Number Systems

KYB

1 Properties of the number systems

Summary

- $\mathbb{N}$: Well-ordering principle.
- $\mathbb{Z}$: $ax + by = \gcd(a, b)$ for some $x, y \in \mathbb{Z}$.
- $\mathbb{Q}$: For any $p, q \in \mathbb{R}$, $\exists r \in \mathbb{Q}$ s.t. $p < r < q$.
- $\mathbb{R}$: Every nonempty bounded above set has the least upper bound.
- $\mathbb{C}$: Every polynomial has a root in $\mathbb{C}$.

1.1 An ordered sets

1.1.1 (Partial) Ordered Sets

Definition 1.1.1 (Relation)**.** Suppose X and Y are sets.

- A relation R between X and Y is a subset of $X \times Y$.
- If (x, y) is an element of R, write xRy.

If $X = Y$, we say R is a relation on R.

Example 1.1.2.

- For $\mathbb{R}$, $=$, $\neq$, $<$, $>$, $\leq$, $\geq$, $\cdots$ are relation on $\mathbb{R}$.
- For any set X, $\subset$ is a relation on $\mathcal{P}(X)$.
- Suppose V is a vector space over F and H be a subspace of V. $x \sim y$ iff $x - y \in H$ is a relation on V.

Definition 1.1.3 (Order)**.** An partial order $<$ on a set X (denote $(X, <)$) is a relation satisfying

- $x \not< x$ for any $x \in X$;
- if $x < y$ and $y < z$, then $x < z$.

If $(X, <)$ satisfies one more condition

- $x < y$, or $x = y$, ro $x > y$ for all $x, y \in X$,

$(X, <)$ is called an ordered set.

Definition 1.1.4. Suppose $(X, <)$ is a partially ordered set and S is a nonempty subset of X and $a \in X$.

- a is a *maximal* element of S if $a \in S$ and for all $x \in S$ $a \not< x$.
- a is a *minimal* element of S if $a \in S$ and for all $x \in S$ $x \not< a$.
- a is the *greatest* element of S if $a \in S$ and for all $x \in S$ $x \leq a$.
- a is the *least* element of S if $a \in S$ and for all $x \in S$ $a \leq x$.
- a is an *upper* bound of S if for all $x \in S$ $x \leq a$.
- a is an *lower* bound of S if for all $x \in S$ $a \leq x$.
- a is the *supremum* of S if a is the least upper bound.
- a is the *infimum* of S if a is the greatest lower bound.

1.2 The natural numbers

Remark 1.2.1 (Natural numbers)**.** $\mathbb{N}$ satisfies

- $1 \in \mathbb{N}$ is the minimal (least) element of $\mathbb{N}$.
- If $n \in \mathbb{N}$, then $n+1 \in \mathbb{N}$.
- There is no $n \in \mathbb{N}$ such that $n+1=1$.
- For $m, n \in \mathbb{N}$, $m = n$ or $m > n$ or $m < n$.
- $\cdots$.

Proposition 1.2.2 (Well-ordering principle)**.** Any nonempty subset S of $\mathbb{N}$ has a minimal element.

Proof. Suppose S is finite. Then we can find a minimal element.

Suppose S is infinite. Choose $n \in S$ and consider $A = S \cap \{1, \cdots, n\}$. We can find a minimal element $m \in A$ and m is also minimal element of S. □

Remark 1.2.3. If we put finitely many real numbers into $\mathbb{N}$, WoP still holds. For example, $\mathbb{N}_0 = \{0\} \cup \mathbb{N}$ has WoP.

Example 1.2.4 (Application of WoP, mathematical induction)**.** For each $n \in \mathbb{N}$, let $P(n)$ is a statement. Suppose

1. $P(1)$ is true.
2. If $P(n)$ is true, then $P(n+1)$ is true.

Then for all $n \in \mathbb{N}$, $P(n)$ is true.

Proof. Let $S = \{n \in \mathbb{N} \mid P(n) \text{ is false }\}$. Sinse $P(1)$ is true, $\mathbb{N} - S$ is nonempty. If S is empty, MI holds.

Suppose not. Choose a minimal element m of S. Then $P(m-1)$ is true and $P(m)$ is false. By condition 2, $P(m)$ must be true. (contradiction) □

Remark 1.2.5 (Unboundness of natural numbers)**.** $\mathbb{N}$ has no upper bound.

