

VE203 DISCRETE MATHEMATICS RECITATION CLASS

 $\begin{array}{c} {\rm Hamster} \\ {\rm April} \ 12, \ 2022 \end{array}$

Contents

1	Sets	8																				3
	1.1	Exercise																				
	1.2	Solution																				
2	Log	8														4						
	2.1	Exercise																				4
	2.2	Solution																				4
3	Relations															Ę						
	3.1	Exericse																				Ę
	3.2	Solution																				6
4	Equ	Equinumerosity													7							
	$4.\overline{1}$	Exercise																				7
	4.2	Solution																				
5	Par	tial Orde	er																			g
	5.1	Exercise																				Ć
	5.2	Solution																				10
6	Pige	Pigeonhole Principle 11																				
	6.1	Exercise																				11
	6.2	Solution																				11
7	Euclidean Algorithm 1													11								
	7.1	Exericse	_																			11
	7.2	Solution																				
8	Group Theory														13							
	8.1	Exercise																				13
	8.2	Solution																				
9	Gra	1 0													16							
		Exercise																				16
		Solution																				

1 Sets

1.1 Exercise

Let A, B, M be three sets and $A, B \subset M$. Show that

1.
$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$

2.
$$A - (B \cup C) = (A - B) \cap (A - C)$$

3.
$$(A - B) \cup (B - A) = (A \cup B) - (A \cap B)$$

1.2 Solution

1. Let $x \in A \cup (B \cap C)$.

$$x \in A \cup (B \cap C) \Leftrightarrow x \in A \lor x \in B \cap C$$

$$\Leftrightarrow x \in A \lor (x \in B \land x \in C)$$

$$\Leftrightarrow (x \in A \lor x \in B) \land (x \in A \lor x \in C)$$

$$\Leftrightarrow (x \in A \cup B) \land (x \in A \cup C)$$

$$\Leftrightarrow x \in (A \cup B) \cap (A \cup C)$$

Therefore, $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

2. Let $x \in A - (B \cup C)$.

$$x \in A - (B \cup C) \Leftrightarrow x \in A \land x \notin B \cup C$$

$$\Leftrightarrow x \in A \land (x \notin B \land x \notin C)$$

$$\Leftrightarrow x \in A \land x \notin B \land x \notin C$$

$$\Leftrightarrow (x \in A \land x \notin B) \land (x \in A \land x \notin C)$$

$$\Leftrightarrow x \in A - B \land x \in A - C$$

$$\Leftrightarrow x \in (A - B) \cap (A - C)$$

Therefore, $A - (B \cup C) = (A - B) \cap (A - C)$.

3. Let E be the universal set. Denote $A^c = E - A$.

$$(A - B) \cup (B - A) = (A \cap B^c) \cup (B \cap A^c)$$

$$= ((A \cap B^c) \cup B) \cap ((A \cap B^c) \cup A^c)$$

$$= ((A \cup B) \cap (B^c \cup B)) \cap ((A \cup A^c) \cap (B^c \cup A^c))$$

$$= (A \cup B) \cap E \cap E \cap (B^c \cup A^c)$$

$$= (A \cup B) \cap (B^c \cup A^c)$$

$$= (A \cup B) \cap (B \cap A)^c$$

$$= (A \cup B) - (A \cap B)$$

This completes the proof.

2 Logic

2.1 Exercise

Prove that

1.
$$P \Rightarrow (Q \Rightarrow R) \equiv (P \land Q) \Rightarrow R$$

2.
$$((P \lor Q) \land \neg Q) \Rightarrow P$$
 is a tautology

3.
$$(A \Rightarrow (B \Rightarrow C)) \Rightarrow (B \Rightarrow (A \Rightarrow C))$$
 is a tautology

2.2 Solution

1.

$$P \Rightarrow (Q \Rightarrow R) \equiv P \Rightarrow (\neg Q \lor R)$$
$$\equiv P \lor (\neg Q \lor R)$$
$$\equiv (\neg P \lor \neg Q) \lor R$$
$$\equiv \neg (P \land Q) \lor R$$
$$\equiv (P \land Q) \Rightarrow R$$

2.

