Solutions to Exam I

Problem 1. a) State all 9 axioms about addition and multiplication (4 about $+$, 4 about $\cdot$ and one connecting $+$ and $\cdot$.) (7 points)

b) Using only the axioms for $+$ prove that if $a + c = b + c$ then $a = b$. (6 points)

c) Using only the axioms prove that $0 \cdot a = 0$ for any a. Hint. $0 + 0 = 0$. (6 points)

Solution: a) We consider a set R on which two operations $+$ (addition) and $\cdot$ (multiplication) are defined and two **different** elements 0 and 1 are distinguished. We impose the following axioms. There are 4 axioms about addition:
A1 (commutativity of addition): $a + b = b + a$ for any $a, b \in R$.
A2 (associativity of addition): $(a + b) + c = a + (b + c)$ for any $a, b, c \in R$.
A3 (identity for addition): $a + 0 = a$ for any $a \in R$.
A4 (additive inverse): for any $a \in R$ there exists $-a \in R$ such that $a + (-a) = 0$.

There are 4 axioms about multiplication:
M1 (commutativity of multiplication): $a \cdot b = b \cdot a$ for any $a, b \in R$.
M2 (associativity of multiplication): $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for any $a, b, c \in R$.
M3 (identity for multiplication): $a \cdot 1 = a$ for any $a \in R$.
M4 (no zero divisors): for any $a, b \in R$, if $a \cdot b = 0$ then $a = 0$ or $b = 0$.

Finally there is an axiom connecting addition and multiplication:
D (distributivity of multiplication over addition): $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$.

Remark. (i) Any R as above for which all axioms are satisfied except possibly M4 is called a **commutative ring**. If it satisfies also M4, then it is called an **integral domain**.
(ii) Assuming that all the other axioms hold, M4 is equivalent to the following axiom:
M41 (cancellation for multiplication): For any $a, b, c \in R$, if $a \neq 0$ and $a \cdot b = a \cdot c$ then $b = c$.

b) Suppose that $a + c = b + c$. Adding $-c$ to both sides we get $(a + c) + (-c) = (b + c) + (-c)$. Using associativity of addition, the last equality can be stated as $a + (c + (-c)) = b + (c + (-c))$. By definition of $-c$, we have $c + (-c) = 0$. It follows that $a + 0 = b + 0$. By identity of addition, we get $a + 0 = a$ and $b + 0 = b$. It follows that $a = b$.

c) Let $a \in R$. Multiplying the equality $0 + 0 = 0$ by a we get $(0 + 0) \cdot a = 0 \cdot a$. Using distributivity, we conclude that $(0 \cdot a) + (0 \cdot a) = 0 \cdot a$. By identity for addition, we can write the last equality as $(0 \cdot a) + (0 \cdot a) = 0 + (0 \cdot a)$. By part b), we conclude that $0 \cdot a = 0$.

Problem 2. a) State the axioms about the set of positive elements $\mathbb{N}$. (7 points)

b) What does it mean that $a < b$? (4 points)

c) Prove using only the axioms and the definition in b) that if $0 < a$ and $ab < ac$ then $b < c$. Do a "proof by contradiction". (7 points)

Solution: a) Assume that R satisfies all the 9 axioms stated in Problem 1 a). We add the following axiom for positive elements:

P (positive elements): There is a subset $\mathbb{N}$ of R (elements of which are called positive) with the following properties:
P1 (closure under addition): If a and b are in $\mathbb{N}$ then $a+b \in \mathbb{N}$.
P2 (closure under multiplication): If a and b are in $\mathbb{N}$ then $a \cdot b \in \mathbb{N}$.
P3: $0 \notin \mathbb{N}$.
P4 (trichotomy): For any $a \in R$ one of the following holds: $a \in \mathbb{N}$, or $-a \in \mathbb{N}$, or $a = 0$.

b) By definition, $a < b$ means that $b - a \in \mathbb{N}$.

c) Suppose that $0 < a$ and $ab < ac$. In other words, $a \in \mathbb{N}$ and $ac - ab \in \mathbb{N}$. We want to prove that $b < c$. Suppose that this is not true. This means that $c - b \notin \mathbb{N}$. By trichotomy (axiom P4), we get that either $-(c-b) \in \mathbb{N}$ or $c - b = 0$.

Suppose first that $c - b = 0$. It follows that $b = c$, so $ab = ac$. This means that $ac - ab = 0$ so $ac - ab \notin \mathbb{N}$ by axiom P3. This however contradicts the condition that $ac - ab \in \mathbb{N}$. The contradiction shows that the case $c - b = 0$ is not possible.

