Problem sheet 2

Fields, commutative rings, abelian groups, functions

Vocabulary

(1) Define abelian group and ring and give some illustrative examples.

(2) Define commutative ring and field and give some illustrative examples.

(3) Let R be a ring and let $r \in R$. Define a multiplicative inverse of r and give some illustrative examples.

(4) Let $\mathbb{F}$ be a field. Define $\mathbb{F}[t]$ and $\mathbb{F}(t)$ and give some illustrative examples.

(5) Let $\mathbb{F}$ be a field. Define $\mathbb{F}[[t]]$ and $\mathbb{F}((t))$ and give some illustrative examples.

(6) Let $\mathbb{F}$ be a field. Define the addition and multiplication in $\mathbb{F}[t]$ and $\mathbb{F}(t)$ and give some illustrative examples.

(7) Let $\mathbb{F}$ be a field. Define the addition and multiplication in $\mathbb{F}[[t]]$ and $\mathbb{F}((t))$ and give some illustrative examples.

(8) Define abelian group homomorphism and give some illustrative examples.

(9) Define ring homomorphism and give some illustrative examples.

(10) Define field homomorphism and give some illustrative examples.

(11) Define algebraically closed field and give some illustrative examples.

(12) Define function and equal functions and give some illustrative examples.

(13) Define injective, surjective and bijective functions and give some illustrative examples.

(14) Define composition of functions, the identity function and inverse function and give some illustrative examples.

Results

(1) Let A be an abelian group. Show that $0 \in A$ is is unique.

(2) Let A be an abelian group. Show that if $a \in A$ then its additive inverse then $-a \in A$ is unique.

(3) Let R be a ring. Show that the identity $1 \in R$ is unique.

(4) Let R be a ring and let $r \in R$. Show that if r has a multiplicative inverse then it is unique.

(5) Let R be a ring. Show that $0 \cdot 0 = 0$.

(6) Let A be an abelian group. Show that if $a \in A$ then $-(-a) = a$.

(7) Let R be a ring. Show that if $r \in R$ then $0 \cdot r = 0$.

(8) Let R be a ring. Show that if $r \in R$ and $1 \in R$ is the identity then $(-1) \cdot r = r \cdot (-1) = -r$.

(9) Let $\mathbb{K}$ and $\mathbb{F}$ be fields with identities $1_{\mathbb{K}}$ and $1_{\mathbb{F}}$, respectively.
A **field homomorphism from** $\mathbb{K}$ **to** $\mathbb{F}$ is a function $f: \mathbb{K} \to \mathbb{F}$ such that
   (a) If $k_1, k_2 \in \mathbb{K}$ then $f(k_1 + k_2) = f(k_1) + f(k_2)$,
   (b) If $k_1, k_2 \in \mathbb{K}$ then $f(k_1 k_2) = f(k_1) f(k_2)$,
   (c) $f(1_{\mathbb{K}}) = 1_{\mathbb{F}}$.

Explain why conditions (a) and (b) in the definition of a field homomorphism do not imply condition (c).

(10) Show that if $f: \mathbb{K} \to \mathbb{F}$ is a field homomorphism then $f(0_{\mathbb{K}}) = 0_{\mathbb{F}}$, where $0_{\mathbb{K}}$ and $0_{\mathbb{F}}$ are the zeros in $\mathbb{K}$ and $\mathbb{F}$, respectively.

(11) Show that if $f: \mathbb{K} \to \mathbb{F}$ is a field homomorphism then f is injective.

(12) Show that the field of complex numbers $\mathbb{C}$ is algebraically closed.

(13) Show that every field lies inside an algebraically closed field.

(14) Prove that if $p \in \mathbb{Z}$ and p is prime then $\mathbb{Z}/p\mathbb{Z}$ is a field.

(15) Prove that if $p \in \mathbb{Z}$ and p is not prime then $\mathbb{Z}/p\mathbb{Z}$ is not a field.

(16) Let $n \in \mathbb{Z}_{>0}$. Define the multiplication on $M_n(\mathbb{R})$ and prove that if $a, b, c \in M_n(\mathbb{R})$ then $(ab)c = a(bc)$.