$$\begin{split} ((P \lor Q) \land \neg Q) \Rightarrow P &\equiv ((P \land \neg Q) \lor (Q \land \neg Q)) \Rightarrow P \\ &\equiv (P \land \neg Q) \Rightarrow P \\ &\equiv \neg (P \land \neg Q) \lor P \\ &\equiv (\neg P \lor Q) \lor P \\ &\equiv (\neg P \lor P) \lor Q \\ &\equiv T \end{split}$$

3.

$$\begin{split} (A \Rightarrow (B \Rightarrow C)) \Rightarrow (B \Rightarrow (A \Rightarrow C)) &\equiv (\neg A \lor (\neg B \lor C)) \Rightarrow (\neg B \lor (\neg A \lor C)) \\ &\equiv (\neg A \lor \neg B \lor C) \Rightarrow (\neg A \lor \neg B \lor C) \\ &\equiv T \end{split}$$

3 Relations

3.1 Exericse

1. Let $A: \mathbb{R}^3 \to \mathbb{R}^3$ be given by

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 2 \\ 1 & 1 & 1 \end{pmatrix}$$

Let

$$U = \operatorname{span} \left\{ \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} \right\}$$

Question:

- What's the restriction of A to U?
- What's the image of the restriction?
- What's the inverse of the restriction?

(Take from vv286 lecture slides)

2. Recall that $\mathbb Z$ denotes the set of integers, $\mathbb Z^+$ the set of positive integers, and $\mathbb Q$ the set of rational numbers. Define a function:

$$f: \mathbb{Z} \times \mathbb{Z}^+ \to \mathbb{Q}, \qquad f(p,q) = \frac{p}{q}.$$

- 1. Is f an injection? Why?
- 2. Is f an surjection? Why?
- 3. Is f an bijection? Why?
- 3. Recall that $\mathbb R$ denotes the set of real numbers, while $\mathbb Z$ denotes the set of integers. Define a relation \sim on $\mathbb R$ by

$$x \sim y \Leftrightarrow x - y \in \mathbb{Z}$$

for any $x, y \in \mathbb{R}$. Prove that \sim is an equivalence relation.

3.2 Solution

1.

• restriction:

$$A \mid_{U}: U \to \mathbb{R}^{3}, \qquad Au = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 2 \\ 1 & 1 & 1 \end{pmatrix}$$

where the only visible change is the domain to which we apply A.

• range: Since

$$Au = \begin{pmatrix} 1\\1\\0 \end{pmatrix} = \begin{pmatrix} 3\\3\\2 \end{pmatrix}$$

2.

- 1. No. There are many different choices of $(p,q) \in \mathbb{Z} \times \mathbb{Z}^+$ which are assigned the same value by f. For example, f(1,1) = 1 = f(2,2).
- 2. Yes. Every rational number is, by definition, a quotient of integers, and we can always arrange for the denominator to be positive.

3. No. To be a bijection, a function must be both an injection and a surjection. Since f is not an injection by part 1, it is not a bijection, either.

3.

Reflexive: For any $x \in \mathbb{R}, x - x = 0 \in \mathbb{Z}$, and hence $x \sim x$. Therefore \sim is reflexive.

Symmetric: Suppose that $x, y \in \mathbb{R}$, and that $x \sim y$. Then x - y = n for some integer $n \in \mathbb{Z}$. Hence $y - x = -(x - y) = -n \in \mathbb{Z}$, so that $y \sim x$. This shows that $x \sim y \Rightarrow y \sim x$. Therefore \sim is symmetric.

Transitive: Suppose that $x, y, z \in \mathbb{R}$, that $x \sim y$, and that $y \sim z$. Then $x \sim y = m$ for some integer n, and $y \sim z = n$ for some integer n. Hence $x \sim z = (x - y) + (y - z) = m + n \in \mathbb{Z}$ so that $x \sim z$. This shows that $x \sim y$ and $y \sim z \Rightarrow x \sim z$. Therefore \sim is transitive.

We have now shown that \sim is reflexive, symmetric, and transitive. Therefore \sim is an equivalence relation.