Proof. Suppose not and let M be an upper bound of $\mathbb{N}$. Then for all $n \in \mathbb{N}$, $n \leq M$. Since $M+1 \in \mathbb{N}$, $M+1 \leq M$. But this cannot happen. □

1.3 The integer numbers

Definition 1.3.1 (Divisor)**.** Let $m, n \in \mathbb{Z}$. Suppose $n \neq 0$. If there is $r \in \mathbb{Z}$ such that $m = nr$,

- n divides m,
- m is divided by n.

Write $n|m$, and n is called a diviosr of m and m is called a multiple of n.

Definition 1.3.2 (The Greatest Common divisor)**.** Let $m, n, d \in \mathbb{Z}$. Suppose one of m and n is nonzero.

(1) $d|m$ and $d|n$.

(2) If $c|m$ and $c|n$, then $c \leq d$.

If d satisfies (1), d is called a common divisor. If d also satisfies (2), d is called the greatest common divisor.

If d is a common diviosr, so is $-d$. So the GCD is positive.

Proposition 1.3.3 (The division algorithm)**.** Let $m, n \in \mathbb{Z}$ be nonzero elements with $n > 0$. Then there are unique $q, r \in \mathbb{Z}$ such that

- $0 \leq r < n$;
- $m = qn + r$.

Proof. Let $S = \{m - an \mid |a \in \mathbb{Z}, m - an \geq 0\}$. Since $m + |m|n \geq 0$, S is nonempty. Choose minimal element r of S. Then $m - qn = r$ for some $q \in \mathbb{Z}$. If $r \geq n$, then $m = qn + r = (q+1)n + (r-n)$ implies $r > r - n \in S$. But r is the minimal element of S. So $0 \leq r < n$. Similar way we can show that r is unique. □

Remark 1.3.4. If $n|m$, then $m = qn$. So $m|n$ and $n|m$ implies $m = \pm n$. Hence the GCD (the LCM) makes sense.

Theorem 1.3.5 (Linear combination of GCD)**.** If $m, n \in \mathbb{N}$ are both nonzero, then there is $a, b \in \mathbb{Z}$ such that

$$am + bn = \gcd(m, n).$$

Proof. Let $S = \{xm + yn > 0 \mid x, y \in \mathbb{Z}\}$. Clearly S is nonempty. Let d be the minimal element of S with $am + bn = d$.

Taking the division algorithm on m, then $m = qd + r$.

$$r = m - qd = m - q(am + bn) = (1 - qa)m + (-qb)n$$

So either $r = 0$ or $r \geq d$. But $r < d$ implies $r = 0$, or $m = qd$. Similarly $d|n$. Thus d is CD of m and n.

If c is another CD of m and n, we get $c|am + bn$. Thus $c|d$. □

Proposition 1.3.6 (The Euclidean algorithm)**.** Suppose $m \geq n > 0$. Apply the division algorithm to m and n, and get $m = q_1 n + r_1$ where $0 \leq n$. If $r_1 = 0$, n is a diviosr of m. If not, apply one more to n and r_1, $n = r_1 q_2 + r_2$ where $0 \leq r_2 \leq r_1$. Repeat this untill $0 < r_n < r_{n-1}$ and $r_{n+1} = 0$. Then $r_n = gcd(m, n)$.

Remark 1.3.7.

$$\begin{aligned} m &= q_1 n + r_1 \quad &, 0 < r_1 < n \\ n &= q_2 r_1 + r_2 \quad &, 0 < r_2 < r_1 \\ r_1 &= q_3 r_2 + r_3 \quad &, 0 < r_3 < r_2 \\ &\vdots \quad \vdots \\ r_{n-1} &= q_{n+1} r_n. \end{aligned}$$

Proof. Since $r_n < r_{n-1} < \cdots < n$, we can find such r_n. So it suffices to show that $r_n = \gcd(m,n)$.

Claim) For $a \geq b > 0$, if $a = qb + r$, then $\gcd(a,b) = \gcd(b,r)$.

Clearly $\gcd(b,r)|a$. So $\gcd(b,r)|\gcd(a,b)$. Conversely, $a - qb = r$ implies $\gcd(a,b)|r$. So $\gcd(a,b)|\gcd(b,r)$.

By the claim,

$$\gcd(m,n) = \gcd(n,r_1) = \gcd(r_1,r_2) = \cdots = \gcd(r_{n-1},r_n) = r_n.$$

$\square$

Remark 1.3.8. Using the Euclidean algorithm, we can find $a, b \in \mathbb{Z}$ so that $am + bn = \gcd(m,n)$.

