Cubo Matemática Educacional
Vol., 4. Nº 2, Junio 2002

FINITE FIELDS

V.V. Kirichenko
Faculty of Mechanics and Mathematics, Kiev Taras Shevchenko University,
Volodymyrska str., 64, Kiev, 01033, Ukraine
B.V. Novikov
Faculty of Mechanics and Mathematics, Kharskov University,
Svobody Sq., 4, Kharskov, 61077, Ukraine
A.P. Petravchuk
Faculty of Mechanics and Mathematics, Kiev Taras Shevchenko University,
Volodymyrska str., 64, Kiev, 01033, Ukraine

Content

1 Definition of a field. Examples

The notion of a field (in algebraic sense) is one of the most important notions of algebra (and of whole mathematics). The idea of a field crystallized in the middle of the nineteenth century, when algebraic systems appeared which had features of number systems but many different properties (complex numbers, fields of residues modulo p for a prime p, set (skew field) of quaternions etc) . The field theory was created by many prominent mathematicians of the last two centuries (Gauss, Galois, Kronecker, Dedekind, Wedderburn, Hilbert and many others). The general idea of a field includes the most important properties of the set of rational numbers (and real numbers) concerning the operations of addition and multiplication but all other properties are ignored (concerning, for example, the nearness of numbers on the real line or arithmetic properties of integers). The papers of French mathematicians E.Galois and J. Lagrange devoted to group theory and its applications for solving algebraic equations and works of C.F. Gauss in number theory formed the basis of the theory of fields. The term "field" was for the first time used probably by P. Dirichlet (1871) in his works in the number theory.

Definition 1. A set F consisting of at least two elements is called a field if two binary operations on F are defined which are called addition and multiplication and denoted correspodingly by $(+)$ and $(\cdot)$ and which satisfy the following conditions:

1) the both operations are associative and commutative, i.e. $(a+b)+c = a+(b+c)$, $a+b = b+a$ and $(a\cdot b)\cdot c = a\cdot(b\cdot c)$, $a\cdot b = b\cdot a$;

2) they are connected by means of distributivity law, i.e. $(a+b)\cdot c = a\cdot c + b\cdot c$;

3) there exists in F a zero element 0 such that $a+0 = a$ for all $a \in F$, and for any

element $a \in F$ there exists an opposite element $-a$ such that $a+(-a) = 0$;

4) there exists in F an identity element 1 such that $a\cdot 1 = a$ for all $a \in F$, and for any element $a \in F$, $a \neq 0$ there exists an inverse element a^{-1} such that $a\cdot\ (a^{-1}) = 1$;

Therefore all elements of a field F form a commutative group on addition and all nonzero elements of F form a group (also commutative) on multiplication. By standard way, one can prove that a field possesses the unique zero element 0 and identity element 1 $(0 \neq 1)$ and for any element $a \in F$ the opposite element and the inverse element (in case $a \neq 0$) are uniquely defined. The following relations are also true in fields:
$a\cdot 0 = 0$, $a(b-c) = ab - ac$ for all $a, b, c \in F$.

Example 1. The set of rational numbers $\mathbf{Q}$ with natural operations of addition and multiplication is a field.

The set $\mathbf{R}$ of all real numbers with addition and multiplication of numbers is also a field. The most important field is the field $\mathbf{C}$ of all complex numbers, which contains the both previous fields.

If in the condition 4) of the definition 1 one refuses the requirement of existence of inverse for every nonzero element, one has the definition of commutative ring (with an identity element). The most important examples of rings are the ring $\mathbf{Z}$ of all integers and the ring $F[x]$ of all polynomials over the field F.

Example 2. Let us consider the set $\mathbf{Q}[\sqrt{2}]$ of all numbers of the form $a + b\sqrt{2}$ where $a, b \in \mathbf{Q}$, with operations of addition and multiplication. For any two numbers from $\mathbf{Q}[\sqrt{2}]$, their sum and product are of the same form. The numbers 0 and $1 = 1 + 0\sqrt{2}$ belong to this set and for any $x \in \mathbf{Q}[\sqrt{2}]$ the opposite element $-x$ is of the same form. Further, for any nonzero element $y = a + b\sqrt{2}$ the inverse element is of the form $y^{-1} = (a - b\sqrt{2})/(a^2 - 2b^2)$ and is contained in $\mathbf{Q}[\sqrt{2}]$ (note that $a^2 - 2b^2 \neq 0$ because the numbers a and b are rational). Thus, the set $\mathbf{Q}[\sqrt{2}]$ is also a field. Obviously, $\mathbf{Q} \subset \mathbf{Q}[\sqrt{2}]$.

All above considered fields are number, i.e. their elements are numbers. The following fields consists of subsets of the set $\mathbf{Z}$ of all integers, but not numbers.

Example 3. Let p be an arbitrary prime and $\mathbf{Z}_p$ be the set of all residues modulo p. Elements of $\mathbf{Z}_p$ are of the form $\overline{0} = \{p\mathbf{Z}\}, \overline{1} = \{1+p\mathbf{Z}\}, ..., \overline{p-1} = \{p - 1 + p\mathbf{Z}\}$.

As representatives of these classes we take the smallest non-negative integers contained in them. The operations of addition and multiplication are defined in $\mathbf{Z}_p$ in natural way: $\overline{x} + \overline{y} = \overline{x + y}$, $\overline{x} \cdot \overline{y} = \overline{x \cdot y}$ (the result of the operation does not depend on choice of representatives from the residue classes) . The class $\overline{0}$ is a zero element in $\mathbf{Z}_p$ and the element $\overline{1} = \{1 + p\mathbf{Z}\}$ is the identity in $\mathbf{Z}_p$. If $\overline{x} \neq \overline{0}$, then the $GCD(x, p) = 1$ and therefore there exist elements $y, z \in \mathbf{Z}$, such that $xy + pz = 1$. This implies the relation $\overline{x} \cdot \overline{y} = \overline{1}$ and therefore $\mathbf{Z}_p$ is a field relatively above mentioned operations. Obviously $|\mathbf{Z}_p| = p$. Finite fields are called Galois fields, in honour of the prominent French mathematician Evariste Galois who was one of the creators of group theory and theory of fields. Galois field is often denoted by $GF(k)$ where k is the number of elements of this field (this notation does not cause any misunderstanding because finite fields F_1 and F_2 with $|F_1|$ = $|F_2|$ are isomorphic). It is convenient to illustrate addition and multiplication in small fields by two tables. The result of the operation ($a_i + a_j$ or $a_i \cdot a_j$) is putting on the crossing of the i-th row and the j-th column for all enumerated elements $a_1, ..., a_n$ of the field F. Let us write now tables of addition and multiplication for the simpliest field $\mathbf{Z}_2 = \mathbf{Z}/2\mathbf{Z}$. For convenience, we will write residue classes $\overline{0}$ and $\overline{1}$ without bars.

