**Problem 1** (33 marks)

For $x, y \in \mathbb{Z}$, we define the set

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

a) Prove that for all $m, n, x, y, z \in \mathbb{Z}$, if $z|x$ and $z|y$ then $z|(mx + ny)$. 4 marks

b) Prove that 2 is the smallest positive element of $S_{4,6}$.

*Hint: To show that the element is the smallest, you will need to show that some values cannot be obtained. Use the fact proven in part (a)* 4 marks

c) Find the smallest positive element of $S_{-6,15}$. 4 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 $S_{x,y}$.

d) Prove that $S_{x,y} \subseteq \{n \in \mathbb{Z} : d|n\}$. 4 marks

e) Prove that $d \leq z$. 3 marks

f) Prove that $z|x$ and $z|y$.

*Hint: consider* $(x\%z)$ *and* $(y\%z)$ 8 marks

g) Prove that $z \leq d$. 2 marks

h) Using the answers from (e) and (g), explain why $S_{x,y} \supseteq \{n \in \mathbb{Z} : d|n\}$ 4 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. Two useful consequences of Bézout's identity are:

- If $c|x$ and $c|y$ then $c|\gcd x, y$ (i.e. $\gcd(x, y)$ is a multiple of all common factors of $x$ and $y$)
- If $\gcd(x, y) = 1$, then there is a unique $w \in [0, y)$ such that $xw =_{(y)} 1$ (i.e. multiplicative inverses exist in modulo $y$, if $x$ is coprime with $y$)

**Solution**

a) Given that $z|x$, there exists an integer $a$ such that $x = az$. Similarly, since $z|y$, there exists an integer $b$ such that $y = bz$. We aim to show that $z|(mx + ny)$.

Consider the expression $mx + ny$:

$$\begin{aligned} mx + ny &= m(az) + n(bz) \\ &= maz + nbz \\ &= z(ma + nb). \end{aligned}$$

Since $ma + nb$ is an integer (as integers are closed under addition and multiplication), it follows that $mx + ny$ can be expressed as $z$ times an integer, $z(ma + nb)$.

Therefore, by the definition of divisibility, we conclude that $z|(mx + ny)$. This demonstrates that if $z|x$ and $z|y$, then $z|(mx + ny)$ for any integers $m, n, x, y, z$.

b) Setting $x = -1$ and $y = 1$ gives $mx + ny = -4 + 6 = 2$ proving 2 belongs to $S_{4,6}$. Given that 1 is the only positive integer smaller than 2, it suffices to show that $1 \notin S_{x,y}$. Since 4 and 6 are divisible by 2, according to $a)$ any integer of the form $4x + 6y$ must be divisible by 2. Since 1 is not divisible by 2, it cannot belong to $S_{x,y}$.

c) Set $x = 2$ and $y = 1$ to find 3. Using the same argument as in $b)$ show that 1 and 2 do not belong to $S_{x,y}$.

d) $d|x$ and $d|y$, so $d|(mx+ny)$ for any integers $m, n$. Therefore, if $w \in S_{x,y}$, $d|w$. So $S_{x,y} \subseteq \{n : n \in \mathbf{Z} \text{ and } d|n\}$.

e) $z \in S_{x,y}$ so $d|z$, that is $z = kd$ for some integer $k$. If $z = 0$ then, as $\pm x, \pm y \in S_{x,y}$ it follows that $x = y = 0$ and hence $d = 0$. Otherwise $z > 0$, and as $d$ is a non-negative integer, we have that $k \geq 0$. In both cases, $d \leq z$.

f) Let $r = (x \% z)$ and $q = (x \text{ div } z)$. From the definition of these operations, we have $x = qz + r$, or $r = x - qz$. Since $z \in S_{x,y}$, $z = mx + ny$ for some $m, n \in \mathbb{Z}$. Therefore, $r = (1-m)x - ny$, so $r \in S_{x,y}$. From part $c$), we have that $0 \leq r < z$. From the minimality of $z$, it follows that $r = 0$ and hence $z|x$. Similarly $z|y$.

g) The previous question shows that $z$ is a common divisor of $x$ and $y$. Therefore, by the definition of gcd, $z \leq d$.

h) Since according to $e$) and $g$) we have $z \geq d$ and $z \leq d$, we can conclude that $z = d$. This means that $\{n \in \mathbf{Z} : d|n\} = \{n \in \mathbf{Z} : z|n\}$. Given that $z \in S_{x,y}$, there exist $m, n$ such that $mx + ny = z$. For any element $z' \in \{n \in \mathbf{Z} : z|n\}$ we can write $z' = az$ where $a \in \mathbf{Z}$. This gives $z' = az = (am)x + (an)y$ meaning that $z' \in S_{x,y}$, proving that $\{n \in \mathbf{Z} : z|n\} \subseteq S_{x,y}$.

