MATH 415

Modern Algebra I

Lecture 15:
Rings and fields (continued).
Field of quotients.

Rings

Definition. A **ring** is a set R, together with two binary operations usually called **addition** and **multiplication** and denoted accordingly, such that

- R is an abelian group under addition,
- R is a semigroup under multiplication,
- multiplication distributes over addition.

The complete list of axioms is as follows:
(A0) for all $x, y \in R$, $x + y$ is an element of R;
(A1) $(x + y) + z = x + (y + z)$ for all $x, y, z \in R$;
(A2) there exists an element, denoted 0, in R such that $x + 0 = 0 + x = x$ for all $x \in R$;
(A3) for every $x \in R$ there exists an element, denoted $-x$, in R such that $x + (-x) = (-x) + x = 0$;
(A4) $x + y = y + x$ for all $x, y \in R$;
(M0) for all $x, y \in R$, xy is an element of R;
(M1) $(xy)z = x(yz)$ for all $x, y, z \in R$;
(D) $x(y+z) = xy+xz$ and $(y+z)x = yx+zx$ for all $x, y, z \in R$.

From rings to fields

A ring R is called a **domain** if it has no divisors of zero, that is, $xy = 0$ implies $x = 0$ or $y = 0$.

A ring R is called a **ring with unity** if there exists an identity element for multiplication (called the **unity** and denoted 1).

A **division ring** (or **skew field**) is a nontrivial ring with unity in which every nonzero element has a multiplicative inverse.

A ring R is called **commutative** if the multiplication is commutative.

An **integral domain** is a nontrivial commutative ring with unity and no divisors of zero.

A **field** is an integral domain in which every nonzero element has a multiplicative inverse (equivalently, a commutative division ring).

$$\begin{array}{l} \text{rings} \supset \text{domains} \supset \text{integral domains} \supset \text{fields} \\ \qquad\qquad\qquad\qquad \supset \text{division rings} \supset \end{array}$$

Ring of functions

Let R be a ring and S be a nonempty set. Denote by $\mathcal{F}(S,R)$ the set of all functions $f : S \to R$. Given $f, g \in \mathcal{F}(S,R)$, we let $(f+g)(x) = f(x) + g(x)$ and $(fg)(x) = f(x)g(x)$ for all $x \in S$. That is, to add (or multiply) functions, we add (or multiply) their values at every point. Then $\mathcal{F}(S,R)$ is a ring.

The ring $\mathcal{F}(S,R)$ inherits many properties from the ring R, with one important exception. If R is a nontrivial ring and S has more than one element, then the ring $\mathcal{F}(S,R)$ has divisors of zero. Indeed, take any point $x_0 \in S$, any nonzero element $r \in R$, and let

$$f_1(x) = \begin{cases} r & \text{if } x = x_0, \\ 0 & \text{if } x \in S \setminus \{x_0\}; \end{cases} \quad f_2(x) = \begin{cases} 0 & \text{if } x = x_0, \\ r & \text{if } x \in S \setminus \{x_0\}. \end{cases}$$

Then the functions f_1 and f_2 are nonzero elements of the ring $\mathcal{F}(S,R)$ while $f_1 f_2 = 0$.

Ring of matrices

Let R be a ring. For any integers $m, n > 0$, denote by $\mathcal{M}_{m,n}(R)$ the set of all $m \times n$ matrices with entries from R. Given two matrices $A = (a_{ij})$ and $B = (b_{ij})$ in $\mathcal{M}_{m,n}(R)$, we let $A + B = (c_{ij})$ and $A - B = (d_{ij})$, where $c_{ij} = a_{ij} + b_{ij}$ and $d_{ij} = a_{ij} - b_{ij}$, $1 \leq i \leq m$, $1 \leq j \leq n$. Given matrices $A = (a_{ij}) \in \mathcal{M}_{m,n}(R)$ and $B = (b_{ij}) \in \mathcal{M}_{n,p}(R)$, we let $AB = (c_{ij})$, where $c_{ij} = a_{i1}b_{1j} + a_{i2}b_{2j} + \cdots + a_{in}b_{nj}$, $1 \leq i \leq m$, $1 \leq j \leq p$.

