

FINITE RINGS

Aleksandr Nechaev

Center of New Informational Technologies
of Moscow State University, 119899, Russia;
e-mail: nechaev@cnit.msu.ru

Here we discuss properties of finite associative rings useful for the Theories of Linear Codes and other applications. We consider only associative rings.

Main problems of the Theory of FR:

- the description up to isomorphism;
- the investigation of the constructions of FR with different additional conditions;
- the solution of problems of linear algebra in modules over FR;
- the description of identities of FR and polynomial functions on FR.

SELECTED LIST OF SOME AUTHORS:

LAGRANGE, EULER, GALOIS,
MOLIEN, WEDDERBURN, KRULL, ARTIN, DEURING, DIKSON, HENSEL,
SCHNEIDMÜLLER,
ALBERT, GILMER, SNAPPER, JANUSH, KORBAS, RAGHAVENDRAN, KRUSE,
PRICE, ELDRIDGE, HUNGERFORD, JATEGAONCAR, NAGATA,
McDONALD, ELIZAROV, MARKOV, NECHAEV, CLARK, DRAKE, JAIN, LVOV,
MAL'CEV, WIESENBAUER, FISHER
ARCHIPOV, ANTIPKIN, RYBKIN, RATINOV, FINKELSTEIN, KURAKIN,
GREFERATN, HONOLD, LOPEZ-PERMOUTH, WOOD...

PLAN.

PART 1. CONSTRUCTION OF FINITE RINGS.

1.1 NILRADICAL, SEMI-SIMPLE RINGS.

1.2 QUASI-IDENTITY AND MODULAR RADICAL.

1.3 WEDDERBURN'S RADICAL, W-RINGS.

1.4 LOCAL RINGS.

1.5 FINITE RINGS WITH DIFFERENT CONDITIONS

PART 2. PRINCIPAL IDEAL RINGS.

2.1 GENERAL CONSTRUCTION OF PIR.

2.2 FINITE CHAIN RINGS.

(GALOIS RINGS. COMMUTATIVE CHAIN RINGS.
NONCOMMUTATIVE CHAIN RINGS.)

1 PART 1. CONSTRUCTION OF FINITE RINGS

1.1 NIL-RADICAL, SEMI-SIMPLE RINGS

A left ideal $I \leq {}_R R$ of a ring R is called **nil-ideal** if every element of I is nilpotent and it is called **nilpotent** if $I^n = 0$ for some $n \in \mathbb{N}$.

We define **nil-radical** of R :

$\mathfrak{N}(R)$ = sum of all left (right) nil-ideals of R ;

Jacobson radical of R :

$\mathcal{J}(R)$ = intersection of all maximal left (right) ideals of R .

Proposition 1.1. *For any f.r. R every nil-ideal is nilpotent and $\mathfrak{N}(R) = \mathcal{J}(R)$ is a two-sided nilpotent ideal. There are relations*

$$\mathfrak{N}(\mathfrak{N}(R)) = \mathfrak{N}(R), \quad (\overline{R} = R/\mathfrak{N}(R)) \Rightarrow \mathfrak{N}(\overline{R}) = 0,$$

$$I \triangleleft R \quad \Rightarrow \quad \mathfrak{N}(I) = I \cap \mathfrak{N}(R).$$

Example 1.2. Let $R = \mathbb{Z}_m$, $m \in \mathbb{N}$, $m = p_1^{k_1} \cdot \dots \cdot p_t^{k_t}$. Then $\mathfrak{N}(R) = nR$, where $n = p_1 \cdot \dots \cdot p_t$.

A f.r. R is called **semisimple** if $\mathfrak{N}(R) = 0$.

Theorem 1.3. (*Molien-Wedderburn-Artin*) A f.r. $R \neq 0$ is **semisimple** iff it is a direct sum of full matrix rings over fields:

$$R = M_{n_1}(P_1) \oplus \dots \oplus M_{n_t}(P_t), \quad P_s = GF(q_s), \quad s \in \overline{1, t}. \quad (1)$$

An important class of semisimple f.r. gives

Theorem 1.4. (*Maschke*) Let $P = GF(q)$ and G be a finite group of order $|G| = n$. Then group ring

$$PG \text{ is semisimple} \Leftrightarrow (q, n) = 1.$$

For a f.r. R a quotient ring $\overline{R} = R/\mathfrak{N}(R)$ is called **top factor** of R . Theorem 1.3 imply that if $\overline{R} \neq 0$, then

$$\overline{R} = M_{n_1}(P_1) \oplus \dots \oplus M_{n_t}(P_t), \quad P_s = GF(q_s), \quad s \in \overline{1, t}. \quad (2)$$

A f.r. R with identity is called **primary** (or **semi-local**) if in (2) $t = 1$; R is called **completely primary** (or **local**) if $t = 1, n_1 = 1$.

