Prof. M. Einsiedler
Prof. P. Biran

Musterlösung Serie 3

1. **Linear system.** Using Gauss elimination, find all the solutions to the following system of linear equations over $\mathbb{R}$:

$$\begin{cases} x + 2y + 2z + w & = & -1 \\ 3x + 6y + 2z + 5w & = & 1 \end{cases}$$

Solution: This linear system can be represented by the augmented matrix

$$\left(\begin{array}{cccc|c} 1 & 2 & 2 & 1 & -1 \\ 3 & 6 & 2 & 5 & 1 \end{array}\right).$$

We proceed to row reduction on this matrix:

$$\left(\begin{array}{cccc|c} 1 & 2 & 2 & 1 & -1 \\ 3 & 6 & 2 & 5 & 1 \end{array}\right) \rightsquigarrow \left(\begin{array}{cccc|c} 1 & 2 & 2 & 1 & -1 \\ 0 & 0 & -4 & 2 & 4 \end{array}\right) \rightsquigarrow \left(\begin{array}{cccc|c} 1 & 2 & 2 & 1 & -1 \\ 0 & 0 & 1 & -1/2 & -1 \end{array}\right)$$

This leads to the equivalent system

$$\begin{cases} x + 2y + 2z + w & = & -1 \\ z - \frac{1}{2}w & = & -1 \end{cases} \Leftrightarrow \begin{cases} x & = & 1 - 2y - 2w \\ z & = & \frac{1}{2}w - 1 \end{cases}$$

Hence, the solutions are

$$S = \left\{ (x, y, z, w) \in \mathbb{R}^4 \mid x = 1 - 2b - 2d,\ y = b,\ z = \frac{1}{2}d - 1,\ w = d,\ b, d \in \mathbb{R} \right\}.$$

2. **Fields.** Consider the field $\mathbb{F}_5 := \mathbb{Z}/5\mathbb{Z}$. Its elements are $\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}$, where $\overline{n}$ denotes the residue class of n modulo $5\mathbb{Z}$. Calculate:

(a) all pairs (x, y) satisfying $x + y = \overline{0}$;

(b) the elements $\frac{\overline{3}}{\overline{4}} + \frac{\overline{1}}{\overline{3}}$ in terms of $\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}$;

(c) the value of $\overline{4}^{2022}$.

Solution:

(a) The equation $x + y = \overline{0}$ is equivalent to $y = \overline{0} - x = -x$. For $x = \overline{a}$ with $0 \leqslant a \leqslant 4$, it also holds true that $-x = \overline{-a} = \overline{5 - a}$. Thus the set of solutions is

$$\{(x, -x) \mid x \in \mathbb{F}_5\} = \{(\overline{0}, \overline{0}), (\overline{1}, \overline{4}), (\overline{2}, \overline{3}), (\overline{3}, \overline{2}), (\overline{4}, \overline{1})\}.$$

(b) The calculations

$$\begin{array}{rcccl} \overline{4}\cdot\overline{4} &=& \overline{16} &=& \overline{1}, \\ \overline{3}\cdot\overline{2} &=& \overline{6} &=& \overline{1} \end{array}$$

yield $\frac{\overline{1}}{\overline{4}} = \overline{4}$ and $\frac{\overline{1}}{\overline{3}} = \overline{2}$. Therefore we obtain

$$\frac{\overline{3}}{\overline{4}} + \frac{\overline{1}}{\overline{3}} = \overline{3}\cdot\frac{\overline{1}}{\overline{4}} + \frac{\overline{1}}{\overline{3}} = \overline{3}\cdot\overline{4} + \overline{2} = \overline{14} = \overline{4}.$$

(c) As $2022 = 2\cdot 1011$ and multiplication is associative, we get

$$\overline{4}^{2022} = (\overline{4}^2)^{1011}.$$

Note that $\overline{4}^2 = \overline{1}$ is the unit element of $\mathbb{F}_5$. With induction, one can show that $\overline{1}^n = \overline{1}$ for every integer number n. In particular, we get

$$\overline{4}^{2022} = (\overline{4}^2)^{1011} = \overline{1}.$$

3. **Fields.** Prove that for any $a, b \in \mathbb{F}_3$,

$$(a+b)^3 = a^3 + b^3.$$

Solution: We use the binomial identity to expand the left-hand side

$$(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3.$$

Note that $0 = 3$ in $\mathbb{F}_3 = \mathbb{Z}/3\mathbb{Z}$. This proves the statement.