$$\mathbf{Z}_2 : \qquad \begin{array}{c|cc} + & 0 & 1 \\ \hline 0 & 0 & 1 \\ 1 & 1 & 0 \end{array}\,, \qquad \begin{array}{c|cc} \cdot & 0 & 1 \\ \hline 0 & 0 & 0 \\ 1 & 0 & 1 \end{array}\,.$$

Analogously, we can write two tables for the field $\mathbf{Z}_3$

$$\mathbf{Z}_3 : \qquad \begin{array}{c|ccc} + & 0 & 1 & 2 \\ \hline 0 & 0 & 1 & 2 \\ 1 & 1 & 2 & 0 \\ 2 & 2 & 1 & 0 \end{array}\,, \qquad \begin{array}{c|ccc} \cdot & 0 & 1 & 2 \\ \hline 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 2 \\ 2 & 0 & 2 & 1 \end{array}\,.$$

2 Subfields. Prime fields

In general, algebra studies really not sets with algebraic operations but algebraic operations. Therefore for disengaging from inessential properties of the sets on which algebraic operations are studied, the notion of isomorphism was introduced. For fields, it sounds so: let F and H be two fields. A bijective mapping $\phi : F \longrightarrow H$ is called an isomorphism from F onto H if ϕ preserves sums and products of elements, i.e.

$$\phi(a+b) = \phi(a) + \phi(b), \quad \phi(ab) = \phi(a)\phi(b), \quad \phi(0) = 0, \quad \phi(1) = 1$$

for arbitrary elements $a, b \epsilon F$. Note that the sum and the product of elements a and b are calculating in the field F, but the correspondence operations on elements $\phi(a)$ and $\phi(b)$ are carried out in the field H. In case, when there exists an isomorphism of a field F onto a field H (may be $F = H$) , the fields F and H are called isomorphic (notation $F \simeq H$). From the algebraic viewpoint, isomorphic fields are indistinguishable (although their sets of elements can be radically different) .

Example 4. Let $F = \mathbf{C}$ be the field of complex numbers,

$$\mathbf{C} = \{a + bi |\ a, b \epsilon \mathbf{R}\} \text{ and } K = \{\begin{pmatrix} a & b \\ -b & a \end{pmatrix} |\ a, b \epsilon \mathbf{R}\}$$

be a subset of the matrix ring $M_2(\mathbf{R})$. It is easily seen that sums and products of such matrices are of the same form, zero and identity matrices belong to K, opposite and inverse matrices can be written in the same form. Thus, K is a field contained in the matrix ring $M_2(\mathbf{R})$.

Let the mapping $\phi : F \longrightarrow K$ be defined by the rule:

$$\phi(a+bi) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}.$$

It is easy to check out immediately that for any complex numbers $z_1 = a_1 + b_1 i$ and $z_2 = a_2 + b_2 i$ the following relations hold:

$$\phi(z_1 + z_2) = \phi(z_1) + \phi(z_2) \text{ and } \phi(z_1 z_2) = \phi(z_1)\phi(z_2).$$

Besides,

$$\phi(0) = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \text{ and } \phi(1) = \phi(1+0i) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

and ϕ is obviously a bijection. Thus, ϕ is an isomorphism of the field F onto the field K.

Let F be a field. If a set $K \subseteq F$ is a field relatively the operations from F then K is called a subfield of F. The field F is called an extension of the subfield K. From this definition, it follows particularly that the zero and the identity of the field F belong to the subfield K and are zero and identity element correspodingly for the field K.

If one has a family K_i, $i \in I$ of subfields of the field F, then $K = \cap_{i \in I} K_i$ is a subfield of F. Indeed, K contains 0 and 1 from the field F, and if $a, b \in K$, then $a, b \in K_i$ for all $i \in I$. Therefore $a+b, a-b, ab, ab^{-1}$ for $b \neq 0$ belong to the subfield K_i for all $i \in I$.

Then $a+b, a-b, ab, ab^{-1}$, $(b \neq 0)$ all belong to K, and thus K is a subfield of F.

Definition 2. A field containing no proper subfields is called prime.

Theorem 1. *Given any field F, there exists the unique prime subfield K_0 of F. This field is isomorphic either to the field $\mathbf{Q}$ of rational numbers, or to a field $\mathbf{Z}_p$ for some prime p.*

Proof. Show first the uniqueness of the prime subfield from the field F. Are there two different prime subfields K_1 and K_2 of F, their intersection $K_1 \cap K_2$ is different from both K_1 and K_2, in contradiction to choice of the fields K_1 and K_2. Let K_0 be the intersection of all subfields from the field F. Then K_0 contains 1 and all integer multiples

$$n \cdot 1 = \underbrace{1 + 1 + ... + 1}_{\text{n summands}}.$$

Consider two cases:

(1) $n \cdot 1 \neq 0$ for all integers n. Then the subfield K_0 contains all inverses to the elements $n \cdot 1$, which we will denote $1/n$ and all their multiples m/n. It is easy seen that all such elements form a subfield in K_0, and in view of being K_0 prime, $K_0 = \{m/n,\ n \in \mathbf{Z}\}$. It is almost obvious that $K_0 \simeq \mathbf{Q}$.

(2) There exists an integer n such that $n \cdot 1 = 0$. Take the least positive integer p with property $p \cdot 1 = 0$. It is easily seen that the number p is prime. Indeed, if $p = rs$, $r, s \neq 1$ then $0 = p \cdot 1 = r \cdot 1 \cdot s \cdot 1$ and therefore either $r \cdot 1 = 0$ or $s \cdot 1 = 0$. The later is impossible because of the number p is minimal with property $p \cdot 1 = 0$. We here used the following property of fields: the equality $ab = 0$ implies either $a = 0$ or $b = 0$. Now consider elements $1, ..., (p-1) \cdot 1$ of the subfield K_0. It is easily seen that they form a subfield of the field F and since the field K_0 is minimal it holds $K_0 = \{0, 1, ...(p-1) \cdot 1\}$. Assign to the element $i \cdot 1$ from the field K_0 the residue class $\bar{i}$ from the field $\mathbf{Z}_p$. This correspodence is bijective and is an isomorphism of the prime subfield K_0 onto the field $\mathbf{Z}_p$.