Proposition 1.5. *Let R be a primary f.r. Then $R = M_n(S)$, where S is a local ring. If in addition $R = M_k(T)$, where T is a local ring, then $k = n$, $T \cong S$.*

There is a question: is any f.r. with identity a direct sum

$$R = M_{n_1}(S_1) \oplus \dots \oplus M_{n_t}(S_t), \quad t \geq 1,$$

of full matrix rings over a local rings S_k ? Answer is negative.

1.2 QUASI-IDENTITY AND MODULAR RADICAL.

We cannot assert that any f.r. R with $\bar{R} \neq 0$ contains the identity. However there are some main approximations to an identity of R .

Let $S \subseteq R$ and $\lambda_R(S), \rho_R(S)$ be the left and right annihilators of S in R . We call **quasi-identity** such $e = e^2 \in R$ that $\lambda_R(e) \cup \rho_R(e)$ does not contain nonzero idempotents, i. e. $\lambda_R(e) \cup \rho_R(e) \subseteq \mathfrak{N}(R)$.

Proposition 1.6. *Any f.r. R contains a quasi-identity e . Let $\mathcal{M}(R) = \lambda_R(e)R + R\rho_R(e) \triangleleft R$. Then $\mathcal{M}(R) \triangleleft \mathfrak{N}(R)$ and for any ideal $I \triangleleft R$ the following conditions are equivalent:*

- (a) *quotient ring $\tilde{R} = R/I$ has identity;*
- (b) *the image \tilde{e} of the quasi-identity e in \tilde{R} is identity of \tilde{R} ;*
- (c) $\mathcal{M}(R) \subseteq I$;

Ideal $\mathcal{M}(R) = \lambda_R(e)R + R\rho_R(e)$ does not depend on the choice of the quasi-identity e and is called a **modular radical** of R .

Let $D_l(R)$ ($D_r(R)$) be the set of all left (right) zero divisors of R .

Corollary 1.7. *For a f.r. R with quasi-identity e there are equivalent:*

(a) R is a rind with identity;

(b) e is identity of R ;

(c) $\mathcal{M}(R) = 0$;

(d) the set $R \setminus (D_r(R) \cup D_l(R))$ of regular elements is nonempty;

Under these conditions $D_r(R) = D_l(R) \neq R$ and $R^* = R \setminus D_r(R)$.

1.3 WEDDERBURN'S RADICAL, W-RINGS.

$$\overline{R} = M_{n_1}(P_1) \oplus \dots \oplus M_{n_t}(P_t), \quad P_s = GF(q_s), \quad s \in \overline{1, t} \quad (2)$$

there exists an orthogonal system of idempotents $e_1, \dots, e_t \in R$ such that \bar{e}_k is the identity of $M_{n_k}(P_k)$, $k \in \overline{1, t}$. Then $e = e_1 + \dots + e_t$ is a quasi-identity of R and the latter is a direct sum of subgroups :

$$R = R_1 \oplus \dots \oplus R_t \oplus \mathcal{N} \quad (\mathbf{Pierce\ decomposition}),$$

where $R_k = e_k R e_k = M_{n_k}(S_k)$, S_k is a local f.r., $\overline{S_k} = P_k$, $k \in \overline{1, t}$, and $\mathcal{N} = \lambda_R(e) + \rho_R(e) + \sum_{i \neq j} e_i R e_j$ is a subring of $\mathfrak{N}(R)$.

