Assignment1

z5395765

October 24, 2022

Problem1

For $x, y \in Z$ we define the set:

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

(a) Give four elements of $S_{6,9}$.

$S_{6,9} = \{6m + 9n : m, n \in Z\}$.

let $m = 0, n = 0$, the element is 0.

let $m = 1, n = -1$, the element is -3.

let $m = -1, n = 1$, the element is 3.

let $m = 1, n = 0$, the element is 6.

So, four elements of $S_{6,9}$: -3, 0, 3, 6.

(b) Give four elements of $S_{10,-16}$.

$S_{10,-16} = \{10m - 16 : m, n \in Z\}$.

let $m = 0, n = 0$, the element is 0.

let $m = 1, n = 1$, the element is -6.

let $m = -1, n = -1$, the element is 6.

let $m = 1, n = 0$, the element is 10.

So, four elements of $S_{10,-16}$: -6, 0, 6, 10.

For the following questions, let $d = \text{gcd}(x, y)$ 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 $S_{x,y} \subseteq \{n : n \in Z$ and $d|n\}$.

Suppose $a \in S_{x,y}$, then $a = mx + ny$ for some $m, n \in Z$.

Because $d = gcd(x, y)$, so there exists $x = k_1d$ for some k_1 and $y = k_2d$ for some k_2. Therefore $a = (k_1m+k_2n)d$.

Because $k_1, m, k_2, n \in Z$, so $k_1m + k_2n \in Z$, so there exists $k \in Z$, $a = kd$. Therefore $d|a$.

Therefore $a \in \{n : n \in Z \text{ and } d|n\}$.

Therefore $S_{x,y} \subseteq \{n : n \in Z \text{ and } d|n\}$.

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

Because z is a number in $S_{x,y}$, by the results of c(i), we can get that $d|z$.

Because $z \geq 0$, by definition of gcd, d is also positve,

therefore, $z \div d$ is a positive interger. So $z \div d \geq 1$.

Therefore $d \leq z$.

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

Suppose $x =_{(z)} p, y =_{(z)} q$, which means $z|(x-p)$ and $z|(y-q)$. In order to prove that $z|x$ and $z|y$, I will show that $p, q = 0$.

Because $z|(x-p)$ and $z|(y-q)$, there exists $k_1, k_2 \in Z$,

$$x = k_1 z + p,$$
$$x = k_2 z + q.$$

Because z is the smallest positive number in $S_{x,y}$, therefore $z = m_1 x + n_1 y$ for some $m_1, n_1 \in Z$. Then $z = mx + ny = m(k_1 z + p) + n(k_2 z + q)$.

Then $z = (mk_1 + nk_2)z + mp + nq$. In order to make this equation hold, we must set $mk_1 + nk_2 = 1$ and $mp + nq = 0$. In this case, m and n cannot be 0 at the same time, which means p and q are both 0.

Therefore, $p, q = 0$.

Therefore, $z|x$ and $z|y$.

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

Because $d = gcd(x, y)$, so there exists $x = k_1 d$ for some k_1 and $y = k_2 d$ for some k_2.

Because z is a number in $S_{x,y}$, therefore $z = mx + ny$ for some $m, n \in Z$.

Therefore $z = (k_1 m + k_2 n)d$.

In order to let z be the smallest number in $S_{x,y}$, we just need to set $mk_1 + nk_2$ is the smallest. Because z and d are both positive, so $mk_1 + nk_2$ is a positive integer. The smallest positive integer is 1. So $mk_1 + nk_2 = 1$.

Therefore $z = d$.

Therefore $z \leq d$.

Problem2

For all $x, y \in Z$ with $y > 1$:

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

By Bezout's identity, there exists $m, n \in Z, mx + ny = 1$, then $mx =_{(y)} 1$.

By Euclid's division lemma, for $m \in Z, y \in Z_{>0}$, there exists $q, r \in Z$ with $0 \le r < y$ such that

$$m = qy + r$$

Therefore, $(qy + r)x =_{(y)} 1$, which means $qyr + rx =_{(y)} 1$, since $y|yqr$, so $rx =_{(y)} 1$.

Therefore, there exists $r \in [0, y) \cap N$, $rx =_{(y)} 1$. So there is at least one $w \in [0, y) \cap N$, $wx =_{(y)} 1$.

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

By Bezout's identity, there exists $m, n \in Z, mx + ny = 1$.

Times k on both sides, then $kmx + kny = k$.

Because $y|kx, m \in Z$, then $y|kmx$. Plus, $y|kny$, so $k = kmx + kny$ is multiple of y.

Therefore, $y|k$.