4 Equinumerosity

4.1 Exercise

1. The mapping function $f: \mathbb{N} \to \mathcal{P}(\mathbb{N})$ is defined by

$$f(n) = \mathbb{N} \setminus \left\{ n^2 - (2m - 1) n \right\},\,$$

where $n, m \in \mathbb{N}$. Determine the set $B = \{x \in A \mid x \notin f(x)\}$.

- 2. Prove that the set of all sets does not exist.
- 3. Prove that
- 1. $\mathbb{Z} \approx \mathbb{N}$
- 2. $\mathbb{N} \times \mathbb{N} \approx \mathbb{N}$
- $3. (0,1) \approx \mathbb{R}$
- 4. $[0,1] \approx (0,1)$

4.2 Solution

1. The condition $n \notin f(n)$ is met if n satisfies the equation

$$n = n^2 - (2m - 1) n.$$

Solving it, we obtain:

$$n = n^2 - (2m - 1) n \implies n = n^2 - 2mn + n \implies n(n - 2m) = 0.$$

Since n > 0, the solution is given by n = 2m, where $m \in \mathbb{N}$. Thus, the set B contains all even natural numbers:

$$B = \{x \in A \mid x \notin f(x)\} = \{n \mid n = 2m, m \in \mathbb{N}\}.$$

- 2. Assume, by contradiction, that the set of all sets exists and is denoted as S. Then its power set $\mathcal{P}(S)$ exists as well.
 - $\mathcal{P}(S)$ is a set. Therefore, $\mathcal{P}(S)$ is contained in S. we get $|\mathcal{P}(S)| \leq |S|$.
 - From the other side, according to Cantor's theorem, we know that $|S| < |\mathcal{P}(S)|$.
 - We have a contradiction. This means that the set of all sets does not exist.
 - →The reason why *equinumerous* is NOT an equivalence relation: it concerns the **ALL** sets (the domain and range of this relation does not exist).

3.

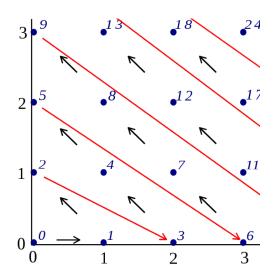
1. Let $f: \mathbb{Z} \to \mathbb{N}$,

$$f(n) = \begin{cases} 0, & n = 0 \\ 2n, & n > 0 \\ 2|n| - 1, & n < 0 \end{cases}$$

It's easy to prove that f is bijective.

2. Cantor's pairing function $\pi: \mathbb{N} \times \mathbb{N} \to \mathbb{N}$:

$$\pi(x,y) = \frac{1}{2}(x+y)(x+y+1) + y$$



3. Let $f:(0,1)\to\mathbb{R}$,

$$f(x) = \tan\left[\pi\left(x - \frac{1}{2}\right)\right]$$

4. Let $f:[0,1] \to (0,1)$,

$$f(x) = \begin{cases} \frac{1}{2}, & x = 0\\ \frac{1}{n+2}, & x = 1/n, n \in \mathbb{N} \setminus \{0\}\\ x, & \text{otherwise} \end{cases}$$

5 Partial Order

5.1 Exercise

- 1. A relation R is defined on ordered pairs of integers as follows: (x,y)R(u,v) if x < u and y > v. Then R is:
- (A) Neither a partial order nor an equivalence relation
- (B) A partial order but not a total order
- (C) A total order

(D) An equivalence relation

2. Consider the set $S = \{a, b, c, d\}$. Consider the following 4 partitions $\pi_1, \pi_2, \pi_3, \pi_4$ on $S : \pi_1 = \{\overline{abcd}\}, \pi_2 = \{\overline{ab}, \overline{cd}\}, \pi_3 = \{\overline{abc}, \overline{d}\}, \pi_4 = \{\overline{a}, \overline{b}, \overline{c}, \overline{d}\}$. Let p be the partial order on the set of partitions $S' = \{\pi_1, \pi_2, \pi_3, \pi_4\}$ defined as follows: $\pi_i p \pi_j$ if and only if π_i refines π_j (assume the refinement relation is strict partial order here). Find the poset diagram for (S', p).

5.2 Solution

1.

2.

