Lecture 7
Rings and fields

The notion of group that we have studied is a generalization of various numeric systems considered with the operation of addition. The usual properties of two operations — addition and multiplication — lead to the abstract notion of a ring. Rings with especially nice properties are called fields.

Definition. A *ring* is a set A supplied with two operations: addition $(+)$ and multiplication $(\cdot)$ such that
1. $(A,+)$ is a commutative group (called the additive group of the ring A),
2. the distributive law holds:

$$\begin{aligned} a\cdot(b+c) &= a\cdot b+a\cdot c,\\ (a+b)\cdot c &= a\cdot c+b\cdot c. \end{aligned}$$

As you can see, the general definition of a ring does not require much from multiplication. If the multiplication does have some addition properties, the following terminology is used:

- If the law of multiplicative associativity $(a\cdot b)\cdot c = a\cdot(b\cdot c)$ holds for all elements a,b,c of A, then the ring is called *associative*.
- If the law of multiplicative commutativity $a\cdot b = b\cdot a$ holds for all elements a,b of A, then the ring is called *commutative*.
- If there is an element $1\in A$ such that for every $a\in A$ we have $1\cdot a = a\cdot 1 = a$, then we say that A is a *ring with unity*.

It follows from the definitions that in the ring with unity 1 the zero element 0 cannot be multiplicatively invertible: there is no such $a\in A$ that $a\cdot 0 = 1$, because $a\cdot 0$ is always 0. Therefore, the whole set A can never form a group with respect to multiplication. The best what one can expect is that all *non-zero* elements of A form a group.

Definition. A *field* is a ring A such that the set of all non-zero elements $A\setminus 0$ forms a group with respect to multiplication.

Remark. It is usually required that a field must be commutative. In French and in Russian, there are different terms for commutative and non-commutative fields ("champs" and "pole" vs. "corps" and "telo", respectively), in English, this distinction does not exist. The simplest and most famous example of a non-commutative field is provided by the field of quaternions (see below).

Examples of rings and fields.
1. $(\mathbb{Z},+,\cdot)$ — the ring of integers.
2. $(\mathbb{R},+,\cdot)$ — the field of real numbers.
3. $(\mathbb{Z}_m,+,\cdot)$ — the ring of residues modulo m.

Exercise: fill in the addition and multiplication tables of $\mathbb{Z}_3$ and $\mathbb{Z}_4$ and check that this field may or may not be a field, depending on the value of the parameter m.

4. $\mathrm{Mat}(n, \mathbb{F})$ — the ring of $n \times n$-matrices over a field $\mathbb{F}$. Operations are the usual matrix addition and matrix multiplication.

Exercise: Check that the number of elements of $\mathrm{Mat}(2, \mathbb{Z}_2)$ is 16. Find all invertible matrices in $\mathrm{Mat}(2, \mathbb{Z}_2)$ (the total number of such matrices is 6) and compile the multiplication table for them. Prove that they form a group isomorphic to D_3.

5. $\mathcal{F}(\mathbb{R}, \mathbb{R})$ — the ring of real-valued functions on the real line. Operations are point-wise addition and multiplication of functions.

6. $\mathbb{B}(M)$ — the ring of subsets of a given set M (the *Boolean algebra* of the set M). The points of $\mathbb{B}(M)$ are arbitrary subsets of M (if M is finite of cardinality n, then $\mathbb{B}(M)$ has 2^n elements). The role of addition and multiplication in this algebra are played by the operations of symmetric difference and intersection, respectively:

$$\begin{aligned} X + Y &= (X \setminus Y) \cup (Y \setminus X), \\ X \cdot Y &= X \cap Y. \end{aligned}$$

Remark. The ring $\mathbb{B}(M)$ is isomorphic to the ring of functions on M with values in the field of residues modulo 2:

$$\mathbb{B}(M) \cong \mathcal{F}(M, \mathbb{Z}_2).$$

To prove this fact, we assign, to every subset $X \subset M$, the *characteristic function* of this subset χ_X defined by

$$\chi_X(a) = \begin{cases} 1, & \text{if } \ a \in X, \\ 0, & \text{otherwise} \end{cases}.$$

The sum of two such functions, computed modulo 2 (i.e. according to the rule $1 + 1 = 0$), corresponds to the symmetric difference of the two subsets, while the product of functions corresponds to the union of the two subsets.