Assignment 1

Sixiang Qiu
October 2021

Problem 1

Problem 1 (22 marks)
For $x, y \in \mathbb{Z}$ we define the set:

$$S_{x,y} = \{mx + ny : m, n \in \mathbb{Z}\}.$$

(a) Give five elements of $S_{4,-6}$. (5 marks)

(b) Give five elements of $S_{12,18}$. (5 marks)

For the following questions, let $d = \gcd(x, y)$ and z be the smallest positive number in $S_{x,y}$, or 0 if there are no positive numbers in $S_{x,y}$.

(c) (i) Show that $S_{x,y} \subseteq \{n : n \in \mathbb{Z} \text{ and } d|n\}$. (4 marks)

(ii) Show that $d \leq z$. (2 marks)

(d) (i) Show that $z|x$ and $z|y$ (*Hint: consider* $(x \% z)$ *and* $(y \% z)$). (4 marks)

(ii) Show that $z \leq d$. (2 marks)

Remark

The result that there exists $m, n \in \mathbb{Z}$ such that $mx + ny = \gcd(x, y)$ is known as Bézout's Identity.

(a)

$$S_{4,-6} = \{\ 4m - 6y : m, n \in Z\ \} \tag{1}$$

Value of m, n	Elements of S
m = 1, n = 1	-2
m = 2, n = 2	-4
m = 3, n = 3	-6
m = 4, n = 4	-8
m = 5, n = 5	-10

(b)

$$S_{12,18} = \{\, 12m + 18y : m, n \in Z \,\} \tag{2}$$

Value of m, n	Elements of S
m = 1, n = 1	30
m = 2, n = 2	60
m = 3, n = 3	90
m = 4, n = 4	120
m = 5, n = 5	150

(c)

(i)

1. Suppose *w* to be elements of *S*,

$$S_{x,y} = \{\, mx + ny : m, n \in Z \,\} \tag{3}$$

2. Then *w* can be expressed in the form as follow, where x, y are Integers.

$$w = mx + ny \quad (m, n \in Z) \tag{4}$$

3. Since $d \ = \ gcd\ (\ x,\ y\ )$, then $d \mid x$ and $d \mid y$,
4. Since m, n are Integers, then $d \mid mx$ and $d \mid ny$,
5. Clearly, $d \mid (\ mx \ + \ ny\ )$, that is $d \mid w$,
6. Clearly,

$$w \ \in \{\, n : n \in Z \; and \; d \mid n \,\} \tag{5}$$

7. Then,

$$S_{x,y} \subseteq \{\, n : n \in Z \; and \; d \mid n \,\} \tag{6}$$

(ii)

1. In the definition of greatest common divisor,

   we have $d \ \geq \ 0\ (\ d \ = \ 0\ for\ x \ = \ y \ = \ 0\ )$.

2. · From question **(c) (i)**, we have $d \mid w$ (*w* stands for elements in set *S*)

   · Clearly, *z* is one of the elements in set *S*

   Therefore, $d \mid z$.

3. Since *z* is positive (*z* = 0 if there are no positive element in set *S*) and $d \mid z$,

   Therefore, $z \ = \ Cd\ (\ where\ C\ is\ a\ positive\ Integer\ )$.

   Therefore, $z \ \geq \ d\ (\ z \ = \ d\ for\ x \ = \ y \ = \ 0\ )$.

(d)

(i)

1. To prove this question, here refers to definition from Lecture material as follow.

Definition

Let $m, p \in \mathbb{Z}$, $n \in \mathbb{Z}_{>0}$.