A f.r. R is called **Wedderburn** - or **W - ring**, if $R = 0$, or

$$R = M_{n_1}(S_1) \oplus \dots \oplus M_{n_t}(S_t), \quad t \geq 1. \quad (3)$$

Theorem 1.8. *For a f.r. R with left identity there are equivalent:*

- (a) *R is a Wedderburn ring;*
- (b) *any two-sided idempotent ideal of R is left principal;*
- (c) *for any idempotent $f \in R$ the ideal RfR is left principal.*

Theorem 1.9. *Any f.r. R contains ideal $\mathcal{W} = \mathcal{W}(R)$ such that*

$$\forall I \triangleleft R \quad (R/I \text{ is a W-ring}) \quad \iff \quad (\mathcal{W} \subseteq I).$$

We call $\mathcal{W}(R)$ **Wedderburn radical of R** . There are inclusions $\mathcal{M}(R) \subseteq \mathcal{W}(R) \subseteq \mathfrak{N}(R)$, (each can be strict).

1.4 LOCAL RINGS

So the description of finite rings with identity is reduced modulo some nilpotent ideal to the description of local finite rings (LFR).

Theorem 1.10. *For a f.r. S with identity: there are equivalent*

- (a) S is a LFR;
- (b) S does not contain proper idempotents;
- (c) $S \setminus S^*$ is a subgroup of the group $(S, +)$;
- (d) $\mathfrak{N}(S) = S \setminus S^*$.

Let S be a LFR, $\overline{S} = GF(q)$, $q = p^r$, p be a prime and n be the nilpotency index of the ideal $\mathfrak{N}(S)$. Then S contains a strictly descending chain of ideals

$$S \triangleright \mathfrak{N}(S) \triangleright \dots \triangleright \mathfrak{N}(S)^t \triangleright \dots \triangleright \mathfrak{N}(S)^{n-1} \triangleright 0,$$

and for some integer $1 \leq d \leq n \leq c$ we have

$$\text{char}S = p^d, \quad |S| = q^c, \quad |\mathfrak{N}(S)| = q^{c-1}.$$

$$S \triangleright \mathfrak{N}(S) \triangleright \dots \triangleright \mathfrak{N}(S)^t \triangleright \dots \triangleright \mathfrak{N}(S)^{n-1} \triangleright 0.$$

The factors $\mathfrak{N}_t = \mathfrak{N}(S)^t / \mathfrak{N}(S)^{t+1}$, $t \in \overline{0, n-1}$, are left and right spaces over \overline{S} ,

$$\dim_{\overline{S}} \mathfrak{N}_t = \dim \mathfrak{N}_{t\overline{S}} = m_t, \quad t \in \overline{0, n-1}, -$$

Loevy invariants of LFR S . We have:

$$|\mathfrak{N}(S)^t| = q^{m_t + \dots + m_{n-1}}, \quad t \in \overline{0, n-1}$$

. Commutative local rings firstly was studied by Krull (1922, [5, 6]).

EXAMPLES of LFR. $GF(q)$, \mathbb{Z}_{p^n} , $GF(q)[x]/(f(x))$, where $f(x) \in GF(q)[x]$ is a degree of an irreducible polynomial, and more general:

Finite chain rings: LFR with $m_1 = 1$;

Galois rings (LFR with $\mathfrak{N}(S) = pS$).

Up to now (2008) we have no full description of LFRs.

1.5 RINGS OF FIXED ORDER, NILPOTENT AND OTHERS.

A f.r. R is called **decomposable**, if it is a direct sum of two nonzero two-sided ideals, and **indecomposable** in other case.

Theorem 1.11. *Any f.r. is a direct sum of indecomposable ideals:*

$$R = A_1 \oplus \dots \oplus A_s, \quad s \geq 1$$

. Such a decomposition is defined uniquely up to permutation and isomorphism of items, and for a ring with identity — uniquely up to permutation of items.

Here each item A_i is a p_i -ring for some prime p_i , i.e. a ring of the order $p_i^{n_i}$, $n_i \in \mathbb{N}$. A f.r. with identity is decomposable exactly if it contains a proper central idempotent.