(17) Let $f: S \to T$ be a function. Prove that an inverse function to f exists if and only if f is bijective.

(18) DeMorgan's laws. Let A, B and C be sets. Show that
   (a) $(A \cup B) \cup C = A \cup (B \cup C)$,
   (b) $A \cup B = B \cup A$,
   (c) $A \cup \emptyset = A$,
   (d) $(A \cap B) \cap C = A \cap (B \cap C)$,
   (e) $A \cap B = B \cap A$, and
   (f) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

(19) Let S, T, U be sets and let $f\colon S \to T$ and $g\colon T \to U$ be functions. Show that

(a) If f and g are injective then $g \circ f$ is injective,

(b) If f and g are surjective then $g \circ f$ is surjective.

(c) If f and g are bijective then $g \circ f$ is bijective.

(20) Let $f\colon S \to T$ be a function and let $U \subseteq S$. The **image** of U under f is the subset of T given by

$$f(U) = \{f(u) \mid u \in U\}.$$

Let $f\colon S \to T$ be a function. The **image** of f is the subset of T given by

$$\mathrm{im}\ f = \{f(s) \mid s \in S\}.$$

Note that $\mathrm{im}\ f = f(S)$.

Let $f\colon S \to T$ be a function and let $V \subseteq T$. The **inverse image** of V under f is the subset of S given by

$$f^{-1}(V) = \{s \in S \mid f(s) \in V\}.$$

Let $f\colon S \to T$ be a function and let $t \in T$. The **fiber** of f over $t is the subset of f \mathrm{S} given by f^{-1}(t) =$ $\{s \in S \mid f(s) = t\}$. Let $f\colon S \to T$ be a function. Show that the set $F = \{f^{-1}(t) \mid t \in T\}$ of fibers of the map f is a partition of S.

(21) (a) Let $f\colon S \to T$ be a function. Define

$$\begin{array}{rccc} f'\colon & S & \longrightarrow & \mathrm{im}\ f \\ & s & \longmapsto & f(s) \end{array}$$

Show that the map f' is well defined and surjective.

(b) Let $f\colon S \to T$ be a function and let $F = \{f^{-1}(t) \mid t \in \mathrm{im}\ f\} = \{f^{-1}(t) \mid t \in T\} - \emptyset$ be the set of nonempty fibers of the map f. Define

$$\begin{array}{rccc} \hat{f}\colon & F & \longrightarrow & T \\ & f^{-1}(t) & \longmapsto & t \end{array}$$

Show that the map $\hat{f}'$ is well defined and injective.

(b) Let $f\colon S \to T$ be a function and let $F = \{f^{-1}(t) \mid t \in \mathrm{im}\ f\} = \{f^{-1}(t) \mid t \in T\} - \emptyset$ be the set of nonempty fibers of the map f. Define

$$\begin{array}{rccc} \hat{f}'\colon & F & \longrightarrow & \mathrm{im}\ f \\ & f^{-1}(t) & \longmapsto & t \end{array}$$

Show that the map $\hat{f}''$ is well defined and bijective.

(22) Let S be a set. The **power set** of S, 2^S, is the set of all subsets of S.

Let S be a set and let $\{0,1\}^S$ be the set of all functions $f\colon S \to \{0,1\}$. Given a subset $T \subseteq S$ define a function $f_T\colon S \to \{0,1\}$ by

$$f_T(s) = \begin{cases} 0, & \text{if } s \notin T, \\ 1, & \text{if } s \in T. \end{cases}$$

Show that

$$\begin{array}{rccc} \varphi\colon & 2^S & \longrightarrow & \{0,1\}^S \\ & T & \longmapsto & f_T \end{array} \qquad \text{is a bijection.}$$

(23) Let $*\colon S \times S \to S$ be an associative operation on a set S. An **identity** for $*$ is an element $e \in S$ such that if $s \in S$ then $e * s = s * e = s$.

Let e be an identity for an associative operation $*$ on a set S. An **left inverse** for s is an element $t \in S$ such that $t * s = e$. A **right inverse** for s is an element $t' \in S$ such that $s * t' = e$. An **inverse** for s is an element $s^{-1} \in S$ such that $s^{-1} * s = s * s^{-1} = e$.