As given in question, a relation R is defined on ordered pairs of integers as follows:

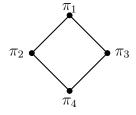
$$(x,y)R(u,v)$$
 if $x < u$ and $y > v$,

reflexive property is not satisfied here, because there is > or < relationship between (x, y) pair set and (u, v) pair set.

Other way, if there would have been $x \leq u$ and $y \geq v$ (or x = u and y = v) kind of relation among elements of sets then reflexive property could have been satisfied.

Since reflexive property in not satisfied here, so given relation can not be equivalence, partial order total order relation.

So, option (A) is correct.



A partition is said to refine another partition if it splits the sets in the second partition to a larger number of sets.

Therefore, the partial order contains the following ordered pairs:

$$\{(\pi_4, \pi_1), (\pi_4, \pi_2), (\pi_4, \pi_3), (\pi_3, \pi_1), (\pi_2, \pi_1)\}$$

Pigeonhole Principle 6

6.1Exercise

1. Consider a sequence $\{\sqrt{3}, 2\sqrt{3}, 3\sqrt{3}, \cdots\}$ Prove that there are infinite number of terms have a mantissa of less than 0.01.

6.2Solution

Proof. We represent $\{x\}$ as the decimal part of x (e.g., $\{\sqrt{3}\}$) = 0.732...). - 100 holes: [0, 0.01), [0.01, 0.02), ..., [0.99, 1). - 101 pigeons: $\{\sqrt{3}\}, \{2\sqrt{3}\}, \dots, \{101\sqrt{3}\}.$ $\exists m, n \in \{1, 2, \dots, 101\}, m < n, s.t. \{m\sqrt{3}\}, \{n\sqrt{3}\}$ belong to the same hole. Then, we have

- Either $\{(n-m)\sqrt{3}\}\in[0,0.01),$
- or $\{(n-m)\sqrt{3}\}\in(0.99,1)$.

If $\{(n-m)\sqrt{3}\} \in [0, 0.01)$, we are done. If $\{(n-m)\sqrt{3}\}\in(0.99,1)$, represent $(n-m)\sqrt{3}=\lceil(n-m)\sqrt{3}\rceil-t,t\in$ (0, 0.01). $\lfloor \frac{1}{t} \rfloor \cdot (n-m)\sqrt{3} = \lfloor \frac{1}{t} \rfloor \cdot \lceil (n-m)\sqrt{3} \rceil - \lfloor \frac{1}{t} \rfloor \cdot t$ $\Rightarrow \left\{ \left\lfloor \frac{1}{t} \right\rfloor \cdot (n-m)\sqrt{3} \right\} = 1 - \left\lfloor \frac{1}{t} \right\rfloor \cdot t. \text{ Denote it as } A.$ $A > 1 - \frac{1}{t} \cdot t = 0;$ $A < 1 - \left(\frac{1}{t} - 1 \right) \cdot t = t < 0.01.$ Therefore, $\lfloor \frac{1}{t} \rfloor (n-m)\sqrt{3}$ have a mantissa of less than 0.01.

Euclidean Algorithm 7

7.1Exericse

- 1. Let F_n be Fermat Primes, i.e. $F_n = 2^{2^n} + 1$. Prove that they are pairwise coprime, namely $gcd(F_n, F_m) = 1$.
- 2. Use the **Euclidean Algorithm** to find a integer pair (x,y) that 111x - 321y = 75.

7.2 Solution

1. Just assume that n > m, let n = m + k, we have

$$F_m = 2^{2^m} + 1$$

$$F_{m+k} = 2^{2^{m+k}} + 1 = 2^{2^{m} \cdot 2^k} + 1$$

So

$$F_{m+k} - 2 = 2^{2^m \cdot 2^k} - 1 = (2^{2^m})^{2^k} - 1$$

Since

$$2^{2^m} + 1 \mid (2^{2^m})^{2^k} - 1 \Rightarrow F_m \mid F_{m+k} - 2$$

Considering F_n, F_m are odd numbers, so $gcd(F_n, F_m) = 1$.