Let $\mathcal{N}(k)$ ($\mathcal{N}_e(k)$, $\mathcal{N}_0(k)$) be the set of classes of isomorphic indecomposable rings (correspondingly rings with identity, nilpotent rings) of order k ; let $[R]$ be a class of rings isomorphic to R ; $(G)_0$ be a ring with zero multiplication on abelian group G . Then for any prime p

$$|\mathcal{N}(p)| = 2; \quad \mathcal{N}_e(p) = \{[GF(p)]\}; \quad \mathcal{N}_0(p) = \{[(\mathbb{Z}_p, +)_0]\}.$$

$$|\mathcal{N}(p^2)| = 9; \quad \mathcal{N}_e(p^2) = \{[GF(p^2)], [GF(p)[x]/(x^2)], [\mathbb{Z}_{p^2}]\};$$

$$\mathcal{N}_0(p^2) = \{[(\mathbb{Z}_p \oplus \mathbb{Z}_p)_0], [(\mathbb{Z}_{p^2}, +)_0], [p\mathbb{Z}_{p^3}], [xGF(p)[x]/(x^3)]\}.$$

$$|\mathcal{N}(2^3)| = 32, \quad |\mathcal{N}_e(2^3)| = 7, \quad |\mathcal{N}_0(2^3)| = 18;$$

$$|\mathcal{N}(p^3)| = 3p + 30, \quad |\mathcal{N}_1(p^3)| = 8, \quad |\mathcal{N}_0(p^3)| = 3p + 15, \quad \text{for } p \geq 3.$$

Parameters $|\mathcal{N}_x(p^4)|$ have different expressions already for the cases: $p = 2, 3$, $p \equiv 1 \pmod{3}$, $p \equiv 2 \pmod{3}$ (Elizarov, 1993, [13]).

For $n \rightarrow \infty$ we have equivalence of functions (Knopfmacher 1975):

$$|\mathcal{N}(p^n)| \sim |\mathcal{N}_0(p^n)| \sim p^{(4/27)n^3}$$

. So “almost all” f.r. of the given order are nilpotent.

However nilpotent rings are difficult for investigation. Results of Kruse, Price (1976 [13,14]) give a chance to classify nilpotent rings of order p^4 . If R is an indecomposable right principal ideal ring and $R^n = 0, R^{n-1} \neq 0$, then R is a commutative chain ring and $|R| = p^n$ for a prime p .

A nilpotent f.r. R of characteristic m can be considered as an ideal of a f.r. $R' = R \times \mathbb{Z}_m$ with identity $(0, 1)$, having componentwise addition and multiplication defined by the equality

$$(r, k)(s, l) = (rs + rl + ks, kl).$$

There exists a description of FRs with any of the following properties:

- (a) the group $(R, +)$ or R^0 is cyclic (McDonald, 1974 [3]);
- (b) the group R^* is cyclic (**Gilmer ring**, 1973 [3]);
- (c) $|D_r(R)|^2 = |R|$ (**Corbas ring** (Corbas, 1969 [3]));
- (d) the product of any two zero divisors is zero (Corbas, 1970 [3]);
- (e) R is non-nilpotent and $(R, +)$ is a group of type (p^a, p^b) , or (p^a, p^b, p) (Elizarov, 1985-93 [12, 13]).

The results about p -rings with a given type of additive group see also in (Flor, Wiesenbauer, Elizarov, Antipkin, 1974-82 [15, 16, 17]).

If $|R| = p^k$, p — prime, $k \leq 4$, then $R \leq M_n(S)$ for some commutative ring S , but it is false for $k \geq 5$ (Sychovich, 1985) .

2 PART 2. PRINCIPAL IDEAL RINGS

A f.r. R with identity is called **left principal ideal ring (LPIR)** if any left ideal $I \leq {}_R R$ is a left principal: $I = Ra$; it is called **principal ideal ring (PIR)** if it is LPIR and RPIR.

2.1 GENERAL CONSTRUCTION OF PIR

Theorem 2.1. (Nechaev, 1973 [7]): *For a f.r. R with identity are equivalent*

- (a) R is a left PIR;
- (b) any two-sided ideal of R is a left principal;
- (c) R is PIR;
- (d) R is a W -ring with W -decomposition of a form

$$R = M_{n_1}(S_t) \oplus \dots \oplus M_{n_t}(S_t), t \geq 1, \quad (2)$$

where $S_i (i \in \overline{1, t})$ is a local PIR.

This result common with Theorem 1.8 give interesting pair of specific for finite rings results of type

LEFT \Rightarrow RIGHT.

2.2 FINITE CHAIN RINGS.

A ring S is called a

left chain ring if the lattice of all its left ideals is a chain;

chain ring if S is a left and right chain ring.