Matrix multiplication is associative. Indeed, let $A = (a_{ij}) \in \mathcal{M}_{m,n}(R)$, $B = (b_{jk}) \in \mathcal{M}_{n,p}(R)$ and $C = (c_{k\ell}) \in \mathcal{M}_{p,q}(R)$. Then $(AB)C = (d_{i\ell})$ and $A(BC) = (d'_{i\ell})$ are matrices in $\mathcal{M}_{n,q}(R)$. Using distributive laws in R, we obtain that

$$d_{i\ell} = \sum_{k=1}^{p} \sum_{j=1}^{n} (a_{ij}b_{jk})c_{k\ell}, \quad d'_{i\ell} = \sum_{j=1}^{n} \sum_{k=1}^{p} a_{ij}(b_{jk}c_{k\ell}).$$

Hence $(AB)C = A(BC)$ since R is a ring.

As a consequence, square matrices in $\mathcal{M}_{n,n}(R)$ form a ring.

Direct product of rings

Suppose $R_1, R_2, \ldots, R_n$ are rings. We define addition and multiplication on the Cartesian product $R_1 \times R_2 \times \cdots \times R_n$ by

$$(r_1, r_2, \ldots, r_n) + (r_1', r_2', \ldots, r_n') = (r_1 + r_1', r_2 + r_2', \ldots, r_n + r_n'),$$
$$(r_1, r_2, \ldots, r_n)(r_1', r_2', \ldots, r_n') = (r_1 r_1', r_2 r_2', \ldots, r_n r_n')$$

for all $r_i, r_i' \in R_i$, $1 \leq i \leq n$.

Then $R_1 \times R_2 \times \cdots \times R_n$ is a ring called the **direct product** of rings $R_1, R_2, \ldots, R_n$.

The ring $R_1 \times R_2 \times \cdots \times R_n$ is commutative if each of the rings $R_1, R_2, \ldots, R_n$ is commutative. It is a ring with unity if each of the rings $R_1, R_2, \ldots, R_n$ has the unity.

If at least two of the rings $R_1, R_2, \ldots, R_n$ are nontrivial, then the direct product $R_1 \times R_2 \times \cdots \times R_n$ admits divisors of zero.

Complex numbers

$\mathbb{C}$: complex numbers.

Complex number: $\boxed{z = x + iy,}$

where $x, y \in \mathbb{R}$ and $i^2 = -1$.

$i = \sqrt{-1}$: imaginary unit

Alternative notation: $z = x + yi$.

$x =$ real part of z,
$iy =$ imaginary part of z

$y = 0 \implies z = x$ (real number)
$x = 0 \implies z = iy$ (purely imaginary number)

We add, subtract, and multiply complex numbers as polynomials in i (but keep in mind that $i^2 = -1$).

If $z_1 = x_1 + iy_1$ and $z_2 = x_2 + iy_2$, then

$$z_1 + z_2 = (x_1 + x_2) + i(y_1 + y_2),$$
$$z_1 - z_2 = (x_1 - x_2) + i(y_1 - y_2),$$
$$z_1 z_2 = (x_1 x_2 - y_1 y_2) + i(x_1 y_2 + x_2 y_1).$$

Given $z = x + iy$, the **complex conjugate** of z is $\bar{z} = x - iy$. The **modulus** of z is $|z| = \sqrt{x^2 + y^2}$.

$z\bar{z} = (x + iy)(x - iy) = x^2 - (iy)^2 = x^2 + y^2 = |z|^2$.

$$z^{-1} = \frac{\bar{z}}{|z|^2}, \qquad (x + iy)^{-1} = \frac{x - iy}{x^2 + y^2}.$$

Complex exponentials

Definition. For any $z \in \mathbb{C}$ let

$$e^z = 1 + z + \frac{z^2}{2!} + \cdots + \frac{z^n}{n!} + \cdots$$

Remark. A sequence of complex numbers $z_1 = x_1 + iy_1,\ z_2 = x_2 + iy_2, \ldots$ converges to $z = x + iy$ if $x_n \to x$ and $y_n \to y$ as $n \to \infty$.

Theorem 1 If $z = x + iy,\ x, y \in \mathbb{R},$ then

$$e^z = e^x(\cos y + i \sin y).$$

In particular, $e^{i\phi} = \cos\phi + i\sin\phi,\ \phi \in \mathbb{R}.$

Theorem 2 $e^{z+w} = e^z \cdot e^w$ for all $z, w \in \mathbb{C}.$

Proposition $e^{i\phi} = \cos\phi + i\sin\phi$ for all $\phi \in \mathbb{R}$.