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

Suppose there are more than one $w \in [0, y) \cap N$ such that $wx =_{(y)} 1$. Let's say two w satisfy this equation, then let $w_1x =_{(y)} 1$ and $w_2x =_{(y)} 1$, $w_1 \neq w_2$, which means

$$y|(w_1x - 1),$$
$$y|(w_2x - 1).$$

Therefore,

$$w_1x = k_1y + 1 \text{ for some } k_1,$$
$$w_2x = k_2y + 1 \text{ for some } k_2.$$

Subtract two equation, we get that $(w_1 - w_2)x = (k_1 - k_2)y$. So, $y|(w_1 - w_2)x$.

By the results of (b), we can get that $y|(w_1 - w_2)$.

Because $w \in [0, y) \cap N$, $w_1 - w_2$ can only be 0, so $w_1 = w_2$, which contradicts my suppose.

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

Problem3

Prove that for all $m, n \in N_{>0}$ with $n \le m$:

$$\tfrac{3}{2}(n + (m\%n)) < m + n.$$

Proof of Problem3

Let $m\%n = p$, which means $m = kn + p$ for $k \in Z$. So $\frac{3}{2}(n + (m\%n)) = \frac{3}{2}(n + p)$.

Let $S = \frac{3}{2}(n+p) - (m+n)$, in order to prove $\frac{3}{2}(n + (m\%n)) < m + n$,we just need to prove $S < 0$.

$S = \frac{3}{2}(n+q) - (m+n) = \frac{1}{2}n + \frac{3}{2}p - (kn+p) = \frac{1}{2}(n+p) - kn$.

Because $m, n \in N_{>0}$ with $n \leq m$, so for the equation $m = kn + p$, $k \geq 1$ and $0 < p < n$.

Because $0 < p < n$, so $S < \frac{1}{2}(n+n) - kn$, therefore $S < (1-k)n$.

Therefore, $S < 0$.

Therefore, $\frac{3}{2}(n + (m\%n)) < m + n$.

Problem4

(a) prove $A \cap \emptyset = \emptyset$.

$$\begin{aligned}
A \cap \emptyset &= A \cap (A \cap A^c) && \text{(Complement with } \cap\text{)} \\
&= (A \cap A) \cap A^c && \text{(Associativity of } \cap\text{)} \\
&= A \cap A^c && \text{(Idempotence of } \cap\text{)} \\
&= \emptyset && \text{(Complement with } \cap\text{)}
\end{aligned}$$

(b) prove $(A \setminus C) \cup (B \setminus C) = (A \cup B) \setminus C$

$$\begin{aligned}
(A \setminus C) \cup (B \setminus C) &= (A \cap C^c) \cup (B \setminus C) && \text{(Definition of } \setminus\text{)} \\
&= (A \cap C^c) \cup (B \cap C^c) && \text{(Definition of } \setminus\text{)} \\
&= (C^c \cap A) \cup (B \cap C^c) && \text{(Commutatitivity of } \cap\text{)} \\
&= (C^c \cap A) \cup (C^c \cap B) && \text{(Commutatitivity of } \cap\text{)} \\
&= C^c \cap (A \cup B) && \text{(Distributivity of } \cap \text{ over } \cup\text{)} \\
&= (A \cup B) \cap C^c && \text{(Commutatitivity of } \cap\text{)} \\
&= (A \cup B) \setminus C && \text{(Definition of } \setminus\text{)}
\end{aligned}$$

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

$$
\begin{aligned}
A^c \oplus \mathcal{U} &= (A^c \cap \mathcal{U}^c) \cup ((A^c)^c \cap \mathcal{U}) && \text{(Definition of } \oplus) \\
&= (A^c \cap \mathcal{U}^c) \cup (A \cap \mathcal{U}) && \text{(Double complement)} \\
&= (A^c \cap \mathcal{U}^c) \cup A && \text{(Identity of } \cap) \\
&= A \cup (A^c \cap \mathcal{U}^c) && \text{(Commutatitivity of } \cup) \\
&= (A \cup A^c) \cap (A \cup \mathcal{U}^c) && \text{(Distributivity of } \cup \text{ over } \cap) \\
&= \mathcal{U} \cap (A \cup \mathcal{U}^c) && \text{(Complement with } \cup) \\
&= (\mathcal{U} \cap A) \cup (\mathcal{U} \cap \mathcal{U}^c) && \text{(Distributivity of } \cap \text{ over } \cup) \\
&= (\mathcal{U} \cap A) \cup \emptyset && \text{(Complement with } \cap) \\
&= (A \cap \mathcal{U}) \cup \emptyset && \text{(Commutatitivity of } \cap) \\
&= A \cup \emptyset && \text{(Identity of } \cap) \\
&= A && \text{(Identity of } \cup)
\end{aligned}
$$

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

By uniqueness of complement: $A \cap B = \emptyset$ and $A \cup B = \cup$ if and only if $B = A^c$. In order to prove $(A \cup B)^c = A^c \cap B^c$, we just need to show that

(1) $(A \cup B) \cap (A^c \cap B^c) = \emptyset$.