It remains to consider the case when $-(c-b) \in \mathbb{N}$. This means that $b - c \in \mathbb{N}$. Since $a \in \mathbb{N}$, the closure under multiplication axiom yields that $a(b-c) = ab - ac \in \mathbb{N}$. Thus we have both $ac - ab \in \mathbb{N}$ and $ab - ac \in \mathbb{N}$. The closure under addition axiom implies that $(ab - ac) + (ac - ab) = 0 \in \mathbb{N}$. This however contradicts axiom P3. The contradiction proves that our assumption that $b < c$ does not hold is false. Thus $b < c$ is true.

Problem 3. a) State the Induction axiom. (5 points)

b) A sequence is defined recursively as follows: $a_0 = 2$, $a_1 = 3$, $a_{n+1} = 3a_n - 2a_{n-1}$ for $n \geq 1$. Prove by induction that $a_n = 2^n + 1$ for every integer $n \geq 0$. (7 points)

c) Prove by induction that $\sum_{k=1}^{n}(2k-1) = n^2$ for every natural number n. (7 points)

Solution: a) Suppose that $R = \mathbb{Z}$ satisfies all the axioms from problem 1 a) and that $\mathbb{N}$ is a subset of R which satisfies the axioms from problem 2 a). We add the following axiom:

I (induction axiom): Any subset S of $\mathbb{Z}$ such that $1 \in S$ and whenever $a \in S$ then also $a + 1 \in S$ contains the set $\mathbb{N}$.

b) We prove that $a_n = 2^n + 1$ by induction on n. For $n = 0$ we have $a_0 = 2 = 2^0 + 1$, so the result is true for $n = 0$. Furthermore, $a_1 = 3 = 2^1 + 1$, so the result is true for $n = 1$. Assume that $n \geq 1$ and that the result is true for $0, 1, \ldots, n$. We need to prove that the result holds for $n + 1$. By definition, we have $a_{n+1} = 3a_n - 2a_{n-1}$. By inductive assumption, $a_n = 2^n + 1$ and $a_{n-1} = 2^{n-1} + 1$. Thus

$$a_{n+1} = 3(2^n + 1) - 2(2^{n-1} + 1) = 3 \cdot 2^n + 3 - 2^n - 2 = 2 \cdot 2^n + 1 = 2^{n+1} + 1,$$

so the result indeed holds for $n + 1$. By the method of induction, the result is true for every integer $n \geq 0$.

c) We prove that $\sum_{k=1}^{n}(2k-1) = n^2$ by induction on n. When $n = 1$, both the left hand side and the right hand side are 1 so the result holds. Suppose that $n \geq 1$ and the result holds for $1, 2, \ldots, n$. We need to prove the result for $n + 1$, i.e. we need to prove that $\sum_{k=1}^{n+1}(2k-1) = (n+1)^2$. Note that

$\sum_{k=1}^{n+1}(2k-1) = \sum_{k=1}^{n}(2k-1) + (2(n+1)-1) = \sum_{k=1}^{n}(2k-1) + (2n+1)$. By the inductive assumption, we have $\sum_{k=1}^{n}(2k-1) = n^2$ and therefore $\sum_{k=1}^{n+1}(2k-1) = n^2 + (2n+1) = (n+1)^2$, so the result holds for $n+1$. By the method of induction, the result holds for every natural number n.

Problem 4. a) Define the symmetric difference $A \div B$ of two sets. State basic properties of this operation. (5 points)

Solve two of the following three problems.

b) Prove that $(A \setminus B) \cap (C \setminus D) = (A \cap C) \setminus (B \cup D)$. (7 points)

c) Use membership table to prove that $(A \setminus B) \div (A \setminus C) = A \cap (B \div C)$. (7 points)

d) Express each side of the equality

$$(A \setminus B) \cup (B \setminus C) = (A \cup B) \setminus (B \cap C)$$

using only the operation $+$ of symmetric difference and $\cdot$ of intersection. Recall that $X \setminus Y = X + XY$ and $X \cup Y = X + Y + XY$. Then verify that both sides are indeed equal. (7 points)

Solution: a) By definition, $A \div B = (A \setminus B) \cup (B \setminus A)$. In other words, $x \in A \div B$ if and only if x is in either A or B but not both. Thus $A \div B = (A \cup B) \setminus (A \cap B)$. Among the properties of the symmetric difference we have the following:

(1) $A \div B = B \div A$.
(2) $(A \div B) \div C = A \div (B \div C)$.
(3) $A \div \emptyset = A$.
(4) $A \div A = \emptyset$.
(5) $(A \div B) \cap C = (A \div C) \cap (B \div C)$.