Definition 3. A field F is called having characteristic 0 if its prime subfield is isomorphic to the field $\mathbf{Q}$. If the prime subfield of a field F is isomorphic to the field $\mathbf{Z}_p$ the field F is called of prime characteristic $p > 0$.

Note that in every field F of prime characteristic p it holds

$$\underbrace{a + a + ... + a}_{p} = (p \cdot 1) \cdot a = 0 \cdot a = 0$$

for any element $a \in F$. Thus, F regarding as a group with operation of addition is of exponent p (i.e. all its elements are order p). Fields $\mathbf{Q}, \mathbf{R}, \mathbf{C}$ above considered are of characteristic 0, the field $\mathbf{Z}_p$ has characteristic p.

Example 4. Let F be an arbitrary field and $F(x)$ the set of rational fractions with coefficients from the field F, i.e. $F(x) = \{f(x) \mathbin{/} g(x) \mid f(x), g(x) \in F[x],\ g(x) \neq 0$. where $F[x]$ is the the ring of polynomials in one variable x. It can be easily checked out that $F(x)$ is a field relatively natural operations of addition and multiplication of rational fractions. This field has the same characteristic as the field F.

3 Extensions of fields. The splitting field of a polynomial

Let F be a field and K its proper subfield. Take an element $\theta \epsilon F$, $\theta \notin K$ and consider the intersection of all subfields of F, containing both K and θ. This subfield is denoted by $K(\theta)$ and is called the prime extension of the field K; θ is called the primitive element of this extension. Since $K(\theta)$ contains subfield K and the element θ, the subfield $K(\theta)$ contains all terms of the form $f(\theta)$ where $f(x)$ is an arbitrary polynomial with coefficients from K. Moreover, all elements of the form $f(\theta)/g(\theta)$ where $f(x), g(x) \epsilon K[x]$, $g(\theta) \neq 0$ belongs to the field $K(\theta)$. But all such terms obviously form a field and therefore $K(\theta) = \{f(\theta)/g(\theta) — f(x), g(x) \epsilon K[x], g(\theta) \neq 0\}$. In case when the field $K(\theta)$ is isomorphic to the field $K(x)$ of all rational fractions, the element θ is called transcendental over the field K and algebraic over K in other case. If an element θ is algebraic over K, there exists a nonzero polynomial $f(x) \epsilon K[x]$ with property $f(\theta) = 0$. Then a polynomial $m_\theta(x)$ of the least degree with leading coefficient 1 (monic polynomial) can be found such that $m_\theta(\theta) = 0$. This polynomial is called the minimal polynomial of the element θ over the field K. The field $K(\theta)$ then consists of all elements from F of the form $a_0 + a_1\theta + ... + a_{n-1}\theta^{n-1}$, where $a_i \epsilon K$, $i = 1, ..., n$, $n = deg\ m_\theta(x)$.

Obviously, the field $K(\theta)$ can be regarded as a vector space over the field K with basis $\{1...., \theta^{n-1}\}$. In general. every extension F of the field K can be regarded as a vector space over K; its dimension $dim_K F$ is called the degree of extension F/K and often denoted by $[F : K]$. For a transcendental element θ over K , the degree of extension $[K(\theta) : K] = \infty$ because all elements $\{1, \theta, ..., \theta^n, ...\}$ are linearly independent over K. In case of algebraic element θ one has $[K(\theta) : K] = deg\ m_\theta(x)$.

Indeed, the following statement holds:

Theorem 2. *Let $F \supset K$ be an extension of the field K. Then an element $\theta \epsilon F$ is algebraic over K if and only if $[K(\theta) : K] < \infty$. If the element θ is algebraic over K, then $K(\theta) = K[\theta]$ where $K[\theta] = \{f(\theta) | f(x) \epsilon K[x]\}$.*

Example 5. The field **C** of complex numbers is an extension of the field **R**. Its degree equals 2 because $\mathbf{C} = \mathbf{R} \cdot 1 + \mathbf{R} \cdot i$. and elements 1 and i are linearly independent over **R**. The minimal polynomial for i is $m_i(x) = x^2 + 1$.

If there is a sequence of fields $F \supset K \supset P$ (a tower of extensions), then one has three vector spaces: F over K, K over P and F over P.

Theorem 3. *Let $F \supset K \supset P$ be a tower of extensions. The degree $[F : P]$ is finite if and only if the degrees $[F : K]$ and $[K : P]$ are finite. In case of their finiteness the following equality holds*

$$[F : P] = [F : K][K : P].$$

Let now K be any field and $f(x)$ an irreducible polynomial from $K[x]$. There is a standard procedure how to construct an extension of the field K which contains at least one root of the polynomial $f(x)$. To build such an extension, consider residue ring of the form $K[x]/(f(x))$ where $(f(x))$ is the ideal of the ring $K[x]$ consisting of all multiples of the polynomial $f(x)$. The elements of this residues ring are subsets of polynomials of the form $\overline{g} = g(x)+K[x]f(x)$, i.e. residues modulo $f(x)$. Dividing with remainder the polynomial $g(x)$ by $f(x)$, one can write every polynomial from the set $\overline{g}$ in the form $r(x)+f(x)h(x)$ where $deg\, r(x) < deg\, g(x)$. If $\overline{g}(x) = g(x)+(f(x))$ is a nonzero residue class, there exist polynomials $u(x)$ and $v(x)$ such that $u(x)g(x)+v(x)f(x) = 1$. After passing to residue classes modulo $(f(x))$ one gets a relation of the form $\overline{u}\,\overline{g} = \overline{1}$, where $\overline{1} = 1 + (f(x))$ is the identity element of the ring $K[x]/(f(x))$. Thus, every nonzero element of the ring $K[x]/(f(x))$ is invertible and this ring is a field. Residue classes containing elements of the ring K form a subfield in $K[x]/(f(x))$ which is isomorphic to the ring K, i.e. $K[x]/(f(x))$ is an extension of the field K. Note that the element $\overline{x} = x + (f(x))$ is a root of the polynomial $f(x)$; more precisely of the image of this polynomial in the ring of polynomials over the field $K[x]/(f(x))$. Indeed, if $f(x) = a_0 + a_1x + ... + a_nx^n$, then in the field $K[x]/(f(x))$ one has $\overline{a}_0 + \overline{a}_1\overline{x} + ... + \overline{a}_n\overline{x}^n = \overline{f}(x) = \overline{0}$. So we have proved a known Kronecker's theorem about symbolic adjunction of a root.