(a) Let $*$ be an operation on a set S. Show that if S contains an identity for $*$ then it is unique.

(b) Let e be an identity for an associative operation $*$ on a set S. Let $s \in S$. Show that if s has an inverse then it is unique.

(24) (a) Let S and T be sets and let ι_S and ι_T be the identity maps on S and T, respectively. Show that for any function $f\colon S \to T$,

$$\iota_T \circ f = f \qquad \text{and} \qquad f \circ \iota_S = f.$$

(b) Let $f\colon S \to T$ be a function. Show that if an inverse function to f exists then it is unique. (Hint: The proof is very similar to the proof of Ex. (23b) above.

Examples and computations

(1) Let $\mathbb{F}$ be a field. Define $M_{5\times 3}(\mathbb{F})$ and addition and show that it is an abelian group.

(2) Let $\mathbb{F}$ be a field. Define $M_{5\times 3}(\mathbb{F})$ and addition and multiplication and show that it is a ring.

(3) Calculate

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 0 & 1 & 3 \\ 0 & 3 & 2 & 5 \\ 4 & 5 & 2 & -3 \end{pmatrix} \qquad \text{and} \qquad \begin{pmatrix} 1 & 2 & 3 & 4 & \\ 2 & 3 & 4 & 0 & \\ & 3 & 4 & 0 & 1 \\ 4 & 0 & 1 & 2 & \end{pmatrix}$$

(4) For $i, j \in \{1, 2, 3, 4\}$ let $a_{ij}, b_{ij}, c_{ij} \in \mathbb{R}$. Calculate the $(2, 4)$-entry of

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44} \end{pmatrix} \left(\begin{pmatrix} b_{11} & b_{12} & b_{13} & b_{14} \\ b_{21} & b_{22} & b_{23} & b_{24} \\ b_{31} & b_{32} & b_{33} & b_{34} \\ b_{41} & b_{42} & b_{43} & b_{44} \end{pmatrix} \begin{pmatrix} c_{11} & c_{12} & c_{13} & c_{14} \\ c_{21} & c_{22} & c_{23} & c_{24} \\ c_{31} & c_{32} & c_{33} & c_{34} \\ c_{41} & c_{42} & c_{43} & c_{44} \end{pmatrix} \right) \qquad \text{and}$$

$$\left(\begin{pmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44} \end{pmatrix} \begin{pmatrix} b_{11} & b_{12} & b_{13} & b_{14} \\ b_{21} & b_{22} & b_{23} & b_{24} \\ b_{31} & b_{32} & b_{33} & b_{34} \\ b_{41} & b_{42} & b_{43} & b_{44} \end{pmatrix} \right) \begin{pmatrix} c_{11} & c_{12} & c_{13} & c_{14} \\ c_{21} & c_{22} & c_{23} & c_{24} \\ c_{31} & c_{32} & c_{33} & c_{34} \\ c_{41} & c_{42} & c_{43} & c_{44} \end{pmatrix}$$

(5) Find a multiplicative inverse of $\begin{pmatrix} 1 & 2 \\ 2 & 0 \end{pmatrix}$ in $M_2(\mathbb{R})$.

(6) Define $\mathbb{Q}$ and addition and multiplication and show that it is a field.

(7) Define $\mathbb{R}$ and addition and multiplication and show that it is a field.

(8) Define $\mathbb{C}$ and addition and multiplication and show that it is a field.

(9) Define addition and multiplication for the collection of all expressions $p(x)/q(x)$ where $p(x)$ and $q(x)$ are polynomials in x with real coefficients and $q(x)$ is not the zero polynomial and show that it is a field.

(10) Show that the set of integers with the usual addition and multiplication does *not* give us a field.

(11) Let $\mathbb{F}$ have two elements $\{0, 1, \}$ with the following addition and multiplication tables

$$\begin{array}{ccc} + & 0 & 1 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{array} \qquad\qquad \begin{array}{ccc} \cdot & 0 & 1 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \end{array}$$

Show that $\mathbb{F}$ forms a field.