Theorem 2.2. *For a f.r. S with identity the following conditions are equivalent:*

(a) S is a local PIR;

(b) S is a chain ring;

(c) S is a left chain ring;

(d) S is a local f.r. with Loewy invariants $m_1 = \dots = m_n = 1$;

(e) S is a local f.r. with $m_1 = 1$;

(f) S is a local f.r. and $\mathfrak{N}(R)$ is a left principal ideal;

(g) the lattice of all one-sided ideals of S is a chain

$$S \triangleright \mathfrak{N}(S) \triangleright \dots \triangleright \mathfrak{N}(S)^t \triangleright \dots \triangleright \mathfrak{N}(S)^{n-1} \triangleright 0.$$

for some $n \in \mathbb{N}$.

The simplest, most investigated and most important in theory and applications finite chain rings are

2.2.1 GALOIS RINGS.

(Krull, Janush, Raghavendran, Nechaev, Kuzmin, Kurakin)

If R is a f.r. with identity then $D_l(R) = D_r(R) = D(R) = R \setminus R^*$ is the set of all two-sided zero divisors of R .

The shortness definition of a GR: a f.r. R with identity e is called a **Galois Ring (GR)** if $D(R) = \lambda R$ for some $\lambda \in \mathbb{N}$.

Theorem 2.3. *Let R be a GR. Then R is a commutative local PIR and there exist prime p and $r, n \in \mathbb{N}$ such that*

$$\mathfrak{N}(R) = R \setminus R^* = pR;$$

the top factor $\overline{R} = R/\mathfrak{N}(R)$ is $\overline{R} = GF(q)$, $q = p^r$.

The lattice of all ideals of R is a chain

$$R \triangleright \mathfrak{N} = pR \triangleright \dots \triangleright \mathfrak{N}^t = p^t R \triangleright \dots \triangleright \mathfrak{N}^n = p^n R = 0.$$

There are equalities: $\text{char } R = p^n$, $|R| = q^n$,

$$|R^*| = q^{n-1}(q-1), \quad |p^i R| = q^{n-i}, \quad i \in \overline{0, n}.$$

Theorem 2.4. For any $n, r \in \mathbb{N}$ and for every prime $p \in \mathbb{N}$ there exists unique up to isomorphism GR R of the characteristic p^n consisting of q^n elements, where $q = p^r$.

DENOTATION: $R = GR(q^n, p^n)$ (sometimes $R = GR(r, p^n)$) [7,31-33].

SIMPLEST EXAMPLES: $GF(q) = GR(q, p)$, $\mathbb{Z}_{p^n} = GR(p^n, p^n)$.

CONSTRUCTION. A monic polynomial $F(x) \in R[x]$ is called a **Galois polynomial (GP)** if its image $\overline{F}(x)$ under the natural epimorphism $R \rightarrow \overline{R} = R/pR = GF(q)$ is irreducible in $\overline{R}[x]$.

Theorem 2.5. Let $R = GR(q^n, p^n)$ and $F(x) \in R[x]$ be a GP of the degree m . Then

$$S = R[x]/F(x)R[x]$$

is a GR: $S = GR((q^m)^n, p^n)$, contained all roots of any GP

$G(x) \in R[x]$ such that $\deg G \mid m$. For $\xi \in S$ the equality $S = R[\xi]$ holds iff ξ is a root of some GP $G(x) \in R[x]$ of the degree m .

We call S a **Galois extension of GR R of the degree m** .

Any GR $R = GR(q^n, p^n)$, $q = p^r$, is a Galois extension of the degree r of the subring \mathbb{Z}_{p^n} .

Teichmüller- or p-adic coordinate set of $R = GR(q^n, p^n)$:

$$\Gamma(R) = \{\alpha \in R : \alpha^q = \alpha\}, \quad |\Gamma(R)| = q.$$

Any $a \in R$ has unique **p-adic decomposition**:

$$a = a_0 + a_1p + \dots + a_{n-1}p^{n-1}, \quad a_s = \gamma_s(a) \in \Gamma(R), \quad s \in \overline{0, n-1}.$$

$\gamma_s : R \rightarrow \Gamma(R)$ — **s-th p-adic coordinate function**.