Theorem 4. *Given an irreducible polynomial $f(x)$ over a field K, there exists an extension $F \supset K$, which contains at least one root of $f(x)$. One may take this field so that it is isomorphic to the fields of residues $K[x]/(f(x))$.*

Repeating, if necessary, just now described procedure of adjunction of a root one can build an extension of the field K such that the polynomial $f(x)$ decomposes into linear factors.

The field F is called splitting field of the polynomial $f(x)$ over the field K if $F = K(c_1, ..., c_n)$, where $c_1, ..., c_n$ are all roots of the polynomials $F(x)$, i.e. F can be constructed from K by adjunctions of roots only the polynomial $f(x)$.

For any polynomial $f(x) \epsilon K[x]$ of degree $n > 0$ there exists at least one splitting field.

Moreover, any two splitting fields F_1 and F_2 of a polynomial $f(x)$ over the field K are isomorphic.

Example 6. The polynomial $f(x) = x^2 + x + 1$ is irreducible over the field $\mathbf{Z}_2$.

Indeed, none of the elements from the field $\mathbf{Z}_2$ is a root of this polynomial. Since the degree $f(x)$ is two, this polynomial is irreducible. We now build an extension of the field $\mathbf{Z}_2$ which contains a root θ of this polynomial. Consider the ring of residue classes $\mathbf{Z}_2[x]/(f(x))$. There are four such classes: $0+(f)$, $1+(f)$, $x+(f)$, $x+1+(f)$. Note that $x^2 \equiv x+1(mod(f))$, because of relation $x^2-x-1 = x^2+x+1 \epsilon (f(x))$ (in a field of characteristic $p = 2$, it holds $a = -a$ for any element a from this field). Since $\theta^2 = \theta + 1$ in the field $\mathbf{Z}_2[x]/(f(x))$ (we will denote it by $GF(4)$), one can write down the addition table for this field:

$GF(4)$:

$+$	0	1	θ	θ^2
0	0	1	θ	θ^2
1	1	0	θ^2	θ
θ	θ	θ^2	0	1
θ^2	θ^2	θ	1	0

Analogously, one can write down the multiplcation table for this field. For convenience. write the result of dividing x^3 and x^4 by $f(x) = x^2+x+1$ in the polynomial ring $\mathbf{Z}_2[x]$: $x^3 = (x^2 + x + 1)(x + 1) + 1$; $x^4 = (x^2 + x + 1)(x^2 + x) + x$. It follows from these relations that $x^3 = 1(mod(f))$; $x^4 = x(mod(f))$. Thus, in the field $GF(4)$ the following equalities hold: $\theta^3 = 1$ and $\theta^4 = \theta$.

$GF(4)$:

$\cdot$	0	1	θ	θ^2
0	0	0	0	0
1	1	0	θ	θ^2
θ	0	θ	θ^2	1
θ^2	0	θ^2	1	0

4 Finite fields. Basic properties

Let F be a finite field. Then the prime subfield F_0 from F is isomorphic to the field $\mathbf{Z}_p$ for some prime p and the characteristic of F is p. Regarding F

as a vector space of dimension n over the subfield F_0, we obtain $|F| = p^n$. Indeed, after choosing of a basis in the vector space F over F_0, one can see that F is isomorphic to the vector space F_0^n of rows $(\alpha_1, ..., \alpha_n)$ of length n. At that the coordinates α_i independently run over p values from F_0 and therefore $|F| = p^n$.

Theorem 5. *Given a finite field F and an integer $n > 0$, there exists an extension $K \supset F$ of degree $n = [K : F]$. All such extensions are isomorphic one to each another.*

Note that the uniqueness (up to isomorphism) of the above mentioned extension follows from the isomorphism of splitting fields of the polynomial $x^{q^n} - x$ because the field K of degree n over the field F ($|F| = q$) has q^n elements and all these elements are roots of the polynomial $x^{q^n} - x$.

Taking in the last theorem instead F the prime field $\mathbf{Z_p}$, one obtains that for any prime p and any integer $n > 0$ there exists a field consisting of p^n elements and it is unique up to isomorphism. The finite field consisting of p^n elements (p is its characteristic) is often denoted by $GF(p^n)$ or $GF(q)$ where $q = p^n$, or $\mathbf{F_q}$.

If F is an arbitrary field then the set of all nonzero elements of F form a group relatively of multiplication. This group is called the multiplicative group of the field F and is often denoted by F^* . For a finite field $GF(q)$ the multiplicative group F^* is of order $q - 1$. Let m be the exponent of the group F^* , i.e. the least positive integer m with property $a^m = 1$ for any $a \in F^*$. If $m < q - 1$ then the polynomial $x^m - 1$ has more than m roots (namely $q - 1$) in F. It is impossible, and therefore $m = q - 1$. Thus, we have proved the following

Theorem 6. *The multiplicative group $\mathbf{F_q^*}$ of a finite field $\mathbf{F_q}$ is cyclic (of order $q - 1$) .*

Definition 4. An isomorphism $\phi : F \longrightarrow F$ of a field F onto itself is called an automorphism of the field F.

Example 7. Let $\mathbf{C}$ be the field of complex numbers and $\phi : \mathbf{C} \longrightarrow \mathbf{C}$ defined by the rule $\phi(z) = \overline{z}$ where $\overline{z}$ is conjugated to z. Then $\phi(z_1 + z_2) = \phi(z_1) + \phi(z_2)$, $\phi(z_1 z_2) = \phi(z_1)\phi(z_2)$, $\phi(0) = 0$, $\phi(1) = 1$ and therefore ϕ is an automorphism of the field $\mathbf{C}$.

All automorphisms of the field F form a group (denoted by $Aut(F)$) relatively to the composition. Obvious, the identity mapping from F onto F is an automorphism and is an identity element of the group $Aut(F)$.

Example 8. Let $\mathbf{F_q}$ be a finite field consisting of $q = p^n$ elements where

p is a prime. Consider the mapping $\phi : \mathbf{F_q} \longrightarrow \mathbf{F_q}$ defined by the rule $\phi(x) = x^p$. Since $(x+y)^p = x^p + y^p$ (coefficients $(\left\{ {p \atop i} \right\}$, $i \neq 0$ by other monomials are zero in the field of characteristic p) and $(xy)^p = x^p y^p$, the mapping ϕ preserves sums and products. The equality $\phi(x) = \phi(y)$ means $x^p = y^p$ and therefore $(x-y)^p = 0$. From this, it follows $x = y$, i.e. the mapping ϕ is injective. As the field is finite, the mapping ϕ is also surjective and is an automorphism of the field $\mathbf{F_q}$. This automorphism is called Frobenius automorphism. If F is the field consisting of p^n elements then the Frobenius automorphism $\phi : x \longrightarrow x^p$ is of order n and generates the group $Aut(F)$. Thus, the group of automorphisms of the finite field $\mathbf{F_{p^n}}$ is cyclic of order n.