- 2. This is a really boring quesion, but this is highly likely to appear in the exam.
 - Step 1. gcd(111, 321) = 3, so we reduce the equation to 37x 107y = 25. We first solve 37x 107y = 1.
 - Step 2. Apply the algorithm

$$107 = 37 \times 2 + 33$$
$$37 = 33 \times 1 + 4$$
$$33 = 4 \times 8 + 1$$
$$4 = 1 \times 4$$

So

$$1 = 33 \times 1 - 4 \times 8$$

$$= 33 \times 1 - (37 - 33 \times 1) \times 8$$

$$= 37 \times (-8) + 33 \times 9$$

$$= 37 \times (-8) + (107 - 37 \times 2) \times 9$$

$$= 107 \times 9 + 37 \times (-26)$$

One solution for 37x - 107y = 1 is given as (x, y) = (-26, -9), so the solution for 37x - 107 = 25 can be (x, y) = (-650, -225).

8 Group Theory

8.1 Exercise

1. $\mathbb{Z}^2 = \mathbb{Z} \times \mathbb{Z}$ denotes the set of pairs of integers:

$$\mathbb{Z}^2 = \{ (m, n) \mid m, n \in \mathbb{Z} \}.$$

It is a group under "vector addition", that is,

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

Consider the set

$$H = \{(x, y) \mid x + y \geqslant 0\}.$$

Check if H is a subgroup of \mathbb{Z}^2 .

2.

- Can an abelian group have a non-abelian subgroup?
- Can a non-abelian group have an abelian subgroup?
- Can a non-abelian group have a non-abelian subgroup?
- 3. Prove that
- S_n is non-Abelian for $n \ge 3$;
- A_n is a subgroup of S_n ;
- $|A_n| = \frac{n!}{2}$.
- 4. Prove: For any subgroup $H \leq G$, the (left) cosets of H partition the group G.

8.2 Solution

1.

- Associativity:

Suppose $(a, b), (c, d), (e, f) \in H$, then

$$[(a,b) + (c,d)] + (e,f) = (a,b) + [(c,d) + (e,f)] = (a+c+e,b+d+f).$$

- Closure:

Suppose $(a, b), (c, d) \in H$. This means

$$a+b \geqslant 0$$
 and $c+d \geqslant 0$.

Then

$$(a+c) + (b+d) = (a+b) + (c+d) \ge 0 + 0 = 0.$$

Therefore,

$$(a,b) + (c,d) = (a+c,b+d) \in H.$$

Thus, H is closed under addition.

- Identity:

Since
$$0 + 0 = 0 \ge 0$$
, I have $(0, 0) \in H$.

- Inverses:

$$(1,2) \in H$$
, because $1+2=3 \ge 0$. But $(1,2)=(1,2) \notin H$, because

$$1 + (2) = 3 \ge 0.$$

Thus, the inverse axiom fails.

Hence, H is not a subgroup of G.

- 2. No; Yes; Yes.
- Every subgroup of an abelian group is abelian. If G is an abelian group and H is a subgroup of G, then the operation on H is commutative because it is already commutative in G and H is a subset of G. Hence an abelian group cannot have a non-abelian subgroup.

- A non-abelian group can have an abelian subgroup. For example, the symmetric group S_3 of permutation of degree 3 is non-abelian while its subgroup A_3 is abelian.
- A non-abelian group can have a non-abelian subgroup. For example, S_4 is a non-abelian group and its subgroup A_4 is also non-abelian.

3.

(-) All that we need to do here is to find two permutations σ and τ in S_n with $n \ge 3$ such that $\sigma \tau \ne \tau \sigma$. Indeed, consider the permutations

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & \cdots & n \\ 1 & 3 & 2 & 4 & 5 & \cdots & n \end{pmatrix} \quad \text{and} \quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & \cdots & n \\ 3 & 2 & 1 & 4 & 5 & \cdots & n \end{pmatrix}.$$

Then,

$$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & \cdots & n \\ 2 & 3 & 1 & 4 & 5 & \cdots & n \end{pmatrix} \quad \text{and} \quad \tau\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & \cdots & n \\ 3 & 1 & 2 & 4 & 5 & \cdots & n \end{pmatrix},$$

so that $\sigma \tau \neq \tau \sigma$.