4. **Linear System.** Fix $b_1, b_2, b_3 \in \mathbb{R}$. Determine when the following linear system of equations has a solution and describe its set of solutions $S \subseteq \mathbb{R}^3$ when it does

$$\begin{pmatrix} 0 & 7 & -2 \\ -1 & 2 & -1/2 \\ 4 & -1 & 0 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} b_1 \\ b_2 \\ b_3 \end{pmatrix}.$$

Solution: We write the augmented matrix for this system

$$\left(\begin{array}{ccc|c} 0 & 7 & -2 & b_1 \\ -1 & 2 & -1/2 & b_2 \\ 4 & -1 & 0 & b_3 \end{array}\right) \rightsquigarrow \left(\begin{array}{ccc|c} -1 & 2 & -1/2 & b_2 \\ 4 & -1 & 0 & b_3 \\ 0 & 7 & -2 & b_1 \end{array}\right) \rightsquigarrow \left(\begin{array}{ccc|c} 1 & -2 & 1/2 & -b_2 \\ 4 & -1 & 0 & b_3 \\ 0 & 7 & -2 & b_1 \end{array}\right)$$

$$\rightsquigarrow \left(\begin{array}{ccc|c} 1 & -2 & 1/2 & -b_2 \\ 0 & 7 & -2 & b_3 + 4b_2 \\ 0 & 7 & -2 & b_1 \end{array}\right) \rightsquigarrow \left(\begin{array}{ccc|c} 1 & -2 & 1/2 & -b_2 \\ 0 & 7 & -2 & b_3 + 4b_2 \\ 0 & 0 & 0 & b_1 - b_3 - 4b_2 \end{array}\right)$$

So, the equivalent system is

$$\begin{cases} x - 2y + \frac{1}{2}z &= -b_2 \\ 7y - 2z &= b_3 + 4b_2 \\ 0 &= b_1 - b_3 - 4b_2 \end{cases}$$

If $b_1 - b_3 - 4b_2 \neq 0$, then the system does not have any solutions. If we do have $b_1 - b_3 - 4b_2 = 0$, then the set of solutions is

$$S = \left\{(x, y, z) \in \mathbb{R}^3 \mid x = \tfrac{1}{14}(z + 4b_3 + 2b_2),\ y = \tfrac{1}{7}(2z + b_3 + 4b_2)\right\}.$$

5. **Fields.** Let $(k, +, \cdot, 0, 1)$ be a field and let $\alpha \in k$ such that $x^2 = \alpha$ does not have any solutions in k. Let τ be a formal symbol outside of k such that $\tau^2 = \alpha \in k$. Show that

$$k[\tau] = \{a + b\tau \mid a, b \in k\}$$

with the following operations

$$\begin{array}{rccc} + : & k[\tau] \times k[\tau] & \to & k[\tau] \\ & (a + b\tau, c + d\tau) & \mapsto & a + c + (b + d)\tau \end{array}$$

$$\begin{array}{rccc} \cdot : & k[\tau] \times k[\tau] & \to & k[\tau] \\ & (a + b\tau, c + d\tau) & \mapsto & ac + \alpha bd + (bc + ad)\tau \end{array}$$

as its addition and multiplication, and equipped with $0 + 0\tau$ as its 0 and $1 + 0\tau$ as its 1 is a field.

Can you give explicit examples of this construction?