Let F be a field , K its subfield. All automorphisms of the field F leaving fixed all elements of the subfield K form a subgroup H from $Aut(F)$. Conversely, taking any subgroup H from the group $Aut(F)$ one can show that the set of all elements from F leaving fixed relatively to the automorphisms from H make up a subfield F_H from F.

These correspondences replace all inclusions of subfields (subgroups) by opposite inclusions of subfields (corespodingly subgroups). Under some restrictions there is a bijective correspondence between subfields of F and subgroups of $Aut(F)$. This correspondence is called Galois correspondence and is one of the most important tool for studying of fields and their extensions. More precisely, the Galois theory studies normal and separable extensions F of a field K of finite degree and establishes a bijective connection between intermediate subfields P: $F \supset P \supset K$ and subgroups of the group $Aut(F/K)$ of all automorphisms of F leaving fixed the subfield K. In this case, the group $Aut(F/K)$ is finite and the structure of all intermediate subfields can be investigated by studying of the group $Aut(F/K)$.

Theorem 7. *Let $\mathbf{F}_{p^n}$ be a field of order p^n and ϕ the Frobenius automorphism of the field $\mathbf{F}_{p^n}$. If $\mathbf{F}_{p^d}$ is a subfield of $\mathbf{F}_{p^n}$ then $d\,|\,n$. Conversely, to every divisor d of the number n there is exact one subfield $\mathbf{F}_{p^d} = \{x \in \mathbf{F}_{p^n} |\ \phi^d(x) = x\}$. All automorphisms leaving fixed the subfield $\mathbf{F}_{p^d}$ form a subgroup $Aut(\mathbf{F}_{p^n}/\mathbf{F}_{p^d}) =< \phi^d >$. This correspondence between subfields of a finite field and subgroups of automorphism group (Galois correspondence) is bijective and makes all inclusions opposite.*

5 The Dedekind number (the number of monic irreducible polynomials of given degree)

Theorem 8. *Let* $\mathbf{F}_\mathrm{q}$ *be a finite field. For any positive integer* m *there exists at least one irreducible polynomial of degree* m *over* $\mathbf{F}_\mathrm{q}$.

Actually, the number of all irreducible monic polynomials of degree m (with leading coefficient being equal 1) over the field $\mathbf{F}_q$ can be exactly counted. This number is often called the Dedekind's number and denoted by $D_{m,q}$. To write down a formula for the Dedekind 's number, we need some information about Möbius function

Definition 5. A function $\mu : \mathbf{N} \longrightarrow \mathbf{Z}$ defined by the rule

$$\mu(n) = \left\{ \begin{array}{cl} 1, & \text{if } n = 1 \\ (-1)^k, & \text{if } n \text{ is product of } k \text{ distinct primes} \\ 0 & \text{if } n \text{ divides by square of a prime} \end{array} \right)$$

is called the Möbius function . This function is widely used in number theory, algebra and combinatorics. It is multiplicative, i.e. is not identically zero and $\mu(mn) = \mu(m)\mu(n)$ for coprime positive integers m and n. It is easily seen that

$$\sum\nolimits_{d|n} \mu(d) = \sum\nolimits_{d|\overline{n}} \mu(d)$$

where $\overline{n} = p_1 \cdots p_k$ is the product of all distinct prime divisors of the number n. Further, note that the number of divisors of the number $\overline{n}$ of the form $d = p_{i_1} \cdots p_{i_r}$ is equal to $\left\{ \begin{smallmatrix} k \\ r \end{smallmatrix} \right\}$. Therefore, it holds for $n > 1$

$$\sum\nolimits_{d|n} \mu(d) = \sum\nolimits_{d|\overline{n}} \mu(d) = \sum\nolimits_{r=0}^{k} \left\{ \begin{matrix} k \\ r \end{matrix} \right\} (-1)^r = (1-1)^r = 0.$$

From this, it follows the relation

$$\sum\nolimits_{d|n} \mu(d) = \left\{ \begin{array}{ll} 1, & \text{if } n = 1 \\ 0, & \text{if } n > 1 \end{array} \right. .$$

The Möbius function allows to find one function by means of another if there is a connection of certain form between them. Let f and g be two functions from the set **N** of all positive integers into **Z**, **R**, $F[x]$ (or another commutative group) connected by the relation

$$f(n) = \sum\nolimits_{d|n} g(d)$$

Then, it holds

$$g(n) = \sum\nolimits_{d|n} \mu(n|d) f(d).$$

This is the inverse formula for Möbius function. If we have two mappings $f, g : \mathbf{N} \longrightarrow G$ where G is a commutative group with multiplicative denotations and

$$f(n) = \prod\nolimits_{d|n} g(d)$$

then

$$g(n) = \prod f(d)^{\mu(n|d)}.$$

Using the inverse formula for Möbius function one can obtain the following expression for the number of monic irreducible polynomials of degree m over $GF(q)$

$$D_{m,q} = \frac{1}{m} \sum\nolimits_{d|n} \mu(d) q^{m|d}.$$

This number is called the Dedekind's number.

6 Wedderburn's theorem

We include the commutativity law in the definition of a field. When the commutativity law for multiplication in the definition of the field is omitted one has the skewfield.

The most important is the skewfield of quaternions **H**. It was first built by Hamilton in 1843. As a real vector space **H** is dimension 4 with the basis $\{\mathbf{1}, \mathbf{i}, \mathbf{j}, \mathbf{k}\}$, i.e.

$$\mathbf{H} = \mathbf{R} + \mathbf{iR} + \mathbf{jR} + \mathbf{kR},$$

where $\mathbf{i}, \mathbf{j}, \mathbf{k}$ are symbols which can be multiplied by the rule

$$\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -1, \quad \mathbf{ij} = \mathbf{k} = -\mathbf{jijk} = \mathbf{i} = -\mathbf{kjki} = \mathbf{j} = -\mathbf{ik}$$

The element $x = \alpha_0 + \alpha_1\mathbf{i} + \alpha_2\mathbf{j} + \alpha_3\mathbf{k}$ is called a quaternion. It can be immediately checked out that $\mathbf{H}$ is an associative ring with identity 1. For every quaternion $x \in \mathbf{H}$ one can define the conjugated quaternion $x^* = \alpha_0 - \alpha_1\mathbf{i} - \alpha_2\mathbf{j} - \alpha_3\mathbf{k}$. The product $xx^* = N(x)$ is called the norm of the quaternion x and equals $\alpha_0^2 + \alpha_1^2 + \alpha_2^2 + \alpha_3^2$. It is easily checked that for element $x^{-1} = x^*/N(x)$ the following holds $xx^{-1} = x^{-1} = 1$ i.e. x^{-1} is the inverse for the element x. All quaternions with zero coefficients at imaginary identities $\mathbf{i}, \mathbf{j}, \mathbf{k}$ form a field which is isomorphic to the field $\mathbf{R}$. Each element of this field commutes with any quaternion from $\mathbf{H}$ i.e. belongs to the center of $\mathbf{H}$. Thus, $\mathbf{H}$ is a division algebra over the field $\mathbf{R}$.