- (-) Obviously, A_n is a subset of S_n . We then show it is a subgroup.
 - (a) Associativity: $\forall x, y, z \in A_n \subset S_n$, since S_n is a group, (xy)z = x(yz).
 - (b) Closure: Since the sum of two even number is even, the composition of two even bijections is even.
 - (c) Identity: 1 = (1) = (01)(01) is even, so $1 = (1) \in A_n$.
 - (d) Inverse: $\forall x \in A_n, \exists x^{-1} \in S_n \text{ is also in } A_n \text{ because it has the same number of transportation as } x, \text{ which is even.}$

Therefore, A_n is a subgroup of S_n .

(-) Denote the set of all odd permutations in S_n as B_n . We aim to prove $|A_n| = |B_n|$, *i.e.*, there exists a bijection between A_n and B_n . Demote this bijection by F, and we have $F: A_n \to B_n$. Let $F(\sigma) = (01)\sigma$, where $\sigma \in A_n$ is even.

- (a) Injection: Assume $\sigma_1, \sigma_2 \in A_n$. If $\sigma_1 \neq \sigma_2$, $(01)\sigma_1 \neq (01)\sigma_2$. Therefore, F is injective.
- (b) Surjection: Every $\tau_1 \in B_n$ can be represented as $(01)\tau_2$ where $\tau_2 \in A_n$ because $\tau_1 = (01)\tau_2 = (01)(01)\tau_1$ where $\tau_2 = (01)\tau_1$ is even. Hence F is surjective.

Therefore, F is a bijection. Considering $|S_n| = n!$, we have $|A_n| = \frac{n!}{2}$.

- 4. We need to show that the union of the left cosets is the whole group, and that different cosets do not overlap.
 - For all $g \in G$, $g \in gH$ since H is a subgroup of G which includes the identity 1_G . This shows that every element of G lies in some coset of H, so the union of the cosets is all of G.
 - Suppose aH and bH are two cosets of H, and suppose they are not disjoint. We must show they are identical: aH = bH. As usual, we can show two sets are equal by showing that each is contained in the other.

Since aH and bH are not disjoint, we can find an element $g \in aH \cap bH$. Write $g = ah_1 = bh_2$ for $h_1, h_2 \in H$. Then

$$a = bh_2h_1^{-1}.$$

Now let $ah \in aH$. Then

$$ah = bh_2h_1^{-1}h.$$

The element on the right is in bH, since it is b times $h_2h_1^{-1}h \in H$. Therefore, $ah \in bH$, i.e., $aH \subset bH$. By symmetry, $bH \subset aH$, so aH = bH.

9 Graph Theory

9.1 Exercise

1. The complement of a simple graph G = (V, E) is given by $G^c = (V, E^c)$, where $E^c = V \times V \setminus E$, i.e., the complement has the same vertex

set and an edge is in E^c if and only if it is not in E. A graph G is said to be *self-complementary* if G is isomorphic to G^c .

- i) Show that a self-complementary graph must have either 4m or 4m+1 vertices, $m \in \mathbb{N}$.
- ii) Find all self-complementary graphs with 8 or fewer vertices.

(Taken from Ve203 FA2020 Assignment10)

9.2 Solution

1.

- i) Consider $G \cup G^c = (V, E \cup E^c) = K_n$, there are in total $\binom{n}{2}$ edges. The total number of edges must be even. We consider the remainder of n modulo 4:
 - n = 4m:

$$\binom{4m}{2} = \frac{4m(4m-1)}{2} = 2m \cdot (4m-1)$$
 - even $\sqrt{ }$

• n = 4m + 1:

$$\binom{4m+1}{2} = \frac{4m(4m+1)}{2} = 2m \cdot (4m+1)$$
 - even $\sqrt{ }$

• n = 4m + 2:

$$\binom{4m+2}{2} = \frac{(4m+1)(4m+2)}{2} = (2m+1) \cdot (4m+1) - \text{odd} \times$$

• n = 4m + 3:

$$\binom{4m+3}{2} = \frac{(4m+3)(4m+2)}{2} = (2m+1) \cdot (4m+3) - \text{odd} \times$$

ii) n can only be 4 or 5. Consider C_5 and P_4 .