b) Note that $x \in (A \setminus B) \cap (C \setminus D)$ if and only if $x \in (A \setminus B)$ and $x \in (C \setminus D)$, which is equivalent to the conditions $x \in A$ and $x \notin B$ and $x \in C$ and $x \notin D$, which in turn is equivalent to the conditions $x \in A$ and $x \in C$ and $x \notin B$ and $x \notin D$ which is equivalent to $x \in (A \cap C)$ and $x \notin (B \cup D)$, which is equivalent to $x \in (A \cap C) \setminus (B \cup D)$. Thus the sets $(A \setminus B) \cap (C \setminus D)$ and $(A \cap C) \setminus (B \cup D)$ have the same elements and therefore they are equal.
Remark. One can also solve this problem using methods employed in parts c) or d).

c)

A	B	C	$A \setminus B$	$A \setminus C$	$(A \setminus B) \div (A \setminus C)$	$B \div C$	$A \cap (B \div C)$
1	1	1	0	0	0	0	0
1	1	0	0	1	1	1	1
1	0	1	1	0	1	1	1
1	0	0	1	1	0	0	0
0	1	1	0	0	0	0	0
0	1	0	0	0	0	1	0
0	0	1	0	0	0	1	0
0	0	0	0	0	0	0	0

Since the columns for $(A\setminus B)\div(A\setminus C)$ and $A\cap(B\div C)$ are equal, we conclude that $(A\setminus B)\div(A\setminus C) = A\cap(B\div C)$.

Remark. The first three columns of the table describe all possible membership patterns. For example, the first row corresponds to elements which belong to all three sets A, B, C, and the 4th row corresponds to elements which belong to A but do not belong to B or C. The second part of the table is then filled by going through each row and putting 1 if the elements described by the first part of the row belong to the set naming a given column and putting 0 if they do not belong to this set. For example, in the second row in the column for $A\setminus C$ we put 1, since elements in this row belong to A, B but not C so they belong to $A\setminus C$.

d) We have

$$(A\setminus B)\cup(B\setminus C) = (A+AB)+(B+BC)+(A+AB)(B+BC) = A+AB+B+BC+AB+ABC+ABB+$$
$$+ABBC = A+B+AB+BC+AB+AB+ABC+ABC = A+B+AB+BC.$$

(we use the properties $X+X=0$ and $XX=X$). Similarly,

$$(A\cup B)\setminus(B\cap C) = (A+B+AB)+(A+B+AB)BC = A+B+AB+ABC+BBC+ABBC =$$
$$= A+B+AB+BC+ABC+ABC = A+B+AB+BC.$$

We see that both $(A\setminus B)\cup(B\setminus C)$ and $(A\cup B)\setminus(B\cap C)$ are equal to $A+B+AB+BC$, hence they are equal to each other.

Problem 5. This problem is optional. You may earn 15 extra points. A set A consists of $2n$ elements. A is split into disjoint pieces B and C, each with n elements.

a) What is the number of subsets of A which contain s elements in B and $n-s$ elements in C?

b) Prove that $\displaystyle\sum_{s=0}^{n}\binom{n}{s}\binom{n}{n-s} = \binom{2n}{n}$. Conclude that $\displaystyle\sum_{s=0}^{n}\binom{n}{s}^2 = \binom{2n}{n}$.

Solution: a) We proved that a set with n elements has $\binom{n}{k}$ subsets with exactly k elements. Thus we can choose the s elements from B in $\binom{n}{s}$ ways and to each such choice we can choose $n-s$ elements from B in $\binom{n}{n-s}$ ways. It follows that we have $\binom{n}{s}\binom{n}{n-s}$ choices for a subset of A which has s elements in B and $n-s$ elements in C.

b) Let us count the number of subsets of A with exactly n elements in two ways. On one hand, we know that this number is equal to $\binom{2n}{n}$. On the other hand, every subset with n elements consists of s elements from B and $n-s$ elements from C, for some $s\in\{0,1,\ldots,n\}$. For a given s we have $\binom{n}{s}\binom{n}{n-s}$ such subsets, as proved in part a). Thus the total number of subsets of A with n elements is equal to $\displaystyle\sum_{s=0}^{n}\binom{n}{s}\binom{n}{n-s}$. This proves that $\displaystyle\sum_{s=0}^{n}\binom{n}{s}\binom{n}{n-s} = \binom{2n}{n}$. Note that $\binom{n}{n-s} = \binom{n}{s}$ for all s. It follows that $\displaystyle\sum_{s=0}^{n}\binom{n}{s}\binom{n}{n-s} = \sum_{s=0}^{n}\binom{n}{s}^2$, so $\displaystyle\sum_{s=0}^{n}\binom{n}{s}^2 = \binom{2n}{n}$.