The famous theorem of Frobenius shows the importance of skewfield of quaternions in algebra:

Theorem 9. *Over the field of real numbers there exist only three finite dimensional associative division algebras:* $\mathbf{R}, \mathbf{C}, \mathbf{H}$.

In finite case there is no distinction between notions "field" and "skewfield" because of the well-known result:

Theorem 10. (Wedderburn) *Any finite skewfield is commutative.*

7 Finite fields and codes

Finite fields are widely used in finite geometries, combinatorics and computer science. They are very important in information and communication theory: signal processing, coding theory, cryptography. We only give a sketch of some ideas of coding theory.

7.1 General properties of codes

Long since people happened to decide a problem of protection of information from hindrances at transmission it on distance[1]. Probably, single reasonable decision of this problem is the attachment to a sent message

[1] It is clear that the same problem appears at storing information. However we shall analyze only the transmission process.

some additional information, which allows to detect and to correct possible distortions. Consider the simplest example.

Example 9. Suppose that we need to send a message A. To insure ourselves, we can double it and send a message block AA. We shall assume that appearing a hindrance at the transmission is sufficiently rare, so at least one of the copies will come to hand without errors. Then there are two possibilities:

1) the addressee gets a message AA; then he can consider the message as correct;

2) he gets a block AB or BA, where B is different from A, and then he can be assured that an error has occurred; however herewith he does not know, what from the messages, A or B, is right and, consequently, he can not correct the error .

If we shall transmit a triple block AAA, the addressee will get one of the messages AAA, AAB, ABA or BAA and will be able not only to detect an error, as well as correct its: it must consider as correct that message, which is contained in the block not less two times.

Formalize now our problem. It is usually expected that process of transmission of information yields the following three conditions:

1) The information is presented as a sequences of words of the same length, constituted of symbols 0 and 1; thereby, it is possible to consider these words as elements of a linear space V over the field $F(2)$. More generally, we can consider vectors over an arbitrary finite field $F(p^m)$.

2) Errors, which are aroused as a result of hindrances, are considered as independent random variables.

3) For checking errors the following trick is used: to each word A, which we want to send, a word $\tilde{A}$ is added (of fixed length too) , hanging from A, and then the word $A\tilde{A}$ will be sent. An addressee, knowing dependency $\tilde{A}$ from A, defines, whether an error has aroused at the transmission.

Words $A\tilde{A}$, A and $\tilde{A}$ are called *a code word, an message part* and *a check part* accordingly. The set of all code words is called *a code*. If $|A| = k$ [2] and $|A| + |\tilde{A}| = n$, the code is called a *(n, k)-code*. Therefore, a (n, k)-code is a subset of a n-dimensional linear space V over the finite field.

Example 10 (checking parity). Let an message part $A = a_1 \dots a_k$ is a k-dimensional vector over $F(2)$ and $\tilde{A}$ consists of one symbol $b = a_1 +$

[2] By $|A|$ the length of the word A is denoted.

$\ldots + a_k(mod2)$. If in the received word the last bit is not equal to the sum of preceding ones, then it is doubtless that an error has occurred at the transmission.

In the last example the code is a hyperplane in a $(k+1)$-dimensional linear space, given by the equation $x_1 + \ldots + x_k = 0$.

From the example 9 and following reasoning it is clear that increasing the length of a check part of a code word, we can detect and correct a greater number of errors. However for such improvement we have to pay a send rate of information. So at the building and analysis of codes their parameter is taken into account - the *rate of a code*, which is equal to k/n, where n is the length of a code word, k is the length of its message part. In the example 9 the rate of the code is $1/2$, whereas in the example 10 it equals $k/(k+1)$.

Other important parameter is the code separation. If $A = a_1 \ldots a_n$ and $B = b_1 \ldots b_n$ are vectors, by a *distance* between them a number pairs of corresponding symbols (a_i, b_i) , different one from another, is called. The distance is denoted by $\rho(A,B)$. For instance, if $A = 00110$, $B = 10100$ then $\rho(A,B) = 2$. For $\rho(A,B)$ usual axioms of the distance are fulfilled:

$$\begin{aligned}
&\rho(A,B) = \rho(B,A),\\
&\rho(A,B) \geq 0,\\
&\rho(A,B) = 0 \Longleftrightarrow A = B,\\
&\rho(A,C) \leq \rho(A,B) + \rho(B,C).
\end{aligned}$$

A *separation* of a code C is the number

$$\rho(C) = min\{\rho(A,B) |\ A, B \epsilon C, A \neq B\}.$$

There is connection between the separation of a code and detection/correction of errors. If it has occurred t errors at transmission of the word A, the received word B differs from A in t positions: i. e. $\rho(A,B) = t$. So under rather greater value of $\rho(C)$ the word B does not coincide with any element from C and an addressee, getting the word B, can be assured that it contains errors. Moreover, if $\rho(B,C) > t$ for all words $C \epsilon C$, $C \neq A$, the word A is uniquely defined by B, and errors which appeared at the transmission can be corrected. This reasoning brings us to a simple, but important statement:

Theorem 11. *If $\rho(C) \geq d$ $(d \epsilon \mathrm{N})$, the code C detects $d-1$ errors and corrects $\left[\frac{d-1}{2}\right]$ errors (here $[x]$ denotes the integer part of the number x).*

Remark. This theorem shows that both of problems – a detecting and correction of errors – are similar. We shall deal only with the last below.

It is clear that codes with the big value $\rho(C)$ are more preferred. However increasing the separation of a code draws a decrease of rate of the code. It is not a single contradiction in Coding Theory. From the standpoint of an engineer a condition of *efficiency of a code* is very important too: encoding and decoding devices must be technically rather simple. Requirement of efficiency of a code is one of the reasons: because of which codes are usually considered as subsets of vector spaces over fields, rather then, generally speaking, of modules over rings.