(2) $(A \cup B) \cup (A^c \cap B^c) = \mathcal{U}$.

proof of (1)

$$
\begin{aligned}
(A \cup B) \cap (A^c \cap B^c) &= (A^c \cap B^c) \cap (A \cup B) && \text{(Commutatitivity of } \cap) \\
&= ((A^c \cap B^c) \cap A) \cup ((A^c \cap B^c) \cap B) && \text{(Distributivity of } \cap \text{ over } \cup) \\
&= (A \cap (A^c \cap B^c)) \cup ((A^c \cap B^c) \cap B) && \text{(Commutatitivity of } \cap) \\
&= ((A \cap A^c) \cap B^c) \cup ((A^c \cap B^c) \cap B) && \text{(Associativity of } \cap) \\
&= ((A \cap A^c) \cap B^c) \cup (A^c \cap (B^c \cap B)) && \text{(Associativity of } \cap) \\
&= (\emptyset \cap B^c) \cup (A^c \cap (B^c \cap B)) && \text{(Complement with } \cap) \\
&= (\emptyset \cap B^c) \cup (A^c \cap \emptyset) && \text{(Complement with } \cap) \\
&= \emptyset \cup (A^c \cap \emptyset) && \text{(Annihilation)} \\
&= \emptyset \cup \emptyset && \text{(Annihilation)} \\
&= \emptyset && \text{(Idempotence of } \cup)
\end{aligned}
$$

proof of (2)

$$
\begin{aligned}
(A \cup B) \cup (A^c \cap B^c) &= ((A \cup B) \cup A^c) \cap ((A \cup B) \cup B^c) && \text{(Distributivity of } \cup \text{ over } \cap\text{)} \\
&= (A^c \cup (A \cup B)) \cap ((A \cup B) \cup B^c) && \text{(Commutatitivity of } \cup\text{)} \\
&= ((A^c \cup A) \cup B) \cap ((A \cup B) \cup B^c) && \text{(Associativity of } \cup\text{)} \\
&= ((A^c \cup A) \cup B) \cap (A \cup (B \cup B^c)) && \text{(Associativity of } \cup\text{)} \\
&= (\mathcal{U} \cup B) \cap (A \cup (B \cup B^c)) && \text{(Complement with } \cup\text{)} \\
&= (\mathcal{U} \cup B) \cap (A \cup \mathcal{U}) && \text{(Complement with } \cup\text{)} \\
&= \mathcal{U} \cap (A \cup \mathcal{U}) && \text{(duality of Annihilation of (a))} \\
&= \mathcal{U} \cap \mathcal{U} && \text{(duality of Annihilation of (a))} \\
&= \mathcal{U} && \text{(Idempotence of } \cap\text{)}
\end{aligned}
$$

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

(e) prove $((A \cup B) \cap (B \cup C)) \cap (C \cup A) = ((A \cap B) \cup (B \cap C)) \cup (C \cap A)$

