ETH Zürich, D-INFK
HS 2020, 13. November 2020

Prof. Ueli Maurer
David Lanzenberger

Diskrete Mathematik

Exercise 10

Exercise 10.5 gives **bonus points**, which can increase the final grade. The solution to this exercise must be your own work. You may not share your solutions with anyone else. See also the note on dishonest behavior on the course website: `https://crypto.ethz.ch/teaching/DM20/`.

10.1 Elementary Properties of Rings ($\star\star$)

The goal of this exercise is to prove Lemma 5.17 (ii) and (iii). You can use only Lemma 5.17 (i), which is proved in the lecture notes. In Subtask b), you can use Subtask a).

Let $\langle R; +, -, 0, \cdot, 1\rangle$ be a ring and let $a, b \in R$. Show that:

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

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

10.2 Properties of Commutative Rings ($\star$)

The goal of this exercise is to prove Lemma 5.18 (ii) and (iii). You cannot use lemmas from the lecture notes.

Let $\langle R; +, -, 0, \cdot, 1\rangle$ be a commutative ring and let $a, b, c \in R$. Show that:

a) If $a|b$, then $a|bc$ for all c.

b) If $a|b$ and $a|c$, then $a|(b+c)$.

10.3 Ideals in Rings ($\star\star$)

We generalize ideals for the integers (Definition 4.4) to arbitrary rings. Let $\langle R; +, -, 0, \cdot, 1\rangle$ be a commutative ring. For $a \in R$, define the ideal $(a) = \{a \cdot r \mid r \in R\}$. Prove that $(a) = R$ if and only if a is a unit.

10.4 Product of Rings ($\star$)

Let $\langle R; +, \cdot\rangle$ be a non-trivial ring. Consider the algebra $\langle R \times R; \oplus, \otimes\rangle$ with the operations defined by

$$(a, b) \oplus (c, d) = (a + c, b + d)$$
$$(a, b) \otimes (c, d) = (a \cdot c, b \cdot d)$$

for all $(a, b), (c, d)$ in $R \times R$. Is it possible that $R \times R$ is an integral domain?

10.5 A Ring with a Special Property ($\star\star$) *(8 Points)*

Let $\langle R; +, \cdot \rangle$ be a ring, such that for all $a, b \in R$ we have

$$(a + a^2)b = b(a + a^2).$$

a) Prove that $x^2y = yx^2$ for all $x, y \in R$.

Hint: Instantiate the assumed property with $a = (x + y)$ and $b = y$.

b) Prove that R is commutative.

Hint: Use Subtask a) (you can use it even if you did not succeed in proving it).

10.6 Linear Equations over a Field ($\star$)

Consider the field $F = \{0, 1, A, B\}$ with 4 elements, described in Example 5.46. Solve the following system of linear equations over F:

$$\begin{aligned} A \cdot x + B \cdot y + B \cdot z &= A \\ x + A \cdot y + z &= 0 \\ B \cdot x + B \cdot y + z &= 1 \end{aligned}$$

10.7 Integral Domains and Fields

a) ($\star$) Recall an example of an integral domain that is not a field.

b) ($\star\star\star$) Prove that every finite integral domain D is a field.

Hint: For an $a \in D \setminus \{0\}$, consider the function $f_a(x) = a \cdot x$.

Due by 24. November 2020.
Exercise 10.5 is graded.