The set $\Gamma(R)$ is closed relative to multiplication in R but not relative to addition. Algebra $(\Gamma(R), \oplus, \cdot)$ with operation \oplus , defined by

$$\alpha \oplus \beta = \gamma_0(\alpha + \beta)$$

, is a field of q elements. For any $\alpha, \beta \in \Gamma(R)$ there holds the equality

$$\gamma_1(\alpha + \beta) = \sum_{i \in \overline{1, p-1}} \oplus \left((-1)^i / i \right) \alpha^{p^{r-1}i} \beta^{p^{r-1}(p-i)} \quad (\text{Kuzmin, Nechaev 1995, [33]}).$$

If $R = \mathbb{Z}_p^n$ then $\Gamma(R)$ not equals to usual **p-ary coordinate set** $\overline{0, p-1}$. We have

$$\Gamma(R) = \{0, 1^{p^{n-1}} = 1, 2^{p^{n-1}}, \dots, (p-1)^{p^{n-1}}\},$$

$$\Gamma(R) = \overline{0, p-1} \iff (p = 2 \text{ or } n = 1).$$

MULTIPLICATIVE GROUP of $R = GR(q^n, p^n)$ is a direct product

$$R^* = \Gamma(R)^* \times (e + pR)$$

of a cyclic group $\Gamma(R)^* = \Gamma(R) \setminus 0$ of the order $q - 1$ and a

p -group $e + pR$, The latter is a direct product of cyclic subgroups (Raghavendran, 1969, [32])

of the orders p^{n-1}, \dots, p^{n-1} , if $p > 2$ or $p = 2, n = 2$,

and orders $2, 2^{n-2}, 2^{n-1}, \dots, 2^{n-1}$, if $p = 2, n > 2$.

GROUP $Aut(R)$ OF AUTOMORPHISMS OF R is a cyclic group of the order r generated by automorphism σ , acting on element

$$a = \sum_{i=0}^{n-1} a_i p^i, \quad a_i = \gamma_i(a), \quad \text{by the rule } \sigma(a) = \sum_{i=0}^{n-1} a_i^p p^i$$

(Frobenius automorphism).

A subring $K < R$ is a GR iff $K = R_\tau = \{a \in R : \tau(a) = a\}$ for some $\tau \in Aut(R)$. In such case $K = GR(p^{tn}, p^n)$, $t = m / \text{ord } \tau$ (Nechaev, 1973, [7]).

Let $R < S = GR(q^{mn}, p^n)$ be a Galois extension of the ring R of the degree m . Then the group $Aut(S/R)$ of automorphisms of S over R is a cyclic group $Aut(S/R) = \langle \sigma \rangle$ of the order m generated by automorphism σ , acting on the element $\alpha \in S$ with p -adic decomposition $\alpha = \sum_{i \in \overline{0, n-1}} \alpha_{s_i} p^i$ as $\sigma(\alpha) = \sum_{i \in \overline{0, n-1}} \alpha_{s_i}^q p^i$.

TRACE from the Galois extension S of the GR R is defined as a function

$$Tr_R^S(x) = \sum_{\tau \in \text{Aut}(S/R)} \tau(x).$$

It is epimorphism of modules $Tr_R^S : {}_R S \rightarrow {}_R R$ [7]. In different applications there are important coordinate functions $\gamma_s(Tr_R^S(x))$. Some expressions for these functions are known (Kuzmin, Nechaev, 1995, [33]). For example:

$$\gamma_0(Tr_R^S(x)) = tr_{\Gamma(R)}^{\Gamma(S)}(\gamma_0(x)) = \gamma_0(x) \oplus \gamma_0(x)^q \oplus \dots \oplus \gamma_0(x)^{q^{n-1}};$$

$$\gamma_1(Tr_R^S(x)) = \Psi(\gamma_0(x)) \oplus tr_{\Gamma(R)}^{\Gamma(S)}(\gamma_1(x)), \text{ where}$$

$$\Psi(x) = \sum_{k_0 + \dots + k_{m-1} = p, k_i \in \overline{0, p-1}} \oplus \frac{1}{k_0! \dots k_{m-1}!} x^{p^{r-1}(k_0 + qk_1 + \dots + q^{m-1}k_{m-1})}.$$

If $p = 2$ we have $\Psi(x) = \varkappa(x)^{2^{r-1}}$, where

$$\varkappa(x) = \sum_{0 \leq i < j \leq m-1} \oplus x^{q^i + q^j}$$

is a quadratic function from the field $\Gamma(S) = GF(q^m)$ into $\Gamma(R) = GF(q)$. Namely this fact allows us to find linear presentation of binary Kerdock code and to describe the generalization of this code over any finite field of the characteristic 2.