---

**Problem 2** (16 marks)

Proof Assistant: https://cgi.cse.unsw.edu.au/~cs9020/cgi-bin/proof_assistant?A1

Prove, using the laws of set operations (and any results proven in lectures), the following identities hold for all sets $A, B, C$.

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

b) $(A \setminus C) \cup (B \setminus C) = (A \cup B) \setminus C$ — 4 marks

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

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

**Solution**

a)

$$\begin{aligned}
\emptyset &= A \cap A^c && \text{(Complementation)}\\
&= A \cap (A^c \cup \emptyset) && \text{(Identity)}\\
&= (A \cap A^c) \cup (A \cap \emptyset) && \text{(Distributivity)}\\
&= \emptyset \cup (A \cap \emptyset) && \text{(Complementation)}\\
&= A \cap \emptyset && \text{(Identity)}
\end{aligned}$$

b)

$$\begin{aligned}
(A \backslash C) \cup (B \backslash C) &= (A \cap C^c) \cup (B \cap C^c) && \text{(Definition of set difference)}\\
&= (A \cup B) \cap C^c && \text{(Distributivity)}\\
&= (A \cup C) \backslash C && \text{(Definition of set difference)}
\end{aligned}$$

c)

$$
\begin{aligned}
A \oplus \mathbf{U} &= (A \setminus \mathbf{U}) \cup (\mathbf{U} \setminus A) && \text{(Definition of symmetric set diffference)}\\
&= (A \cap \mathbf{U}^C) \cup (\mathbf{U} \cap A^c) && \text{(Definition of set difference)}\\
&= (A \cap \emptyset) \cup (\mathbf{U} \cap A^c) && \text{(Uniqueness of complement)}\\
&= \emptyset \cup A^c && \text{(Identity from a)}\\
&= A^c && \text{(Identity)}
\end{aligned}
$$

d) The duality principle applied to part $a$) gives us $\mathbf{U} = A \cup \mathbf{U}$.

The uniqueness of the complement means that if $(A^c \cup B^c) \cup (A \cap B) = \mathbf{U}$ and $(A^c \cup B^c) \cap (A \cap B) = \emptyset$ then $(A \cap B)^c = A^c \cup B^c$.

$$
\begin{aligned}
(A^c \cup B^c) \cup (A \cap B) &= (A^c \cup B^c \cup A) \cap (A^c \cup B^c \cup B) && \text{(Distributivity)}\\
&= (A^c \cup A \cup B) \cap (A^c \cup B^c \cup B) && \text{(Commutativity)}\\
&= (\mathbf{U} \cup B) \cap (A^c \cup \mathbf{U}) && \text{(Complementation)}\\
&= \mathbf{U} \cap \mathbf{U} && \text{(Dual of identity from a)}\\
&= \mathbf{U} && \text{(Identity)}
\end{aligned}
$$

$$
\begin{aligned}
(A^c \cup B^c) \cap (A \cap B) &= (A^c \cap A \cap B) \cup (B^c \cap A \cap B) && \text{(Distributivity)}\\
&= (A^c \cap A \cap B) \cup (A \cap B^c \cap B) && \text{(Commutativity)}\\
&= (\emptyset \cap B) \cup (A^c \cap \emptyset) && \text{(Complementation)}\\
&= \emptyset \cup \emptyset && \text{(Identity from a)}\\
&= \emptyset && \text{(Identity)}
\end{aligned}
$$