- $m \text{ div } n = \lfloor \frac{m}{n} \rfloor$
- $m \,\%\, n = m - (m \text{ div } n) \cdot n$
- $m =_{(n)} p$ if $n | (m - p)$

2. To prove this question, here starts from x since the procedure is the same for those of y.

 From definition 1 and 2, x could be described as following format:

$$x \,\%\, z = x - \lfloor \frac{x}{z} \rfloor \cdot z \tag{7}$$

3. Since *z* is one of the element of set *S*, we have:

$$z = m_1 x + n_1 y \tag{8}$$

Substitute equation (7) with equation (8), we have:

$$\begin{aligned} x \,\%\, z &= x - \lfloor \frac{x}{z} \rfloor \, (m_1 x + n_1 y) \\ &= (1 - \lfloor \frac{x}{z} \rfloor \, m_1) \, x + (-\lfloor \frac{x}{z} \rfloor n_1) \, y \\ &\downarrow \\ x \,\%\, z &= m_2 x + n_2 y \, (\text{where } m_2, \, n_2 \in Z) \end{aligned} \tag{9}$$

Therefore, $x \,\%\, z$ is also one of the element of set *S*.

4.

Fact

- $0 \leq (m \,\%\, n) < n$.
- $m =_{(n)} p$ *if, and only if,* $(m \,\%\, n) = (p \,\%\, n)$.
- $m =_{(n)} (m \,\%\, n)$
- *If* $m =_{(n)} m'$ *and* $p =_{(n)} p'$ *then:*
  - $m + p =_{(n)} m' + p'$ *and*
  - $m \cdot p =_{(n)} m' \cdot p'$.

From the definition above, we have:

$$x \,\%\, z \in [\, 0, \, z \,) \tag{10}$$

5. Since *z* is the smallest positive number in set *S*,

$$x \,\%\, z = 0 \tag{11}$$

6. Therefore, $z \mid x$, vice versa for proof of $z \mid y$.

(ii)

1. From question **(d) (i)**, we have :

   $\cdot\ x \,\%\, z \;=\; 0$

   $\cdot\ y \,\%\, z \;=\; 0,$

   Therefore, z is one of the common divisor of x, y.

2. Since d is the greatest common divisor of x, y.

   Therefore, $z \leq d$.

Problem 2

Problem 2 (12 marks)
For all $x, y \in \mathbb{Z}$ with $y > 1$:

(a) Prove that if $\gcd(x, y) = 1$ then there is at least one $w \in [0, y) \cap \mathbb{N}$ such that $wx =_{(y)} 1$.
(Hint: Use Bézout's identity) (4 marks)

(b) Prove that if $\gcd(x, y) = 1$ and $y | kx$ then $y | k$. (4 marks)

(c) Prove that if $\gcd(x, y) = 1$ then there is at most one $w \in [0, y) \cap \mathbb{N}$ such that $wx =_{(y)} 1$. (4 marks)

(a)

1. **Remark**

   The result that there exists $m, n \in \mathbb{Z}$ such that $mx + ny = \gcd(x, y)$ is known as Bézout's Identity.

   Clearly, w is an Integer, which satisfies Bézout's Identity,

   Substitute m with w, we have:

$$\begin{gathered} wx \;+\; ny \;=\; gcd\,(\,x,\;y\,) \;=\; 1 \\ \downarrow \\ wx \;+\; ny \;=\; 1 \\ \downarrow \\ wx \;-\; 1 \;=\; (-n)\,y \end{gathered} \tag{12}$$

   Therefore, $y \,|\, (\,wx \;-\; 1\,)$.

2. **Definition**

   Let $m, p \in \mathbb{Z},\ n \in \mathbb{Z}_{>0}$.

   - $m \text{ div } n = \lfloor \frac{m}{n} \rfloor$
   - $m \,\%\, n = m - (m \text{ div } n) \cdot n$
   - $m =_{(n)} p$ if $n | (m - p)$

From definition 3, we have:

$$wx =_{(y)} 1 \tag{13}$$

(b)

1. **Fact**

   $\gcd(m, n) \cdot \operatorname{lcm}(m, n) = |m| \cdot |n|$

   From Fact, we have:

$$\begin{gathered} gcd\,(\,x,\ y\,)\ \cdot\ lcm\,(\,x,\ y\,)\ =\ |\,x\,|\ \cdot\ |\,y\,| \\ \downarrow \\ lcm\,(\,x,\ y\,)\ =\ |\,x\,|\ \cdot\ |\,y\,| \end{gathered} \tag{14}$$

2. Clearly, x could not be the multiples of y.

   Otherwise, the result of $lcm\ (x,\ y)$ would be $|x|$ but $|x| \cdot |y|$.

