# IRREDUCIBILITY OF POLYNOMIALS OVER VARIOUS NUMBER FIELDS

**Goptareva Anna Valerievna**

Student, Belgorod State National Research University, Russia, Belgorod

**Bogachev Roman Evgenievich**

научный руководитель, Candidate of Sciences in Philosophy, associate professor, Belgorod state University, Russia, Belgorod

**Abstract.** The article considers irreducibility of polynomials over various number fields. Presently, in algebra and number theory, it is possible to compose many polynomials of different degrees, but each of them may have roots, so it can be decomposed into prime factors, or it may not be.

**Keywords:** mathematics, algebra, polynomials, number fields.

The purpose of this research is to study the concept and properties of irreducible polynomials in solving problems of algebra and number theory. The task of the research is to analyze the concepts of "polynomial" and "number field", define the concepts of polynomial reducibility and irreducibility, identify signs of irreducibility, give problems to prove the irreducibility of polynomials.

Let us consider the basic concept of polynomials and number fields, and study their properties in depth, as well as solve problems of finding roots of a polynomial with rational coefficients.

## 1. Concepts of Polynomials and Their Properties in Algebra.

Let y=f(x) be a rational integral function. Its expression through X may have a different appearance. For example,

$$y = (x - 2)^2(x + 1)^2 = (x^2 - 4x + 4)(x + 1)^2 = (x - 2)^2(x^2 - 2x + 1)$$

It is possible to continue these expressions, but they will all define the same function. The question arises as to how this rational integral function can be represented in a "standard", "canonical form".

Definition. A record of rational integral function is considered canonical if it has no brackets and similar terms, and the summands in it are arranged in a descending order of exponents of X.

The reduction to the canonical form is done as follows: all brackets are expanded using the distributive law

$$a(b + c) = ab + ac$$

After expanding the brackets, all the products of degrees of the variable are replaced and similar summands are given and arranged in a descending order of exponents. The result is an expression of the form:

$$f(x) = a_0 x^n + a_1 x^{n-1} + \cdots + a_n, a_0 \neq 0$$

Such an expression is called a polynomial of X, and n is the degree of this polynomial.

Numbers $a_0; a_1; \ldots; a_n$ refer to coefficients of polynomial f(x). In particular, $a_0$ refers to a higher coefficient, $a_n$ refers to the constant term.

## 2. Types of Number Fields and Their Properties in Algebra.

**In abstract algebra, a field is a set** for elements of which the operations of addition, taking the opposite value, multiplication and division (except for division by 0) are defined, wherein the properties of these operations are close to the properties of ordinary number operations. The simplest field is the field of rational numbers (fractions). Although the names of the field operations are taken from arithmetic, it should be kept in mind that the field elements are not necessarily numbers, and the definitions of the operations may be far from arithmetic. **An algebraic number field, field of algebraic numbers** (or simply – **a number field**) is a finite (and, therefore, algebraic) extension of the field of rational numbers Q.

Thus, a number field is a field containing Q and is a finite-dimensional vector space over it. Number fields and, more general, algebraic extensions of the field of rational numbers are the main object of the study of algebraic number theory.

Example 1. Number fields Q, R, C are the main examples of fields for us.

Example 2. For each prime number p, there is a number field of residues Zp from p elements.

## 3.Irreducible and Reducible Polynomials

**Definition 1:** p(x) over P is irreducible if its divisors are divisors of form c and p(x) and it has no other divisors.

**Definition 2:** $f(x)$ over P is reducible if, in addition to divisors c and c*f(x), this polynomial has other divisors φ(x), where degree of φ(x) is any natural number.

The same polynomial over one field may be irreducible, and over another – reducible.

$f(x)$ of degree $n \geq 1$ is reducible over P if there are polynomials $\varphi(x), g(x)$ over P, that there is an equality

$$f(x) = \varphi(x) * g(x)$$ at same degrees $n \geq 1$

$p(x) \; of$ degree $n \geq 1$ is irreducible over P if in any of its representations of the form

$$p(x) = \varphi(x) * g(x)$$

one of the polynomials has 0 degree, the other – n.

## 4. Problems for Proving Irreducibility of Polynomials

**Example 1.** Polynomial $f(x) = x^2 + 1 = (x - i)(x + i)$ is reducible over field C and irreducible over fields Q and R.

Polynomial $h(x) = x^2 - 5x + 6 = (x - 3)(x - 2)$ is reducible over Q, R and C.

**Example 2.** Over which of the fields N, Q, R or C the polynomials are irreducible:

a) $$f(x) = x^2 - 10x + 21;$$

b) $$h(x) = 3x^2 + x + 3;$$

To solve these problems, let us find the roots of the quadratic equation by the formula:

$$x_{1,2} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

For $f(x) = x^2 - 10x + 21$ we have

$$x_{1,2} = \frac{10 \pm \sqrt{100 - 4 * 21 * 1}}{2 * 1} = \frac{10 \pm 4}{2} => x_1 = 7, x_2 = 3$$

Then, $f(x) = x^2 - 10x + 2 = (x - 7)(x - 3)$. This polynomial is reducible over all fields N, Q, R or C.

The second polynomial $h(x) = 3x^2 + x + 3$ has no real roots, but has imaginary roots

$$x_{1,2} = \frac{-1 \pm \sqrt{1 - 4 * 3 * 3}}{2 * 3} = \frac{-1 \pm \sqrt{37} * i}{6}$$

It means that it is irreducible over N, Q, R.

**Conclusion**. Polynomial $P(\alpha) = a_0 + a_1 \alpha + ... + a_n \alpha^n = 0$ of degree $n$ by $x$ is irreducible if it cannot be represented in a form of product $f(x) = \varphi(x) \cdot g(x)$ of polynomials $\varphi(x)$ and $g(x)$ with integral coefficients, but of degrees less than $n$. If similar is possible, then P(x) is reducible. Such different signs of irreducibility have been studied and formulated. Examples of problems for proving the irreducibility of polynomials in a number field are given. The application of irreducible polynomials in the factorization of set C is considered.

**Bibliography:**

1. Ayerland K., Rosen M. Classical Introduction to Modern Number Theory, M.: Mir, 1987;

2. Algebraic Number Theory / edited by J. Cassels, A. Frelich, M.: Mir, 1969;

3. Field. Algebra/ Wikipedia material/ URL: https://ru.wikipedia.org/wiki/Поле_(алгебра)

4. Collection of Algebra Problems. Complex Numbers/ URL: http://oldskola1.narod.ru/Kochetkov2/Kochetkov242.htm

5. Sergeev A.E., Yakovlev A.V. On Galois Spectra of Polynomials with Integral Parameters // Notes of Scientific Seminars of the St. Petersburg Department of Steklov Mathematical Institute of the Russian Academy of Sciences. 2005. Vol. 321. pp. 275-280.