$$
\begin{aligned}
((A \cup B) \cap (B \cup C)) \cap (C \cup A) &= ((B \cup A) \cap (B \cup C)) \cap (C \cup A) && \text{(Commutatitivity of } \cup\text{)} \\
&= (B \cup (A \cap C)) \cap (C \cup A) && \text{(Distributivity of } \cup \text{ over } \cap\text{)} \\
&= (C \cup A) \cap (B \cup (A \cap C)) && \text{(Commutatitivity of } \cap\text{)} \\
&= ((C \cup A) \cap B) \cup ((C \cup A) \cap (A \cap C)) && \text{(Distributivity of } \cap \text{ over } \cup\text{)} \\
&= ((C \cup A) \cap B) \cup (((C \cup A) \cap A) \cap C) && \text{(Associativity of } \cap\text{)} \\
&= ((C \cup A) \cap B) \cup ((A \cap (C \cup A)) \cap C) && \text{(Commutatitivity of } \cap\text{)} \\
&= ((C \cup A) \cap B) \cup (((A \cap C) \cup (A \cap A)) \cap C) && \text{(Distributivity of } \cap \text{ over } \cup\text{)} \\
&= ((C \cup A) \cap B) \cup (((A \cap C) \cup A) \cap C) && \text{(Idempotence of } \cap\text{)} \\
&= ((C \cup A) \cap B) \cup (C \cap ((A \cap C) \cup A)) && \text{(Commutatitivity of } \cap\text{)} \\
&= ((C \cup A) \cap B) \cup ((C \cap (A \cap C)) \cup (C \cap A)) && \text{(Distributivity of } \cap \text{ over } \cup\text{)} \\
&= ((C \cup A) \cap B) \cup (((A \cap C) \cap C) \cup (C \cap A)) && \text{(Commutatitivity of } \cap\text{)} \\
&= ((C \cup A) \cap B) \cup ((A \cap (C \cap C)) \cup (C \cap A)) && \text{(Associativity of } \cap\text{)} \\
&= ((C \cup A) \cap B) \cup ((A \cap C) \cup (C \cap A)) && \text{(Idempotence of } \cap\text{)} \\
&= ((C \cup A) \cap B) \cup ((C \cap A) \cup (C \cap A)) && \text{(Commutatitivity of } \cap\text{)} \\
&= ((C \cup A) \cap B) \cup (C \cap A) && \text{(Idempotence of } \cup\text{)} \\
&= (B \cap (C \cup A)) \cup (C \cap A) && \text{(Commutatitivity of } \cap\text{)} \\
&= ((B \cap C) \cup (B \cap A)) \cup (C \cap A) && \text{(Distributivity of } \cap \text{ over } \cup\text{)} \\
&= ((B \cap C) \cup (A \cap B)) \cup (C \cap A) && \text{(Commutatitivity of } \cap\text{)} \\
&= ((A \cap B) \cup (B \cap C)) \cup (C \cap A) && \text{(Commutatitivity of } \cup\text{)}
\end{aligned}
$$

Problem5

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) $(X \cup Y)^{(*)} = X^{(*)} \cup Y^{(*)}$

Counterexample:

$X = \{0\}$, $Y = \{1\}$. Then, $X \cup Y = \{0, 1\}$.

Therefore, $0101 \in (X \cup Y)^{(*)}$, while $X^{(*)} \cup Y^{(*)} = \{00..., 11...\}$, 0101 is not in this set.

(b) $(X \cap Y)^{(*)} = X^{(*)} \cap Y^{(*)}$

Counterexample:

$X = \{0, 1\}$, $Y = \{01\}$. Then, $X \cap Y = \emptyset$, $(X \cap Y)^{(*)}$ is also empty set.

While $X^{(*)} \cap Y^{(*)} = \{0101...\}$, which is not empty set.

(c) $X(Y \cup Z) = (XY) \cup (XZ)$

Counterexample:

$X = \{0\}$, $Y = \{1\}$, $Z = \emptyset$. Then, $Y \cup Z = \{1\}$, so $X(Y \cup Z) = \{01\}$

While $XY = \{01\}, XZ = \{0\}, (XY) \cup (XZ) = \{0, 01\}$.

Problem6

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

$f_1 : f(a) = 0, f(b) = 0, f(c) = 0$

$f_2 : f(a) = 0, f(b) = 0, f(c) = 1$

$f_3 : f(a) = 0, f(b) = 1, f(c) = 0$

$f_4 : f(a) = 1, f(b) = 0, f(c) = 0$

$f_5 : f(a) = 0, f(b) = 1, f(c) = 1$

$f_6 : f(a) = 1, f(b) = 0, f(c) = 1$

$f_7 : f(a) = 1, f(b) = 1, f(c) = 0$

$f_8 : f(a) = 1, f(b) = 1, f(c) = 1$

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

Pow($\{a, b, c\}$) $= \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{b, c\}, \{a, c\}, \{a, b, c\}\}$

Therefore, if we consider $0, 1$ of (a) as one element appearing and not appearing in the subset, then it is corresponding to the 8 situations happening the power set of $\{a, b, c\}$.

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

$\{w \in \{0, 1\}^* : length(w) = 3\} = \{000, 001, 010, 011, 100, 101, 110, 111\}$, which is corresponding to contenation of all the results in the function f_i.

Problem7

Show that for any sets A, B, C there is a bijection between $A^{(B\times C)}$ and $(A^B)^C$.