3. However, $y \mid kx$.

   Therefore, $y \mid k$.

(c)

1. From Bézout's Identity, suppose there exists a pair of *w* which:

$$\begin{gathered} w_1 x\ +\ n_1 y\ =\ gcd\,(\,x,\ y\,)\ =\ 1 \\ w_2 x\ +\ n_2 y\ =\ gcd\,(\,x,\ y\,)\ =\ 1 \\ \downarrow \\ (\,w_1\ -\ w_2\,)\,x\ =\ (\,n_2\ -\ n_1\,)\,y \\ \downarrow \\ y \mid (\,w_1\ -\ w_2\,)\,x \end{gathered} \tag{15}$$

2. From question **(b)**, which, $if\ gcd\,(\,x,\ y\,)\ =\ 1\ and\ y \mid kx\ then\ y \mid k$:

$$y \mid (\,w_1\ -\ w_2\,) \tag{16}$$

3. Since:

$$\begin{gathered} w_1\ \in\ [\,0,\ y\,) \\ w_2\ \in\ [\,0,\ y\,) \\ \downarrow \\ -\,y\ <\ w_1\ -\ w_2\ <\ y \end{gathered} \tag{17}$$

4. Statement in Line 3 contradicts the Statement in Line 2.

   Therefore, there is at most one *w*.

Problem 4

Problem 4 (16 marks)

Use the laws of set operations (and any results proven in lectures) to prove the following identities:

(a) (Annihilation): $A \cap \emptyset = \emptyset$ (4 marks)

(b) $(A \setminus C^c) \cup (B \cap C) = C \cap (B \cup A)$ (4 marks)

(c) $A^c \oplus \mathcal{U} = A$ (4 marks)

(d) (De Morgan's law): $(A \cap B)^c = A^c \cup B^c$ (4 marks)

Proof assistant

https://www.cse.unsw.edu.au/~cs9020/cgi-bin/logic/21T3/set_theory/assignment

(a)

$A \cap \emptyset$	$= A \cap (A \cap A^c)$	(Complement with ∩)
	$= (A \cap A^c) \cap A$	(Commutatitivity of ∩)
	$= (A^c \cap A) \cap A$	(Commutatitivity of ∩)
	$= A^c \cap (A \cap A)$	(Associativity of ∩)
	$= A^c \cap A$	(Idempotence of ∩)
	$= A \cap A^c$	(Commutatitivity of ∩)
	$= \emptyset$	(Complement with ∩)

(b)

$(A \setminus C^c) \cup (B \cap C)$	$= (A \cap C^{cc}) \cup (B \cap C)$	(Definition of \)
	$= (A \cap C) \cup (B \cap C)$	(Double complement)
	$= (C \cap A) \cup (B \cap C)$	(Commutatitivity of ∩)
	$= (C \cap A) \cup (C \cap B)$	(Commutatitivity of ∩)
	$= C \cap (A \cup B)$	(Distributivity of ∩ over ∪)
	$= C \cap (B \cup A)$	(Commutatitivity of ∪)

(c)

$A^c \oplus \mathcal{U}$	$= (A^c \cap \mathcal{U}^c) \cup (A^{cc} \cap \mathcal{U})$	(Definition of $\oplus$)
	$= (A^c \cap \mathcal{U}^c) \cup (A \cap \mathcal{U})$	(Double complement)
	$= (A^c \cap \mathcal{U}^c) \cup A$	(Identity of $\cap$)
	$= ((A^c \cap \mathcal{U}) \cap \mathcal{U}^c) \cup A$	(Identity of $\cap$)
	$= (A^c \cap (\mathcal{U} \cap \mathcal{U}^c)) \cup A$	(Associativity of $\cap$)
	$= (A^c \cap \emptyset) \cup A$	(Complement with $\cap$)
	$= (A^c \cap (A \cap A^c)) \cup A$	(Complement with $\cap$)
	$= ((A \cap A^c) \cap A^c) \cup A$	(Commutatitivity of $\cap$)
	$= (A \cap (A^c \cap A^c)) \cup A$	(Associativity of $\cap$)
	$= (A \cap A^c) \cup A$	(Idempotence of $\cap$)
	$= \emptyset \cup A$	(Complement with $\cap$)
	$= A \cup \emptyset$	(Commutatitivity of $\cup$)
	$= A$	(Identity of $\cup$)