Proof: $e^{i\phi} = 1 + i\phi + \dfrac{(i\phi)^2}{2!} + \cdots + \dfrac{(i\phi)^n}{n!} + \cdots$

The sequence $1, i, i^2, i^3, \ldots, i^n, \ldots$ is periodic:
$\underbrace{1, i, -1, -i}, \underbrace{1, i, -1, -i}, \ldots$

It follows that

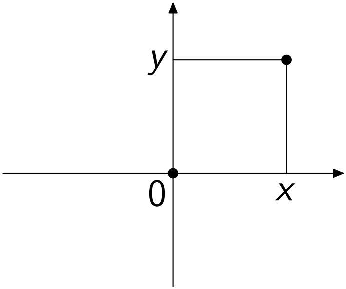
$$e^{i\phi} = 1 - \frac{\phi^2}{2!} + \frac{\phi^4}{4!} - \cdots + (-1)^k \frac{\phi^{2k}}{(2k)!} + \cdots$$

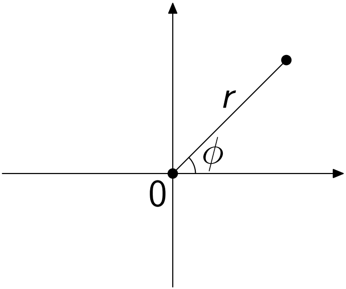
$$+ \ i\left(\phi - \frac{\phi^3}{3!} + \frac{\phi^5}{5!} - \cdots + (-1)^k \frac{\phi^{2k+1}}{(2k+1)!} + \cdots\right)$$

$$= \cos\phi + i\sin\phi.$$

Geometric representation

Any complex number $z = x + iy$ is represented by the vector/point $(x, y) \in \mathbb{R}^2$.





$$x = r\cos\phi,\ \ y = r\sin\phi \implies z = r(\cos\phi + i\sin\phi) = re^{i\phi}$$

If $z_1 = r_1 e^{i\phi_1}$ and $z_2 = r_2 e^{i\phi_2}$, then
$z_1 z_2 = r_1 r_2 e^{i(\phi_1+\phi_2)}$, $z_1/z_2 = (r_1/r_2)e^{i(\phi_1-\phi_2)}$.

From a ring to a field

Question 1. When a ring R can be extended to a field?

An obvious necessary condition is commutativity. Another necessary condition is absence of zero divisors (which is equivalent to cancellation laws).

Proposition If an element of a ring with unity has a multiplicative inverse, then it is not a divisor of zero.

Question 2. When a semigroup S can be extended to a group?

Theorem If S is a commutative semigroup with cancellation, then it can be extended to an abelian group G. Moreover, if $G = \langle S \rangle$, then any element of G is of the form $b^{-1}a$, where $a, b \in S$. Moreover, if $G = \langle S \rangle$, then the group G is unique up to isomorphism.

Theorem Any finite semigroup with cancellation is actually a group.

Lemma If S is a finite semigroup with cancellation, then for any $s \in S$ there exists an integer $k \geq 2$ such that $s^k = s$.

Proof: Since S is finite, the sequence $s, s^2, s^3, \dots$ contains repetitions, i.e., $s^k = s^m$ for some $k > m \geq 1$. If $m = 1$ then we are done. If $m > 1$ then $s^{m-1}s^{k-m+1} = s^{m-1}s$, which implies $s^{k-m+1} = s$.

Proof of the theorem: Take any $s \in S$. By Lemma, we have $s^k = s$ for some $k \geq 2$. Then $e = s^{k-1}$ is the identity element. Indeed, for any $g \in S$ we have $s^k g = sg$ or, equivalently, $s(eg) = sg$. After cancellation, $eg = g$. Similarly, $ge = g$ for all $g \in S$. Finally, for any $g \in S$ there is $n \geq 2$ such that $g^n = g = ge$. Then $g^{n-1} = e$, which implies that $g^{n-2} = g^{-1}$.

Field of quotients

Theorem A ring R with unity can be extended to a field if and only if it is an integral domain.

If R is an integral domain, then there is a (smallest) field F containing R called the **quotient field** of R (or the **field of quotients**). Any element of F is of the form $b^{-1}a$, where $a, b \in R$. The field F is unique up to isomorphism.

Examples. • The quotient field of $\mathbb{Z}$ is $\mathbb{Q}$.
• The quotient field of $\mathbb{R}[X]$ is $\mathbb{R}(X)$.
• The quotient field of $\mathbb{Z}[\sqrt{2}] = \{m + n\sqrt{2} \mid m, n \in \mathbb{Z}\}$ is $\mathbb{Q}[\sqrt{2}] = \{p + q\sqrt{2} \mid p, q \in \mathbb{Q}\}$.