ETH Zürich, D-INFK
HS 2020, 25. November 2020

Prof. Ueli Maurer
David Lanzenberger

Diskrete Mathematik

Solution 10

10.1 Elementary Properties of Rings

a) We have

$$(-a)b + ab \overset{\text{distrib.}}{=} (-a+a)b \overset{\text{def. inverse}}{=} 0b \overset{\text{Lemma 5.17 (i)}}{=} 0.$$

Therefore, $(-a)b$ is the additive inverse of ab, which means that $(-a)b = -ab$.

b) We have

$$(-a)(-b) + (-(ab)) \overset{\text{a)}}{=} (-a)(-b) + (-a)b \overset{\text{distrib.}}{=} (-a)(-b+b) \overset{\text{def. inverse}}{=} (-a)0 \overset{\text{Lemma 5.17 (i)}}{=} 0.$$

Therefore, $(-a)(-b)$ is the additive inverse of $-(ab)$, which means that $(-a)(-b) = -(-(ab)) = ab$.

10.2 Properties of Commutative Rings

a) From $a|b$ it follows that $\exists d\ b = ad$ and, thus, $bc = (ad)c = a(dc)$. Hence, $a|bc$.

b) From $a|b$ it follows that $\exists d\ b = ad$ and from $a|c$ it follows that $\exists e\ c = ae$. By the distributive law, we have $b + c = ad + ae = a(d + e)$. Hence, $a|(b + c)$.

10.3 Ideals in Rings

We show the implication in both directions.

$(\implies)$ Assume that $(a) = R$. This implies that $1 \in (a)$. By the definition of (a), this means that $1 = a \cdot r$ for some $r \in R$. This r is the inverse of a, so a is a unit.

$(\impliedby)$ Assume that a is a unit. This means that there exists $a^{-1} \in R$, such that $a \cdot a^{-1} = 1$. To show that $R \subseteq (a)$, we notice that for any $s \in R$, we have $s = 1 \cdot s = (a \cdot a^{-1}) \cdot s = a \cdot (a^{-1} \cdot s) = a \cdot r$, where $r \in R$. This implies that $s \in (a)$. Moreover, trivially, $(a) \subseteq R$. Hence, $(a) = R$.

10.4 Product of Rings

The neutral element of the operation $\oplus$ is $(0, 0)$. We further have $(1, 0) \otimes (0, 1) = (0, 0)$ and R being non-trivial implies $(1, 0) \neq (0, 0)$ and $(0, 1) \neq (0, 0)$. Hence, $R \times R$ has zero divisors. Since no integral domain can have zero divisors, $R \times R$ is not an integral domain.

10.5 A Ring with a Special Property

a) Let $x, y \in R$ be arbitrary. We choose $a = x + y$ to obtain

$$\begin{aligned} a + a^2 &= (x+y) + (x+y)^2 \\ &= (x+y) + (x+y)x + (x+y)y && \text{(distrib.)} \\ &= x + y + x^2 + yx + xy + y^2 && \text{(distrib.)} \\ &= (x + x^2) + (y + y^2) + xy + yx. && \text{(commut. +, assoc. +)} \end{aligned}$$

By assumption we have $(a^2 + a)b = b(a^2 + a)$ for any $b \in R$. For $b = x$ we obtain

$$\begin{aligned} &(a^2 + a)b = b(a^2 + a) \\ \iff &((x + x^2) + (y + y^2) + xy + yx)x = x((x + x^2) + (y + y^2) + xy + yx) \\ \overset{\text{(distr.)}}{\iff} &(x + x^2)x + (y + y^2)x + xyx + yx^2 = x(x + x^2) + x(y + y^2) + x^2y + xyx. \end{aligned}$$

Note that xyx appears on both sides of the equation, so we can subtract it on both sides. Moreover, by assumption we have $(x + x^2)x = x(x + x^2)$ and $(y + y^2)x = x(y+y^2)$, so we can subtract the two expressions on both sides of the equation. Hence, $x^2y = yx^2$.

b) Let $x, y \in R$ be arbitrary. By assumption we have $(x+x^2)y = y(x+x^2)$. Observe that

$$(x + x^2)y = y(x + x^2) \overset{\text{(distr.)}}{\iff} xy + x^2y = yx + yx^2.$$

Since by Subtask a) we have $x^2y = yx^2$, subtracting on both sides of the equation yields $xy = yx$.

10.6 Linear Equation over a Field

In order to solve the system of equations, we can use Gaussian elimination over F. The system can be expressed as the following matrix:

$$\begin{bmatrix} A & B & B & A \\ 1 & A & 1 & 0 \\ B & B & 1 & 1 \end{bmatrix}$$

First, we multiply the first row by the multiplicative inverse of A, which is B. We get:

$$\begin{bmatrix} 1 & A & A & 1 \\ 1 & A & 1 & 0 \\ B & B & 1 & 1 \end{bmatrix}$$

Note that in F every element is its own additive inverse, so subtraction (formally, adding the inverse of an element) is the same operation as addition. So, we can add the first row to the second row and get $\begin{bmatrix} 0, & 0, & B, & 1 \end{bmatrix}$. Then, we add the first row multiplied by B to the third row and get $\begin{bmatrix} B + (B \cdot 1), & B + (B \cdot A), & 1 + (B \cdot A), & 1 + (B \cdot 1) \end{bmatrix} = \begin{bmatrix} 0, & A, & 0, & A \end{bmatrix}$.

After swapping the third and the second row, we now get the following matrix:

$$\begin{bmatrix} 1 & A & A & 1 \\ 0 & A & 0 & A \\ 0 & 0 & B & 1 \end{bmatrix}$$

We multiply the second row by the multiplicative inverse of A and get and the third row by the multiplicative inverse of B and get:

$$\begin{bmatrix} 1 & A & A & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & A \end{bmatrix}$$

From the second and third rows we have $z = A$ and $y = 1$. Further, from the first row we get $x = 1 - (A \cdot y) - (A \cdot z) = 1 + A \cdot (y + z) = 1 + A \cdot B = 0$. Hence, the solution is $x = 0$, $y = 1$ and $z = A$.

10.7 Integral Domains and Fields

a) For example, $\mathbb{Z}$, $\mathbb{Z}[x]$, $\mathbb{Q}[x]$.

b) We have to prove that every $a \in D \setminus \{0\}$ is a unit. Let $a \in D \setminus \{0\}$ be arbitrary. We define the function $f_a : D \to D$ by $f_a(x) = a \cdot x$. We show that f_a is bijective:

injective: Assume that there exist $x, y \in D$ such that $f_a(x) = f_a(y)$ and $x \neq y$.

$$0 = f_a(y) - f_a(x) = a \cdot y - (a \cdot x) = a \cdot y + a \cdot (-x) = a \cdot (y - x),$$

where the third step follows from Lemma 5.17, and the last step uses the distributive law. Since by assumption $a \neq 0$ and $y - x \neq 0$, it follows that a is a zero-divisor, which is a contradiction with D being an integral domain.

surjective: If f_a was not surjective, we would have $y \notin Im(f_a)$ for some $y \in D$, which for finite D implies $|Im(f_a)| < |D|$. But since f_a is injective, the function $f'_a : D \to Im(f_a)$ defined by $f'_a(x) = f_a(x)$ is bijective, so $|Im(f_a)| = |D|$, which is a contradiction.

The inverse of a is $f_a^{-1}(1)$, because $a \cdot f_a^{-1}(1) = f_a(f_a^{-1}(1)) = 1$, hence, a is a unit.