Problem 5

Problem 5 (12 marks)
Let $\Sigma = \{0, 1\}$. For each of the following, prove that the result holds for all sets $X, Y, Z \subseteq \Sigma^*$, or provide a counterexample to disprove:

(a) $(X \cap Y)^* = X^* \cap Y^*$ (4 marks)

(b) $(XY)^* = (YX)^*$ (4 marks)

(c) $X(Y \cap Z) = (XY) \cap (XZ)$ (4 marks)

(a)

1. Suppose $X = \{\ 001\ \}$ *while* $Y = \{\ 0,\ 1\ \}$:

$$\begin{gathered} X \cap Y = \{\lambda\} \\ \downarrow \\ (X \cap Y)^* = \{\lambda\} \end{gathered} \tag{18}$$

2. Clearly, $X = \{\ 001\ \}$ is one of the element of Y^3.
3. Therefore, $\{\ 001\ \} \in X^* \cap Y^*$.
4. Therefore, $(X \cap Y)^* \neq X^* \cap Y^*$, equation in question **(a)** disproved.

(b)

1. Suppose $X = \{ 0 \}$ *while* $Y = \{ 1 \}$:

$$\begin{aligned} XY &= \{ 01 \} \\ YX &= \{ 10 \} \\ &\downarrow \\ (XY)^* &= \{\lambda,\ 01,\ 0101,\ 010101,\ \dots \} \end{aligned} \tag{19}$$

2. Clearly, $YX \notin (XY)^*$
3. Therefore, $(XY)^* \neq (YX)^*$, equation in question **(b)** disproved.

(c)

1.

$$X(Y \cap Z) = \{ xy : x \in X \text{ and } y \in (Y \cap Z) \} \tag{20}$$

$$\begin{aligned} (XY) \cap (XZ) = &\{ xy : x \in X \text{ and } y \in Y \} \cap \\ &\{ xy : x \in X \text{ and } y \in Z \} \end{aligned} \tag{21}$$

2. Since the fore part of XY is the same as those of XZ,

   Their intersection is actually the intersection of their rear part,

   Equation (21) can be written as:

$$(XY) \cap (XZ) = \{ xy : x \in X \text{ and } (y \in Y \text{ and } y \in Z) \} \tag{22}$$

   Therefore, $y \in (Y \cap Z)$
3. Therefore, $X(Y \cap Z) = (XY) \cap (XZ)$

Problem 6

Problem 6 (12 marks)

(a) List all possible functions $f : \{a, b, c\} \to \{0, 1\}$, that is, all elements of $\{0, 1\}^{\{a,b,c\}}$. (4 marks)

(b) Describe a connection between your answer for (a) and $\mathrm{Pow}(\{a, b, c\})$. (4 marks)

(c) Describe a connection between your answer for (a) and $\{w \in \{0, 1\}^* : \mathrm{length}(w) = 3\}$. (4 marks)

(a)

Functions	Expressions
1	$f(a) = 0$ $f(b) = 0$ $f(c) = 0$

Functions	Expressions
2	$f(a) = 1$ $f(b) = 1$ $f(c) = 1$
3	$f(a) = 0$ $f(b) = 0$ $f(c) = 1$
4	$f(a) = 0$ $f(b) = 1$ $f(c) = 0$
5	$f(a) = 0$ $f(b) = 1$ $f(c) = 1$
6	$f(a) = 1$ $f(b) = 0$ $f(c) = 0$
7	$f(a) = 1$ $f(b) = 1$ $f(c) = 0$
8	$f(a) = 1$ $f(b) = 0$ $f(c) = 1$

(b)

1. **Fact**

   Always $|Pow(X)| = 2^{|X|}$

   From Fact, we have:

   $$\begin{aligned} |\ Pow\ (\ \{\ a,\ b,\ c\ \}\ )\ | &= 2^{|\{a,b,c\}|} \\ &= 2^3 \ = \ 8 \end{aligned} \tag{23}$$

2. Also, $|\ \{0,\ 1\}^{\{a,b,c\}}\ | \ = \ 8$.
3. Therefore, the cardinality of answer for question (a) is equal to those of $Pow\ (\ \{\ a,\ b,\ c\ \}\ )$.