7.2 Linear codes

In this subsection we shall consider only codes over $F(2)$. Let C be a (n,k)-code contained in a vector space V $(dim\, V = n)$. C is called *linear*: if it is a subspace in V.

For a linear code the determination of the separation of a code $\rho(C)$ is simplified. Define a *weight* of a vector $x \in V$ as the number $w(x)$ of its nonzero coordinates. Then $\rho(x,y) = w(x-y)$, whence it follows

Lemma 1. *If* C *is a linear code then* $\rho(C) = min\{w(x) |\ x \in C,\ x \neq 0\}$.

Since check symbols of a code word are defined by its message part, the linear code will be determined by the equation

$$Hx = 0, \qquad (1)$$

where $x \in V$ and H is a $(n-k) \times n$-matrix of rank $n-k$, which is called a *check matrix*.

Using the check matrix, we can find out, when the separation of the code equals 1. In this case by Lemma 1 there is a vector $x \in C$, all of whose coordinates but one (say, the ith) equal 0. But according to (1) this is possible, only if the ith column of H is zero. Therefore $\rho(B,C) \geq 2$ if and only if H contains no zero columns. Similarly, there is a vector of the weight 2 in C if and only if H has two equal columns. Now it follows from Theorem 11 for $d = 3$:

Theorem 12. *If* H *does not contain equal columns and all its columns are nonzero then* C *corrects any single error.*

Such simple characterization of linear codes, correcting one error, allows us to build those of them, which possess the most rate. To do this we fix a length $r = n - k$ of the check part. Then maximal length of words of a code, satisfying Theorem 12, is $2^r - 1$ (in this case the matrix H contains all $2^r - 1$ different nonzero columns of height r). The codes with such matrices are called *Hamming codes.* Their rate is equal to $1 - \frac{r}{2^r-1}$ and they are enough efficient in the meaning that was spoken in the end of preceding subsection about.

Example 11. A minimal Hamming code is obtained for $r = 1$, $n = 3$. The matrix H is of the form

$$H = \begin{pmatrix} 110 \\ 101 \end{pmatrix},$$

and the system of the equations is reduced to the equality $x_1 = x_2 = x_3$. So in this case encoding is realized by the tripling of each symbol (see example 9).

7.3 BCH-codes

Building of efficient codes which correct at least two errors, turns out to be a more difficult problem and requires to use the theory of finite fields. The first such codes were built by Bose, Chaudhuri and Hoquenghem in 1959-1960 and are called BCH-codes after the names of their authors. They are a generalization of Hamming codes and also turn out to be linear. Moreover, they belong to the class of so called polynomial codes. We will begin our consideration with just this class.

Let integer positive numbers $k, n \in \mathbf{N}$, $k < n$ and a polynomial $f(t) = f_0 + f_1 t + ... + f_k t^k$ over $F(2)$ be fixed. Besides, let U, V be vector spaces over $F(2)$, $dim\, U = n - k$, $dim\, V = n$. Compare to each vector $a = (a_0, ..., a_{n-k-1}) \in U$ a polynomial $a(t) = a_0 + a_1 t + ... + a_{n-k-1} t^{n-k-1}$. Then the polynomial $b(t) = a(t)f(t)$ can be identified with a vector from V. So the subset $C_f = \{a(t)f(t)|\ a \in U\} \subset V$ may be consider as a code.[3] It is called a *polynomial code.* Evidently, a polynomial code is linear.

As in the preceding subsection the *weight* of a polynomial $g(t)$ is the number $w(g)$ of its nonzero coefficients. From Lemma 1 it follows at once **Lemma 2.** $\rho(C_f) = min\{w(af)|\ a \neq 0, deg\, a \leq n - k - 1\}$.

[3] It needs to require additionally that f_0 and f_k did not be equal to zero, otherwise the first and last coordinates of the code vectors will carry no information.

In what follows the next assertion plays the main role for BCH-codes:
Theorem 13. *Let ε be a primitive root of nth degree out of 1, g be a polynomial different from 0, $deg\, g < n$. Suppose that $\varepsilon, \varepsilon^2, ..., \varepsilon^{d-1}$ are roots of the polynomial g for certain $d \leq n$. Then $w(g) \geq d$.*
Proof. Since $d \leq n$, all numbers $\varepsilon, \varepsilon^2, ..., \varepsilon^{d-1}$ are different. Assume that $w(g) \leq d-1$. Then g can be presented in the form $g(t) = \sum_{i=1}^{s} \alpha_i t^{k_i}$, where $s < d$, $0 \leq k_1 < ... < k_s \leq n-1$ and $\alpha_i \neq 0$ for all i. From the condition of Theorem we get the system of equations

$$g\left(\varepsilon^l\right) = \sum_{i=1}^{s} \alpha_i \left(\varepsilon^{k_i}\right)^l = 0 \qquad (1 \leq l \leq s),$$

which is linear relatively to $\alpha_1, ..., \alpha_s$. Since this system has a nonzero solution,

$$\begin{vmatrix} \varepsilon^{k_1} & \dots & \varepsilon^{k_s} \\ \varepsilon^{2k_1} & \dots & \varepsilon^{2k_s} \\ \dots & \dots & \dots \\ \varepsilon^{sk_1} & \dots & \varepsilon^{sk_s} \end{vmatrix} = 0$$

From properties of van der Monde's determinant it follows that $\varepsilon^{k_i} \neq \varepsilon^{k_j}$ for some $i \neq j$. But this is impossible because $k_i, k_j < n$.

Now we can pass on the building BCH-codes. Choose a generator of the multiplicative group of $F(2^m)$ (which is cyclic by theorem 6) as ε. Then ε is a primitive root of degree $n = 2^m - 1$. Fix certain $d \leq n$. Denote by f_i the minimal polynomial over $F(2)$ of the element ε^i $(1 \leq i \leq d-1)$ and set f =g.c.d.$(f_1, ..., f_{d-1})$. Then by Theorem 13, $w(a\,f) \geq d$ for any polynomial $a(t) \neq 0$ such that $\deg(a\,f) < n$. We obtain the polynomial code $C_f = \{a(t)f(t) |\ deg\, a \leq n-1-deg\, f\}$ of the length n with the check part of the length deg f and with the separation of the code $\geq d$. It is called a *BCH-code*.

