Project 6 - Groups, rings, and fields.

Groups

By a **group** we understand a system $(G, *, e)$ consisting of a nonempty set G, a binary operation $*$, and a distinguish element e such that the following axioms hold true:

(1) $\forall a, b, c \in G(a * (b * c) = (a * b) * c)$
(2) $\forall a \in G(a * e = e * a)$
(3) $\forall a \in G \exists b \in G(a * b = b * a = e)$

If, on top of that, the binary operation $*$ has the property

$$\forall a, b \in G(a * b = b * a),$$

we call G **Abelian** (or **commutative**).

In the following examples check that each described structure is a group, familiarize yourself with the used notation, and determine which of the groups are Abelian.

Number groups:

(1) $(\mathbb{Z}, +, 0)$, $(\mathbb{Q}, +, 0)$, $(\mathbb{R}, +, 0)$, $(\mathbb{C}, +, 0)$ – additive groups of integers, rationals, reals and complex numbers.
(2) $(\mathbb{Q}^{(p)}, +, 0)$ – additive group of rational p-integers, that is rational numbers of the form a/b, where $a, b \in \mathbb{Z}$, $gcd(a, b) = 1$, p does not divide b, and p is a fixed prime number.
(3) $(\mathbb{Q}_{(p)}, +, 0)$ – additive group of p-quotients, that is rational numbers of the form a/p^k, where p is a fixed prime number, $k \in \mathbb{Z}$.
(4) $(\mathbb{Q}^*, \cdot, 1)$, $(\mathbb{R}^*, \cdot, 1)$, $(\mathbb{C}^*, \cdot, 1)$ – multiplicative groups of nonzero rationals, reals, and complex numbers.
(5) $(\mathbb{Q}^+, \cdot, 1)$, $(\mathbb{R}^*, \cdot, 1)$ – multiplicative groups of positive rationals, and reals.
(6) $(\mathbb{C}_1, \cdot, 1)$ – multiplicative group of complex numbers of radius 1.
(7) $(\mathbb{C}(n), \cdot, 1)$ – multiplicative group of n-th roots of unity.
(8) $(\mathbb{Q}(\infty), \cdot, 1)$ – multiplicative group of roots of unity.

Residue groups:

(1) Let n be an integer, let $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$. In the set $\mathbb{Z}_n$ we define the binary operation $\oplus$ as follows: $a \oplus b =$ the remainder of the division of $a + b$ by n. Check that $(\mathbb{Z}_n, \oplus, 0)$ is a group.
(2) Let n be an integer, let $U(n) = \{k \in \mathbb{Z}_n : gcd(k, n) = 1\}$. In the set $U(n)$ we define the binary operation $\otimes$ as follows: $a \otimes b =$ the remainder of the division of $a \cdot b$ by n. Check that $(U(n), \otimes, 1)$ is a group.

Permutation groups:

(1) Let X be a nonempty set, let $S(X)$ denote the set of all functions $f : X \to X$ that are one-to-one and onto. Check that $(S(X), \circ, id_X)$ is a group, where $\circ$ denoted the composition of two functions, and id_X is the identity function.

Matrix groups:

(1) Let $M(n, K)$ be the set of all $n \times n$ matrices with coefficients from K. Check that $(M(n, K), +, 0)$ is an Abelian group.
(2) Let $GL(n, K) = \{A \in M(n, K) : \det A \neq 0\}$. Check that $(GL(n, K), \cdot, I)$ is a group.
(3) Let $SL(n, K) = \{A \in GL(n, K) : \det A = 1\}$. Check that $(SL(n, K), \cdot, I)$ is a group.
(4) Let $O(n, K) = \{A \in GL(n, K) : A \cdot A^t = I\}$. Check that $(O(n, K), \cdot, I)$ is a group.

Rings and fields

By a **ring** we understand a system $(R, +, \cdot, 0, 1)$, where $(R, +, 0)$ s an Abelian group, and $\cdot$ satisfies the following conditions:

(1) $\forall a, b, c \in R(a \cdot (b \cdot c) = (a \cdot b) \cdot c)$
(2) $\forall a, b, c \in R(a \cdot (b + c) = a \cdot b + a \cdot c)$
(3) $\forall a, b, c \in R((a + b) \cdot c = a \cdot c + b \cdot c$
(4) $\forall a \in R(a \cdot 1 = 1 \cdot a = a)$

If, on top of that, the operation $\cdot$ satisfies the confition

$$\forall a, b \in R(a \cdot b = b \cdot a)$$

we call R a **commutative ring**. Moreover, if R is a commutative ring such that

$$\forall a \in R \setminus \{0\} \exists b \in R(a \cdot b = b \cdot a = 1)$$

we call R a field.

Number rings:

(1) $(\mathbb{Z}, +, \cdot, 0, 1)$, $(\mathbb{Q}, +, \cdot, 0, 1)$, $(\mathbb{R}, +, \cdot, 0, 1)$, $(\mathbb{C}, +, \cdot, 0, 1)$ – check that these structures are commutative rings. Which of them are fields?

Residue rings:

(1) $(\mathbb{Z}_n, \oplus, \otimes, 0, 1)$ – check that this is a commutative ring. When is it a field?