(c)

1. Suppose $\Sigma = \{ 0, 1 \}$, then:

$$
\begin{gathered}
|\{ w \in \{ 0, 1 \}^* : \mathit{length}(w) = 3 \}| \\
\downarrow \\
|\{ w \in \Sigma^* : \mathit{length}(w) = 3 \}| \\
\downarrow \\
|\Sigma^3| = |\Sigma|^3 = 2^3 = 8
\end{gathered}
\tag{24}
$$

2. Also, $|\{0, 1\}^{\{a,b,c\}}| = 8$.

3. Therefore, the cardinality of answer for question (a) is equal to those of $\{ w \in \{ 0, 1 \}^* : \mathit{length}(w) = 3 \}$.

Problem 8

Problem 8 **(16 marks)**

Recall the relation composition operator ; defined as:

$$R_1; R_2 = \{(a, c) : \text{there is a } b \text{ with } (a, b) \in R_1 \text{ and } (b, c) \in R_2\}$$

Let S be an arbitrary set. For each of the following, prove it holds for any binary relations $R_1, R_2, R_3 \subseteq S \times S$, or give a counterexample to disprove:

(a) $(R_1; R_2); R_3 = R_1; (R_2; R_3)$ (4 marks)

(b) $I; R_1 = R_1; I = R_1$ where $I = \{(x, x) : x \in S\}$ (4 marks)

(c) $(R_1 \cup R_2); R_3 = (R_1; R_3) \cup (R_2; R_3)$ (4 marks)

(d) $R_1; (R_2 \cap R_3) = (R_1; R_2) \cap (R_1; R_3)$ (4 marks)

(a)

1. For better flow of writing, syntax there is a b, is substituted with $\exists b$,

   Therefore:

$$
\begin{gathered}
R_1; R_2 = \{ (a, c) : \mathit{there\ is\ a\ b\ with}\ (a, b) \in R_1\ \mathit{and}\ (b, c) \in R_2 \} \\
\downarrow \\
R_1; R_2 = \{ (a, c) : \exists b\ (\ (a, b) \in R_1 \ \wedge\ (b, c) \in R_2\ ) \}
\end{gathered}
\tag{25}
$$

2. Suppose $< x, z > \in (R_1; R_2); R_3$:

$$
\begin{gathered}
\exists y_1\ ((< x, y_1 > \in (R_1; R_2)) \wedge (< y_1, z > \in R_3)) \\
\Updownarrow \\
\exists y_1\ ((\exists y_2 (< x, y_2 > \in R_1) \wedge (< y_2, y_1 > \in R_2)) \wedge (< y_1, z > \in R_3)) \\
\Updownarrow \\
\exists y_1\ \exists y_2\ (((< x, y_2 > \in R_1) \wedge (< y_2, y_1 > \in R_2)) \wedge (< y_1, z > \in R_3)) \\
\Updownarrow \\
\exists y_1\ \exists y_2\ ((< x, y_2 > \in R_1) \wedge ((< y_2, y_1 > \in R_2) \wedge (< y_1, z > \in R_3))) \\
\Updownarrow \\
\exists y_2\ ((< x, y_2 > \in R_1) \wedge \exists y_1\ ((< y_2, y_1 > \in R_2) \wedge (< y_1, z > \in R_3))) \\
\Updownarrow \\
\exists y_2\ ((< x, y_2 > \in R_1) \wedge (< y_2, z > \in (R_2; R_3)))
\end{gathered}
\tag{26}
$$

$$\Updownarrow$$
$$< x, z > \in R_1; (R_2; R_3)$$

3. Therefore, $(R_1; R_2); R_3 \ = \ R_1; (R_2; R_3)$.

(b)