(12) Show that the set of all real numbers of the form $a + b\sqrt{2}$ with $a.b \in \mathbb{Q}$ is a subfield of $\mathbb{R}$.

(13) Show that the set of all real numbers of the form $a + b\sqrt[3]{2}$ with $a, b \in \mathbb{Q}$ does not form a subfield of $\mathbb{R}$.

(14) Explain how to make a subfield of $\mathbb{R}$ which contains $\sqrt[3]{2}$ as well as the rational numbers.

(15) Write down the multiplication table for $\mathbb{Z}/7\mathbb{Z}$.

(17) Find an element a of $\mathbb{Z}/7\mathbb{Z}$ so that every non-zero element of $\mathbb{Z}/7\mathbb{Z}$ is a power of a.

(18) Show that $\mathbb{Z}/9\mathbb{Z}$ with addition and multiplication modulo 9, does not form a field. Show that the set of polynomials, with coefficients from the real numbers, does not form a field.

(19) Let $\mathbb{C}((t))$ denote the set of power series of the form $c_{-k}t^{-k} + c_{-k+1}t^{-k+1} + \cdots + c_0 + c_1 t + \cdots + c_s t^2 + \cdots$ with the operations of addition and multiplication of power series. Show that $\mathbb{C}((t))$ forms a field.

(20) Show that the field of all real numbers of the form $a+b\sqrt[3]{2}$ with $a, b \in \mathbb{Q}$ is not algebraically closed.

(21) Let $p \in \mathbb{Z}_{>0}$ be prime. Show that the field $\mathbb{Z}/p\mathbb{Z}$ is not algebraically closed.

(22) Which of the following are fields using the usual definitions of addition and multiplication? Explain your answers.
   (a) The positive real numbers.
   (b) The set of all numbers of the form $a\sqrt{2}$, where a is a rational number.

(23) (Testing for subfields) Let $\mathbb{K}$ be a subset of a field $\mathbb{F}$ and define addition and multiplication in $\mathbb{K}$ using the operations in $\mathbb{F}$. Explain why $\mathbb{K}$ is a field if the following four conditions are satisfied:

(a) $\mathbb{K}$ is closed under addition and multiplication,

(b) $\mathbb{K}$ contains 0 and 1,

(c) If $a \in \mathbb{K}$ then $-a \in \mathbb{K}$,

(d) If $a \in \mathbb{K}$ and $a \neq 0$ then $a^{-1} \in \mathbb{K}$.

(24) Show that $\{a + bi \mid a, b \in \mathbb{Q}\}$ forms a field with the usual operations of addition and multiplication of complex numbers. (Here $i = \sqrt{-1}$.)

(25) (Fields have no zero divisors) Using the field axioms, show that in any field: if $a \cdot b = 0$ then $a = 0$ or $b = 0$.

(26) (Solving equations in fields) Solve the following equations in $\mathbb{Z}/7\mathbb{Z}/$: (i) $x^2 = 2$, (ii) $x^2 = 3$.

(27) Is $\mathbb{Z}/7\mathbb{Z}$ algebraically closed? (An answer without proof receives no credit.)

(28) Factor the polynomial $x^2 - 2$ over $\mathbb{Z}/7\mathbb{Z}$.

(29) Find the inverse of 35 in $\mathbb{Z}/24\mathbb{Z}$ and the inverse of 24 in $\mathbb{Z}/35\mathbb{Z}$.

(30 Solve the equation $24x + 5 = 0$ in $\mathbb{Z}/35\mathbb{Z}$.

(31) What is the smallest subfield of $\mathbb{C}$ containing the rational numbers and i.

(32) What is the smallest subfield of $\mathbb{C}$ containing the rational numbers and $\sqrt[4]{5}$.

(33) What is the smallest subfield of $\mathbb{C}$ containing the rational numbers and $\sqrt{2}$ and i.

(34) Find addition and multiplication tables describing a field $\mathbb{F}$ consisting of exactly 4 elements $\{0, 1, a, b\}$. (Consider all the field axioms, including the distributive law.)