Proof of Problem7

By definition, bijection is a function is a function that is bijective. So I will show that there is a bijection between $A^{(B\times C)}$ and $(A^B)^C$ by showing that there is a function between $A^{(B\times C)}$ and $(A^B)^C$ which is both injective and surjective.
By definition, for any sets A, B, C,

$$A^{(B\times C)} \text{ is the set of all functions from } B\times C \text{ to } A.$$
$$(A^B)^C \text{ is the set of all functions from } C \text{ to } A^B.$$

Problem8

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 conterexample to disprove:

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

Suppose there is $(a,b)\in R_1, (b,c)\in R_2, (c,d)\in R_3$.
By definition, $R_1;R_2 = \{(a,c) : \text{there is a } b \text{ with } (a,b)\in R_1 \text{ and } (b,c)\in R_2\}$.
Therefore, $(R_1;R_2);R_3 = \{(a,d) : \text{there is a } c \text{ with } (a,c)\in R_1;R_2 \text{ and } (c,d)\in R_3\}$.
Plus $R_2;R_3 = \{(b,d) : \text{there is a } c \text{ with } (b,c)\in R_2 \text{ and } (c,d)\in R_3\}$.
Therefore,

$$\begin{aligned}(R_1;R_2);R_3 &= \{(a,d) : \text{there is a } b \text{ with } (a,b)\in R_1 \text{ and } (b,d)\in R_2;R_3\}\\ &= R_1;(R_2;R_3).\end{aligned}$$

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

Suppose there is $(a,a),(b,b)\in I, (a,b)\in R_1$.
By definition,

$$\begin{aligned}I;R_1 &= \{(a,b) : \text{there is a } a \text{ with } (a,a)\in I \text{ and } (a,b)\in R_1\}\\ &= \{(a,b) : \text{there is a } b \text{ with } (a,b)\in R_1 \text{ and } (b,b)\in I\}\\ &= R_1;I\\ &= \{a,b\}\\ &= R_1.\end{aligned}$$

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

Suppose there is $(a_1, b), (a_2, c) \in R_1, (b, c) \in R_2, (c, d) \in R_3$.

Then $R_1 \cup R_2 = \{(a_1, b), (a_2, c), (b, c)\}$. Therefore,

$$\begin{aligned}
(R_1 \cup R_2); R_3 &= \{(a_2, d), (b, d) : \text{there is a } c \text{ with } (a_2, c), (b, c) \in R_1 \cup R_2 \text{ and } (c, d) \in R_3\} \\
&= \{(a_2, d) : \text{there is a } c \text{ with } (a_2, c) \in R_1 \cup R_2 \text{ and } (c, d) \in R_3\} \\
&\quad \cup \{(b, d) : \text{there is a } c \text{ with } (b, c) \in R_1 \cup R_2 \text{ and } (c, d) \in R_3\} \\
&= \{(a_2, d) : \text{there is a } c \text{ with } (a_2, c) \in R_1 \text{ and } (c, d) \in R_3\} \\
&\quad \cup \{(b, d) : \text{there is a } c \text{ with } (b, c) \in R_2 \text{ and } (c, d) \in R_3\} \\
&= (R_1; R_3) \cup (R_2; R_3).
\end{aligned}$$

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

Suppose there is $(a, b), (a, c_1), (a, e_1), (a, e_2) \in R_1, (b, c_2), (c_1, d), (e_1, f_1) \in R_2, (c_1, d), (b, c_2), (e_2, f_2) \in R_3$.

Then $R_2 \cap R_3 = \{(b, c_2), (c_1, d)\}$.

$R_1; R_2 = \{(a, c_2), (a, d), (a, f_1) :$ there is a b, c_1, e_1 with $(a, b), (a, c_1), (a, e_1) \in R_1$ and $(b, c_2), (c_1, d), (e_1, f_1) \in R_2\}$.

$R_1; R_3 = \{(a, c_2), (a, d), (a, f_2) :$ there is a b, c_1, e_2 with $(a, b), (a, c_1), (a, e_2) \in R_1$ and $(b, c_2), (c_1, d), (e_1, f_2) \in R_3\}$.

$$\begin{aligned}
R_1; (R_2 \cap R_3) &= \{(a, c_2), (a, d) : \text{there is a } b, c_1 \text{ with } (a, b), (a, c_1) \in R_1 \text{ and } (b, c_2), (c_1, d) \in R_2 \cap R_3\}. \\
&= \{(a, c_2), (a, d), (a, f_1) : \text{there is a } b, c_1, e_1 \text{ with } (a, b), (a, c_1), (a, e_1) \in R_1 \text{ and} \\
&\quad (b, c_2), (c_1, d), (e_1, f_1) \in R_2\} \cap \{(a, c_2), (a, d), (a, f_2) : \text{there is a } b, c_1, e_2 \text{ with} \\
&\quad (a, b), (a, c_1), (a, e_2) \in R_1 \text{ and } (b, c_2), (c_1, d), (e_1, f_2) \in R_3\} \\
&= (R_1; R_2) \cap (R_1; R_3).
\end{aligned}$$