Further on, since the map $x \longrightarrow x^2$ is an endomorphism of $F(2^m)$ (see example 8) $(h(x))^2 = h(x^2)$ for any polynomial h and any $x \in F(2^m)$. So $f_i(\varepsilon^{2i}) = 0$ and, therefore f_i and f_{2i} coincide for $2i \leq d-1$, since both these polynomials are irreducible. So there are amongst polynomials $f_1, ..., f_{d-1}$ no more than $d/2$ different ones. Hence deg $f_i \leq m = [F(2^m) : F(2)]$ for all $i \leq d-1$, since f_i are irreducible. Consequently, deg $f \leq md/2$.

Thereby, *the built BCH-code has the length* $2^m - 1$ *and corrects* $\left[\frac{d-1}{2}\right]$ *errors. Its check part has length* $\leq md/2$, *so the rate of the code is not less than*

$$1 - \frac{md}{2\,(2^m - 1)}.$$

Example 12. Let $m = 3$, ε be a primitive root of degree $2^3 - 1 = 7$. Its minimal polynomial is of the form $f_1(t) = t^3 + t + 1$, moreover $f_1(\varepsilon^2) = 0$, $f_1(\varepsilon^3) \neq 0$, i.e. $d = 3$. Since $f_1 = f_2$ then $f = f_1$. So the encoding is realized by the transformation

$$(\alpha_0, \alpha_1, \alpha_2, \alpha_3) \longrightarrow (\alpha_0, \alpha_0 + \alpha_1, \alpha_1 + \alpha_2, \alpha_0 + \alpha_2 + \alpha_3, \alpha_1 + \alpha_3, \alpha_2, \alpha_3)$$

If we denote the vector on the right side by $(\beta_0, \beta_1, ..., \beta_6)$ and exclude alphas, we obtain the system of equations which defines the code as a subspace:

$$\begin{cases} \beta_0 + \beta_1 + \beta_2 + \beta_5 = 0 \\ \beta_2 + \beta_4 + \beta_5 + \beta_6 = 0 \\ \beta_0 + \beta_3 + \beta_5 + \beta_6 = 0 \end{cases}$$

Its check matrix is of the form

$$H = \begin{pmatrix} 1110010 \\ 0010111 \\ 1001011 \end{pmatrix}.$$

i.e. our code is a Hamming code. This is not accidental: it can show that all Hamming codes are BCH-codes.

Here is an example of a BCH-code, not being the Hamming one.

Example 13. Set $d = 5$, $m = 4$, $n = 2^4 - 1 = 15$. Minimal polynomials for primitive elements of $F(2^m)$ are of the form $g(t) = t^4 + t + 1$ and $h(t) = t^4 + t^3 + 1$. Let $f_1 = g$. As it is proved above $f_2 = f_4 = f_1$. Besides, $f_3(t) = t^4 + t^3 + t^2 + t + 1$ because $(\varepsilon^3)^5 = 1$. So

$$f = \text{g.c.d.}(f_1, f_2, f_3, f_4) = \text{g.c.d.}(f_1, f_3) = f_1 f_3 = t^8 + t^7 + t^6 + t^4 + 1$$

and we obtain a (15,7)-code, which corrects 2 errors.

7.4 Conclusion

In this section we did not try to give some introduction to Coding Theory, but want to show only fragmentary relations of this theory with finite fields. Indeed, this connection is much deeper. First, there are many kinds of linear codes and analyzing each of them requires its own algebraic approach. Secondly, much attention is attracted to nonlinear codes in last decades, for which methods of Algebraic Geometry over finite fields are used. Finally, the nature of hindrances can be other: for instance, the condition of independence of errors can be not executed, and in this case other methods of building of codes are developed (but with using algebraic tools too).

At last we give a small reference list for the reader who will want to make the closer acquaintance with Coding Theory. Elementary introduction can be found in the book of G. Birkhoff and N. C. Bartee, Modern Applied Algebra, (New York, 1970).

The book [1] pays the greater attention to technical realization of different codes. The monography [11] is really an encyclopedia of Coding Theory (certainly, at the time of its publishing). The applying methods of Algebraic Geometry is shown in the work [18]. A modern introduction in Coding Theory is contained in [14]. Some special questions are considered in [16] and [5].

Bibliography

[1] **Berlekamp E.R.** *Algebraic coding theory* (revised edition), Aegean Park Press, Laguna Hills, Calif. (1984) .

[2] **Beth T., Jungnickel D., Lenz H.** *Design theory,* Cambridge University Press, (1986).

[3] **Blahut R.E.** *Theory and practice of error control codes,* Addison-Wesley, Reading, Mass. (1983).

[4] **Brawley J.V., Schnibben G.E.** *Infinite algebraic extensions of finite fields* AMS, Providence, R.I. (1989).

[5] **Cohen G., Honkala I., S. Litsyn, A. Lobstein,** *Covering codes,* North-Holland Publishing Co., Amsterdam, 1997.

[6] **Golomb S.W.,** *Shift register sequences* (Revised edition), Aegean Park Press, Laguna Hills, Calif. (1982).

[7] **Hartshorn R.** *Foundations of projective geometry,* W.A. Benjamin Inc. New York (1967).

[8] **Jungnickel D.** *Finite fields. Structure and arithmetics,* BI Wissenschaftsverlag, (1993).

[9] **Lidl R., Niederreiter H.** *Finite fields* Encyclopedia of Mathematics, Vol. 20. Cambridge University Press (1983).

[10] **Lueneburg H.** *Galois felder Kreisteilungskoerper und Schieberegisterfolgen,* Bibliographisches Institut, Mannheim (1979).

[11] **MacWilliams F.J. Sloane N.J.A..** *The theory of error-correcting codes,* North Holland. Amsterdam (1977).

[12] **McEliece R.J.** *Finite fields for computer scientists and engineeers,* Kluwer¡ Boston (1987) .

[13] **Menezes A., Blake I., Gao S., Mullin R., Vanstone S., Yaghoobian T.** *Applications of finite fields* Kluwer, Boston (1992).

[14] **Pappini O., Wolfmann J.** *Algebre discrete et codes correcteurs,* Springer Verlag. Berlin, 1995.

[15] **Pohst M., Zassenhaus H.** *Algorithmic algebraic number theory,* Cambridge University Press (1989).

[16] **Pretzel 0.** *Codes and algebraic curves,* Oxford Univ. Press, NY, 1998.

[17] **Schroeder M.R.** *Number theory in science and communication,* (2-nd ed.) Springer, New York, (1986).

[18] **Vladuts S.G., Yu.I.Manin** *Linear codes and modular curves,* Modern Problems of Mathematics, v.25, Moscow, 1984 (in Russian).