1. Suppose $(x, z) \in I; R_1$ *where* $I \ = \ \{(x, x) : x \in S\}$:

$$\begin{gathered} \exists y \ (\ ((x, y) \in I) \wedge ((y, z) \in R_1) \ ) \\ \Downarrow \\ \exists x \ (\ ((x, x) \in I) \wedge ((x, z) \in R_1) \ ) \\ \Downarrow \\ I; R_1 \subseteq R_1 \end{gathered} \tag{27}$$

2. Reversely, suppose $(x, z) \in R_1$, then:

$$\begin{gathered} (x, x) \in I \\ \Downarrow \\ (x, z) \in I; R_1 \\ \Downarrow \\ R_1 \subseteq I; R_1 \end{gathered} \tag{28}$$

   Therefore, $I; R_1 \ = \ R_1$.

3. Suppose $(x, z) \in R_1; I$ *where* $I \ = \ \{(x, x) : x \in S\}$:

$$\begin{gathered} \exists y \ (\ ((x, y) \in R_1) \wedge ((y, z) \in I) \ ) \\ \Downarrow \\ \exists z \ (\ ((x, z) \in R_1) \wedge ((z, z) \in I) \ ) \\ \Downarrow \\ R_1; I \subseteq R_1 \end{gathered} \tag{29}$$

4. Reversely, suppose $(x, z) \in R_1$, then:

$$\begin{gathered} (z, z) \in I \\ \Downarrow \\ (x, z) \in R_1; I \\ \Downarrow \\ R_1 \subseteq R_1; 1 \end{gathered} \tag{30}$$

   Therefore, $R_1; 1 \ = \ R_1$.

5. Therefore, $I; R_1 \ = \ R_1; I \ = \ R_1$.

(c)

1. Suppose $< x, z >\in (R_1 \cup R_2); R_3$:

$$\begin{gathered}
\exists y\,((< x, y >\in (R_1 \cup R_2)) \wedge (< y, z >\in R_3)) \\
\Updownarrow \\
\exists y\,((< x, y >\in R_1 \vee < x, y >\in R_2) \wedge (< y, z >\in R_3)) \\
\Updownarrow \\
\exists y\,(((< x, y >\in R_1) \wedge (< y, z >\in R_3)) \vee ((< x, y >\in R_2) \wedge (< y, z >\in R_3))) \\
\Updownarrow \\
\exists y\,((< x, y >\in R_1) \wedge (< y, z >\in R_3)) \vee \exists y\,((< x, y >\in R_2) \wedge (< y, z >\in R_3)) \\
\Updownarrow \\
< x, z >\in R_1; R_3 \vee < x, z >\in R_2; R_3 \\
\Updownarrow \\
< x, z >\in (R_1; R_3) \cup (R_2; R_3)
\end{gathered} \tag{31}$$

2. Therefore, $(R_1 \cup R_2); R_3 \ = \ (R_1; R3) \cup (R_2; R_3)$.

(d)

1. Suppose $< x, z >\in R_1; (R_2 \cap R_3)$:

$$\begin{gathered}
\exists y\,((< x, y >\in R_1) \wedge (< y, z >\in (R_2 \cap R_3))) \\
\Updownarrow \\
\exists y\,((< x, y >\in R_1) \wedge ((< y, z >\in R_2) \wedge (< y, z >\in R_3))) \\
\Downarrow \\
\exists y\,((< x, y >\in R_1) \wedge (< y, z >\in R_2)) \wedge \exists y\,((< x, y >\in R_1) \wedge (< y, z >\in R_3)) \\
\Updownarrow \\
< x, z >\in R_1; R_2 \wedge < x, z >\in R_1; R_3 \\
\Updownarrow \\
< x, z >\in (R_1; R_2) \cap (R_1; R_3)
\end{gathered} \tag{32}$$

2. Since equation (32) includes an unfold of conjunction, the result should not be equal but inclusion.

   Therefore, $R_1; (R_2 \cap R_3) \subseteq (R_1; R_2) \cap (R_1; R_3)$.

3. Equation in question (d) disproved.