Solutions: We let the reader check from the formulae that $0 + 0\tau$ is the neutral element for the addition and $1 + 0\tau$ is the neutral element for the multiplication. You can also directly see from the formulae that the set $k[\tau]$ is closed under addition and multiplication.

We now show the existence of an additive inverse. Indeed, for any $x = a + b\tau \in k[\tau]$

$$(-1 + 0\tau) \cdot x = -a + (-b)\tau \in k$$

and

$$x + (-1) \cdot x = 0 + 0\tau.$$

Let us now find a multiplicative inverse. Let $x = a + b\tau \in k[\tau] \setminus \{0 + 0\tau\}$ and $x' = a - b\tau \in k[\tau]$. Note that since $a + b\tau \neq 0 + 0\tau$, we have $\neg(a = 0 \wedge b = 0)$. If $b = 0$, then $\frac{1}{a} + 0\tau$ is the multiplicative inverse for x. Assume now that $b \neq 0$ and notice that $x' \neq 0$. If x' were null, then we would have $\tau = \frac{a}{b} \in k$, which we assumed is not true. Notice also that $xx' = a^2 - b^2\alpha \in k$. We then compute

$$\frac{1}{x} = \frac{x'}{xx'} = \frac{a - b\tau}{a^2 - b^2\alpha} = \frac{a}{a^2 - b^2\alpha} - \frac{b}{a^2 - b^2\alpha}\tau \in k[\tau].$$

This is the multiplicative inverse of x.

We let the reader check the associativity of both $+$ and $\cdot$ and the distributivity since the follow from the formula and the check only requires elementary algebra.

6. **Fields.** Let k be a finite field.

(a) Let S be the sum of all elements of k. Show that $S = 0$ is satisfied if and only if k has more than two elements.
Hint: What are the properties of the map

$$\begin{array}{rccc} m_b: & k & \to & k \\ & x & \mapsto & b \cdot x \end{array}$$

for $b \in k^* = k \setminus \{0\}$?
Solution: The map

$$\begin{array}{rccc} m_b: & k & \to & k \\ & x & \mapsto & b \cdot x \end{array}$$

is bijective, Indeed, it admits $m_{b^{-1}}$ as a left-and-right inverse since

$$m_b \circ m_{b^{-1}}(x) = m_b(b^{-1} \cdot x) = (b \cdot b^{-1}) \cdot x = x$$
$$m_{b^{-1}} \circ m_b(x) = m_{b^{-1}}(b \cdot x) = (b^{-1} \cdot b) \cdot x = x.$$

Hence, letting $b \in k^*$,

$$b \cdot S = b \cdot \sum_{x \in k} x = \sum_{x \in k} b \cdot x = \sum_{y \in k} y = S,$$

where we used the bijectivity of m_b to obtain the second to last equality. We deduce that

$$(1 - b) \cdot S = 0.$$

Now, if k has more than 2 elements, then there exists a $b \in k^* \setminus \{1\}$ such that the above equation holds. Since $b \neq 1$, we must have $S = 0$. If k has 2 elements, it must be the field $(\{0, 1\}, +, \cdot, 0, 1) \cong \mathbb{F}_2$ (check this). Then $S = 0 + 1 = 1$.

(b) Let $M = \prod_{x \in k^*} x$ be the product of all non-zero Elements of k. Show that $M = -1$.
Hint: Consider the map $k^* \ni x \mapsto \frac{1}{x} \in k^*$.
Solution: The map $k^* \ni x \mapsto \frac{1}{x} \in k^*$ is bijective and its fix points are $\{\pm 1\}$. In other words, for every $x \in k^*$, the inverse x^{-1} is distinct from x except when $x \in \{\pm 1\}$. We can reorganize the finite product to pair each $x \in k^*$ with its inverse and obtain a product of the form

$$(-1) \cdot 1 \cdot 1 \cdot \cdots \cdot 1 = -1.$$