Example 1.3.9. Ex 2.8.12) $a = 257$, $b = 114$.

$$\begin{aligned} 257 &= 2 \times 114 + 29 \\ 114 &= 3 \times 29 + 27 \\ 29 &= 1 \times 27 + 2 \\ 27 &= 13 \times 2 + 1 \\ 2 &= 2 \times 1. \end{aligned}$$

Note that 257 is a prime number. So $\gcd(257, 114) = 1$.

$$\begin{aligned} 1 &= 27 - 13 \times 2 \\ &= 27 - 13 \times (29 - 1 \times 27) = -13 \times 29 + 14 \times 27 \\ &= -13 \times 29 + 14 \times (114 - 3 \times 29) = 14 \times 114 - 55 \times 29 \\ &= 14 \times 114 - 55 \times (257 - 2 \times 114) = -55 \times 257 + 124 \times 114. \end{aligned}$$

Thus $114^{-1} \equiv 124 \mod (257)$.

1.4 The rational numbers

Remark 1.4.1 (Rationals).

- For any $q \in \mathbb{Q}$, there is $m, n \in \mathbb{Z}$ such that $n \neq 0$ and $q = \frac{m}{n}$. By choosing m, n such that $n \in \mathbb{N}$ and $\gcd(m,n) = 1$, every q has an unique representation $\frac{m}{n}$.

- For any $p < q$ in $\mathbb{R}$, there is $r \in \mathbb{Q}$ so that

$$p < r < q.$$

  In particular, for any $q > 0$, there is $n \in \mathbb{N}$ such that

$$0 < \frac{1}{n} < q.$$

- $(\mathbb{Q}, +, \cdot)$ forms a field. Suppose $S \subset \mathbb{Q}$ is a subfield. Then $S = \mathbb{Q}$. In this sense, we call $\mathbb{Q}$ is a prime field.

  In the same way, if F is a field with characteristic p, then $\mathbb{Z}/p\mathbb{Z}$ is a prime filed of F,i.e. $\mathbb{Z}/p\mathbb{Z} \subset F$ and if $S \subset \mathbb{Z}/p\mathbb{Z}$ is a subfield then $S = \mathbb{Z}/p\mathbb{Z}$.

Definition 1.4.2 (The supremum axiom)**.** Let X be an ordered set. X has the supremum axiom (or the least upper bound property) if every nonempty and bounded above subset has the least upper bound.

Example 1.4.3 (The rational does not has the LUBP)**.** $\mathbb{Q}$ does not have the LUBP.

Consider $S = \{q \in \mathbb{Q} \mid q^2 < 2\}$. S has an upper bound 2. We know that $S = (-\sqrt{2}, \sqrt{2}) \cap \mathbb{Q}$. So if $0 < q < \sqrt{2}$, there is $r \in S$ such that $q < r < 2$, or $q^2 < r^2 < 2$. Hence S has no least upper bound in $\mathbb{Q}$.

1.5 The real numbers

Theorem 1.5.1 (The reals has the LUBP)**.** $\mathbb{R}$ has the least upper bound property by the definition.

(See [completion of metric space] or [dedekind cut])

Exercise 1.5.2. $A = \{\frac{1}{n} \mid n \in \mathbb{N}\}$. $\sup(A) = 1$, $\inf(A) = 0$.

Exercise 1.5.3. $B = \{x \mid -1 < x \leq 2, x \in \mathbb{R}\}$. $\sup(A) = 2$, $\inf(A) = -1$.

Definition 1.5.4. A nonempty subset $A \subset \mathbb{R}$ is called a bounded set if $\exists M > 0$ such that

$$|x| < M, \forall x \in A.$$

Exercise 1.5.5. Suppoe A is a nonempty bounded subset of $\mathbb{R}$. Let α be a lower bound and β be a upper bound of A. Prove that $\alpha \leq \beta$.

Remark 1.5.6. If we allow $\sup(A) = \infty$ and $\inf(A) = -\infty$, every subset has sup and inf.

Exercise 1.5.7. If $A \subset B$, then $\inf(B) \leq \inf(A) \leq \sup(A) \leq \sup(B)$.

Exercise 1.5.8. $\sup(A \cup B) = \max\{\sup(A), \sup(B)\}$.

Exercise 1.5.9. $\inf(A) = -\sup(-A)$.

Exercise 1.5.10. $\sup(A + B) = \sup(A) + \sup(B)$.