Math 437/537—Group Work #1—Solutions
Tuesday, September 17, 2024

There are a few subsidiary facts that follow from the axioms and that prove useful when solving these problems; we gather those subsidiary facts here.

- Notice that if we take $a = 0$ in Axiom 15, we get the statement "for all $b, c \in \mathbb{Z}$, if $0 < b$ and $0 < c$, then $0 < bc$" (since $0c = 0$ by Axiom 10). In other words, the product of two positive integers is again positive. Similarly, if we take $b = 0$ in Axiom 15, we get the statement "for all $a, c \in \mathbb{Z}$, if $a < 0$ and $0 < c$, then $ac < 0$"; in other words, the product of a positive integer and a negative integer is negative.
- Notice also that Axiom 15 contains strict inequalities. However, the variant of Axiom 15 with nonstrict inequalities—namely, "for all $a, b, c \in \mathbb{Z}$, if $a \le b$ and $0 \le c$, then $ac \le bc$"—is also true. It follows from the given Axiom 15 by just checking the new possibilities $a = b$ (multiplication is well-defined) or $c = 0$ (Axiom 10).
- Finally, let -1 be the additive inverse (in the sense of Axiom 5) of 1. Note that for any integer b,

  $$0 = 0b = (1 + (-1))b = 1b + (-1)b = b + (-1)b,$$

  where the equalities follow from Axioms 10, 5, 11, and 9, respectively. Adding $-b$ to both sides, where $-b$ denotes the additive inverse of b, gives

  $$-b = (-b) + 0 = (-b) + \big(b + (-1)b\big) = \big((-b) + b\big) + (-1)b = 0 + (-1)b = (-1)b,$$

  where the equalities follow from Axioms 4, 1, 2, 5, and 4. In other words, we have shown that $-b = (-1)b$; that is, additive inverses are unique and can be obtained by multiplying by the special number -1.

1. *If a and b are positive integers with $a \mid b$, show that $a \le b$. You may assume, for the moment, that there is no integer between 0 and 1.*

Since $a \mid b$, there exists an integer m such that $am = b$. Note that both a and $am = b$ are positive by assumption; in particular, m cannot be negative, since then b would be negative (by the first subsidiary fact above), and Axiom 12 says that an integer cannot be both positive and negative. Similarly, if $m = 0$ then $b = am = a0 = 0$ by Axiom 10, again contradicting Axiom 12 since b is known to be positive. Since $m < 0$ and $m = 0$ are both impossible, we conclude from Axiom 12 that $m > 0$.

Knowing that $m > 0$, we use the assumption that there is no integer between 0 and 1 to conclude that $m \ge 1$. Multiplying both sides by a yields $b = am \ge a$, by the nonstrict variant of Axiom 15 discussed above.

2. *Prove that there is no integer between 0 and 1. You may assume, for the moment, that $1 > 0$.*

Suppose, for the sake of contradiction, that there exists an integer s with $0 < s < 1$ (where we have used the assumption that $0 < 1$). There are two related ways to use Axiom 16 (well-ordering) to derive a contradiction:

(a) Consider the infinite set $S = \{s, s^2, s^3, \cdots\}$ of integers; all of these integers are positive, by repeated use of the first subsidiary fact above. By Axiom 16, S has a least element, say

s^k. But multiplying the inequality $s < 1$ by the positive integer s^k yields $s^{k+1} < s^k$ (using Axiom 9 for the right-hand side), which contradicts the fact that s^k is the smallest element of S.

(b) Alternatively, consider the set E of positive integers less than 1. Suppose, for the sake of contradiction, that E is nonempty. Then E possesses a least element e by Axiom 16. But multiplying the inequalities $0 < e < 1$ by the positive integer e yields $0 < e^2 < e$ (using our positive-times-positive-equals-positive fact for the left-hand side and Axiom 15 for the left-hand side), which shows that $e^2 \in E$ and thus contradicts the fact that e is the smallest element of E.

3. *Prove that* $1 > 0$.

