $+$
$$\forall a \in R \, \exists b \in R \ a + b = 0$$
5. $\times$ is associative
$$\forall a, b, c \in R \ (ab)c = a(bc)$$
6. 1 is an identity under $\times$
$$\forall a \in R \ a \cdot 1 = a \text{ and } 1 \cdot a = a$$
7. $\times$ is distributive over $+$
$$\forall a, b, c \in R \ a(b + c) = ab + ac \text{ and } (a + b)c = ac + bc$$

A ring R is **commutative** when

8. $\times$ is commutative
$$\forall a, b \in R \ ab = ba$$

A **field** is commutative ring R such that

9. every nonzero $a \in R$ has an inverse under $\times$.
$$\forall 0 \neq a \in R \, \exists b \in R \ ab = 1$$

19.2 Theorem. *$\mathbb{Z}$ is commutative Ring. $\mathbb{Q}$ and $\mathbb{R}$ are fields.*

19.3 Example. $\mathbb{N}$ is not a ring (Axiom 4 does not hold)

$\mathbb{Z}$ is not a field (Axiom 9 does not work)

19.4 Example. The set of **integers modulo n**, denoted by $\mathbb{Z}_n$, is a ring for $n \in \mathbb{Z}$ with $n \geq 2$. Informally,

$$\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$$

and addition and multiplication modulo n are denoted as follows:

for $a, b \in \mathbb{Z}_n$

$a + b \in \mathbb{Z}_n$ is the remainder when $a + b \in \mathbb{Z}$ is divided by n

$ab \in \mathbb{Z}_n$ is the remainder when $ab \in \mathbb{Z}$ is divided by n

In $\mathbb{Z}_6$:

$+$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$\times$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

We shall see that $\mathbb{Z}_n$ is a field if and only if n is prime

19.5 Example. The field of **complex numbers** is the set

$$\mathbb{C} = \mathbb{R}^2 = \{(x, y) \mid x \in \mathbb{R}, y \in \mathbb{R}\}$$

and for $x, y \in \mathbb{R}$ we write

$$0 = (0, 0), 1 = (1, 0), i = (0, 1), x = (x, 0), iy = yi = (0, y), x + iy = (x, y)$$

and we define $+$ and $\times$ as follows

for $a, b, c, d \in R$

$$(a + ib) + (c + id) = (a, b) + (c, d) = (a + c, b + d) = (a + c) + i(b + d)$$

$$(a + ib)(c + id) = (ac - bd) + i(ad + bc)$$

Remark. Check that when $(a, b) \neq (0, 0)$, $a + ib$ has an inverse.

19.6 Example.

$$\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{R}$$

is a ring.

$$\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\} \subseteq \mathbb{R}$$

is a field.

$$\mathbb{Z}[\sqrt{3}i] = \{a + b\sqrt{3}i \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$$

is a ring.

$$\mathbb{Q}[\sqrt{3}i] = \{a + b\sqrt{3}i \mid a, b \in \mathbb{Q}\} \subseteq \mathbb{C}$$

is a field.

19.7 Example. If R is a ring (usually commutative), the set of polynomials

$$f(x) = c_0 + c_1x + c_2x^2 + \cdots + c_nx^n$$

with coefficients $c_k \in R$ is a ring (under addition and multiplication of polynomials) which we denote by $R[x]$

19.8 Example. If R is a ring, the set of all $n \times n$ matrices $\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix}$ with entries $A_{kl} = a_{kl} \in R$ is a ring, which we denote by $M_n(R)$ (or $M_{n\times n}(R)$) (under addition and multiplication of matrices.)

Remark. Matrices