Abstract Algebra

August, Evelyn

11/30/2021

$\boxed{\text{11: proposition}}$ Given a ring R and elements $a, b, c \in \mathbb{R}$ the following are true (in the last two, assume that R is a ring with unity)

3 $(-a)(-b) = ab$

4 $a(b-c) = ab - ac$ and $(b-c)a = ba - ca$.

5 $(-1)a = -a$

6 $(-1)(-1) = 1$

$\boxed{\text{proof}}$ Let R be a ring and let a, b, c be arbitrary elements in R. For 5 and 6 let R be a ring with unity.

3 We want to show that $(-a)(-b) = ab$. By property 2, $a(-b) = -(ab)$. Applying property 2 again, $(-a)(-b) = -(-(ab))$. It remains to be shown that $-(-(ab)) = ab$. This is clearly the case, as $ab + (-ab) = ab - ab = 0$, so this follows from the definition of the additive inverse.

4 We want to show that $a(b-c) = ab - ac$. It follows that $a(b-c) = a(b + (-c))$ from the definition of subtraction notation. By property six of rings, this is just $ab + a(-c)$. Applying property 2, this is $ab + (-ac)$, which by the notational convention is just $ab - ac$. Likewise for $(b-c)a$.

5 We want to show that $(-1)a = -a$ (1 being the unity of R). To show this, consider $a + (-1)a$. By property 2, $(-1)a = -(1a)$. By definition of the multiplicative identity, $1a = a$. Substituting, we have $-(1a) = -a$. Substituting again, $a + (-1)a = a - (1a) = a - a$. By definition of the additive inverse, $a - a = 0$. Hence $(-1)a$ is the additive inverse of a, which is $-a$.

6 We want to show that $(-1)(-1) = 1$, where 1 is the unity of R. Consider $(-1)(-1) - 1$. Then, it follows by properties of rings that $(-1)(-1) + (-1) \cdot 1 = (-1)(-1+1) = (-1) \cdot 0 = 0$. Thus $(-1)(-1)$ is the additive inverse of 1, which is -1.

$\boxed{\text{27: proposition}}$ The units of a [commutative] ring divides every element in the ring.

$\boxed{\text{proof}}$ Let R be a ring and let $u \in U(R) \subseteq R$. By the properties of rings there exists some element $1 \in R$ that acts as the multiplicative identity. Then by definition of the units, there exists some $u^{-1} \in R$ such that $uu^{-1} = 1$. Let $a \in R$ be arbitrary. By definition of the multiplicative identity it follows that $1a = a$. Substituting, $(uu^{-1})a = a$. By the associative law of multiplication in rings, $(uu^{-1})a = u(u^{-1}a) = a$. Since $u^{-1}, a \in R$, it follows by the closure of multiplication in a ring that $q = u^{-1}a \in R$. Hence $a = uq$ for some $q \in R$, so by definition of divisibility $u|a$. Since a is arbitrary in R it follows that u divides each element in R. Hence the units of a commutative ring divide every element in the ring. Q.E.D.

$\boxed{\text{43: problem}}$ Let $R = Z \oplus Z \oplus Z$ and $S = \{(a, b, c) \in R | a + b = c\}$. Prove or disprove that S is a subring of R.

$\boxed{\text{solution}}$ Consider the following elements in R: $x = (1, 0, 1)$ and $y = (0, 1, 1)$. We know that $x, y \in R$, since $1+0 = 1$ and $0+1 = 1$. Consider $xy = (1, 0, 1)(0, 1, 1) = (1\cdot 0, 0\cdot 1, 1\cdot 1) = (0, 0, 1)$. However, xy is not an element in R, since $0 + 0 \neq 1$. Thus, S is not a subring of R.