---

**Problem 3** (26 marks)

Let $\Sigma = \{a, b\}$, and let

$$L_2 = (\Sigma^{=2})^* \qquad \text{and} \qquad L_3 = (\Sigma^{=3})^*.$$

a) Give a complete description of $\Sigma^{=2}$ and $\Sigma^{=3}$; and an informal description of $L_2$ and $L_3$. 4 marks

b) Prove that for all $w \in L_1$, $length(w) =_{(2)} 0$. 4 marks

c) Show that $\Sigma^2$ and $\Sigma^3$ give a counter-example to the proposition that for all sets $X, Y \subseteq \Sigma^*$, $(X \cap Y)^* = X^* \cap Y^*$. 4 marks

d) Prove that:

$$L_2 \cap L_3 = (\Sigma^{=6})^*$$

8 marks

e) Using the observation that every natural number $n \geq 2$ is either even or 3 more than a non-negative even number, prove that:

$$L_2 L_3 = \Sigma^* \setminus \{a, b\}$$

6 marks

**Solution**

a) $\Sigma^{=2} = \{aa, ab, bb, ba\}$, $\Sigma^{=3} = \{aaa, aab, aba, abb, baa, bab, bba, bbb\}$. Informally $L_2$ corresponds to concatenating 0 or more words from $\Sigma^{=2}$. $L_3$ corresponds to concatenating 0 or more words from $\Sigma^{=3}$.

b) Since a word $w \in L_2$ consists of the concatenation of an arbitrary number of word of length 2. If $w = \lambda$ then the condition is satisfied since $length(\lambda) = 0$. Otherwise $w$ can be written as $u_1 \ldots u_n$ with $n \geq 1$ and $\forall i \leq n, u_i \in \Sigma^{=2}$ and hence $length(u_i) = 2$ for all $i \leq n$. This implies $length(w) = length(u_1) + \ldots + length(u_n) = 2n$ which modulo 2 is 0.

c) We can prove that $aaaaaa$ belongs in $\left(\Sigma^2\right)^*$ and $\left(\Sigma^3\right)^*$ since it can be written as the concatenation of $aa$ 3 times or $aaa$ 2 times. It therefore belongs to $X^* \cap Y^*$. $\Sigma^2 \cap \Sigma^3 = \emptyset$ (we can check from answer a)), therefore $\left(\Sigma^2 \cap \Sigma^3\right)^* = \{\lambda\}$ which does not contain $aaaaaa$.

d) We proved in part $b)$ that $w \in L_2 \implies length(w) =_{(2)} 0$. Similarly we can show that $w \in L_3 \implies length(w) =_{(3)} 0$. For a word to be contained in the intersection of both languages, its length must be divisible by both 2 and 3. $lcm(2,3) = 6$ and therefore all words in $L_2 \cap L_3$ are of length divisible by 6, giving $L_2 \cap L_3 \subseteq \left(\Sigma^6\right)^*$. The language $L_2$ contains all strings of length divisible by 2 and therefore all strings of length divisible by 6. $L_3$ all strings of length divisible by 3 and therefore all strings of length divisible by 6. Their intersection must thus contain all strings of length divisible by 6, giving $\left(\Sigma^6\right)^* \subseteq L_2 \cap L_3$, proving the equality.

e) Rewrite $\Sigma^* \backslash \{a, b\}$ as $\{\lambda\} \cup \Sigma^{\geq 2}$. $\lambda$ is contained on both sides since $\lambda \in L_2$ and $\lambda \in L_3$, meaning $\lambda\lambda = \lambda \in L_2L_3$ and $\lambda \in \{\lambda\} \cup \Sigma^{\geq 2}$.

Using the given observation, any non-empty word $w \in \Sigma^{\geq 2}$ can be written as $uv$ where $length(u) =_{(2)} 0$ and $length(v) = 0$ or $length(v) = 3$. This implies that $u \in L_2$ and $v \in L_3$ and therefore $w = uv \in L_2L_3$. This along with the statement about the $\lambda$ implies $\{\lambda\} \cup \Sigma^{\geq 2} \subseteq L_2L_3$.

Now given any non-empty $w \in L_2L_3$, we can write $w = uv$ where $u \in L_2$ and $v \in L_3$. Since $length(w) > 0$, we must have either $length(u) \geq 2$ or $length(v) \geq 3$, and can conclude that $length(w) \geq 2$. Since $\Sigma^{\geq 2}$ contains all words of length greater than 2, $w \in \Sigma^{\geq 2}$. This along with the statement about $\lambda$ implies $L_2L_3 \subseteq \{\lambda\} \cup \Sigma^{\geq 2}$, proving the equality.