By Axiom 12, exactly one of the three statements $0 < 1$, $0 = 1$, and $0 > 1$ is true; but it can't be $0 = 1$ by Axiom 9. So all we have to do is prove that $0 > 1$ is impossible. Suppose, for the sake of contradiction, that $0 > 1$. Let -1 denote an additive inverse of 1; applying Axiom 14 to $0 > 1$ yields $0 + (-1) > 1 + (-1)$, or $-1 > 0$ by Axiom 4 and Axiom 5. Then $(-1)(-1) > 0$ by Axiom 15. But $(-1)(-1) = 1$ by the third subsidiary fact discussed above, and so $1 > 0$, which is a contradiction to our assumption that $0 > 1$.

(A related approach is to use the axioms to show that for any nonzero integer a, exactly one of a and $-a$ is positive. One can then show that a^2 is positive for any nonzero integer a. Finally, given the existence of a positive integer b, multiplying the inequality $0 < b$ by 1 gives $0 < b$—which rules out the possibility that 1 is negative, by the first subsidiary fact above.)

The Axioms for the Integers

The following are the axioms of $\mathbb{Z}$. They relate to the addition, multiplication and the order relation ($<$) in $\mathbb{Z}$.

Axiom 1 (AE)**.** If $a, b \in \mathbb{Z}$, then the sum $a + b$ is uniquely defined element in $\mathbb{Z}$.

Axiom 2 (AA)**.** For all $a, b, c \in \mathbb{Z}$ we have $a + (b + c) = (a + b) + c$.

Axiom 3 (AC)**.** For all $a, b \in \mathbb{Z}$ we have $a + b = b + a$.

Axiom 4 (AZ)**.** There is an element 0 in $\mathbb{Z}$ such that $0+a = a+0 = a$ for all $a \in \mathbb{Z}$.

Axiom 5 (AO)**.** If a is an element of $\mathbb{Z}$, then the equation $a + x = 0$ has a solution $-a \in \mathbb{Z}$.

Axiom 6 (ME)**.** If $a, b \in \mathbb{Z}$, then the product $a \cdot b$ (usually denoted by ab) is uniquely defined element in $\mathbb{Z}$.

Axiom 7 (MA)**.** For all $a, b, c \in \mathbb{Z}$ we have $a(bc) = (ab)c$.

Axiom 8 (MC)**.** For all $a, b \in \mathbb{Z}$ we have $ab = ba$.

Axiom 9 (MO)**.** There is an element 1 in $\mathbb{Z}$ such that $1 \neq 0$ and $1 \cdot a = a \cdot 1 = a$ for all $a \in \mathbb{Z}$.

Axiom 10 (MZ)**.** For all $a, b \in \mathbb{Z}$, $ab = 0$ if and only if $a = 0$ or $b = 0$.

Axiom 11 (DL)**.** For all $a, b, c \in \mathbb{Z}$ we have $a(b + c) = ab + ac$.

Axiom 12 (OE)**.** If $a, b \in \mathbb{Z}$, then exactly one of the following three statements is true: $a < b$ or $a = b$, or $b < a$.

Axiom 13 (OT)**.** For all $a, b, c \in \mathbb{Z}$, if $a < b$ and $b < c$, then $a < c$.

Axiom 14 (OA)**.** For all $a, b, c \in \mathbb{Z}$, if $a < b$, then $a + c < b + c$.

Axiom 15 (OM)**.** For all $a, b, c \in \mathbb{Z}$, if $a < b$ and $0 < c$, then $ac < bc$.

Axiom 16 (WO)**.** If S is a nonempty set of positive integers, then there exists $m \in S$ such that $m \leq x$ for all $x \in S$.

Explanation of abbreviations: AE - addition exists, AA - addition is associative, AC - addition is commutative, AZ - addition has zero, AO - addition has opposites, ME - multiplication exists, MA - multiplication is associative, MC - multiplication is commutative, MO - multiplication has one, MZ - multiplication respects zero, DL - distributive law, OE - order exists, OT - order is transitive, OA - order respects addition, OM - order respects multiplication, WO - this is so called the well ordering axiom.