Any LFR S with $\overline{S} = GF(q)$, $char S = p^d$, contains a subring $R = GR(q^d, p^d)$ such that $\overline{S} = \overline{R}$. It allows to investigate S as an (R, R) -bimodule. Here is useful the following

Theorem 2.6. [7] *For any finite (R, R) -bimodule ${}_R M_R$ there exist a generator system $\mu_1, \dots, \mu_k \in M$ and a system of automorphisms $\sigma_1, \dots, \sigma_k \in Aut(R)$, such that*

$$\forall a \in R, l \in \overline{1, k} : \mu_l a = \sigma_l(a) \mu_l,$$

and

$$M = R\mu_1 \oplus \dots \oplus R\mu_k$$

is a direct sum of cyclic (R, R) -bimodules.

This **Theorem about distinguishing basis** allows to prove structure theorems for different classes of finite rings being considered as algebras over GR, in particular it allows to describe finite chain rings (see below) (Nechaev, [7]).

THE BASES OF IDENTITIES (BI) OF A GR $R = GR(q^n, p^n)$.

A polynomial $\Psi(x_1, \dots, x_k) \in \mathbb{Z}[x_1, \dots, x_k, \dots]$ is called **identity of the ring R** if

$$\forall r_1, \dots, r_k \in R \quad \Psi(r_1, \dots, r_k) = 0.$$

A system $\mathcal{B} \subset \mathbb{Z}[x_1, \dots, x_k, \dots]$ of identities is called **bases of identities (BI) of R (in class of associative-commutative rings)** if any identity of R can be deduced from \mathcal{B} by compositions and change of variables.

BI of $GF(q)$, $q = p^r$: $px, x^q - x$.

BI of a GR $R = GR(q^n, p^n)$ is the set of polynomials: $p^n x,$

$$p^j \Psi_0(x_1) \dots \Psi_0(x_u) \Psi_1(y_1) \dots \Psi_1(y_v) \dots \Psi_t(z_1) \dots \Psi_t(z_w)$$

over \mathbb{Z} , satisfying the conditions

$$j + \frac{1}{q-1}(u(q-1) + v(q^2-1) + \dots + w(q^t-1)) = n,$$

where $\Psi_j(x) \in \mathbb{Z}[x]$ — polynomials, defined recursively by

$$\Psi_0(x) = x^q - x, \quad \Psi_t(x) = \Psi_{t-1}(x)^q - p^{q^t-1} \Psi_{t-1}(x), \quad t \geq 1$$

(Nechaev, 1982, [9]).

2.2.2 STRUCTURE THEOREMS FOR CHAIN RINGS

As it was noted above, finite chain ring S is a local f.r. with $\mathfrak{N}(S) = S\pi$ for some $\pi \in \mathfrak{N}(S)$. The lattice of all left (right) ideals of S is a chain of two-sided ideals $\mathfrak{N}(S)^i = R\pi^i = \pi^i R$:

$$S \triangleright \mathfrak{N}(S) \triangleright \dots \triangleright \mathfrak{N}(S)^{n-1} \triangleright \mathfrak{N}(S)^n = 0, \quad n = \text{ind } \mathfrak{N}(S) \in \mathbb{N}$$

If $\bar{S} = S/\mathfrak{N}(S) = GF(q)$, $q = p^r$, then $|S| = q^n$, $\text{char } S = p^d$ for some $1 \leq d \leq n$; and the ring S contains a Galois subring $R = GR(q^d, p^d)$ with property $\bar{R} = \bar{S}$, moreover in this case $S = R[\pi]$. Parameter $\varepsilon \in \mathbb{N}$, such that $pS = \mathfrak{N}(S)^\varepsilon$, is called the **ramification index** of S .

COMMUTATIVE CHAIN RINGS.

Theorem 2.7. (*Snapper 1951*) *Let S be a commutative chain ring. Then π is a root of an **Eisenstein polynomial***

$$c(x) = x^\varepsilon - c_{\varepsilon-1}x^{\varepsilon-1} - \dots - c_0 \in R[x],$$

where $c_0, \dots, c_{\varepsilon-1} \in pR$, $c_0 \notin p^2R$, if $d > 1$, and

$$S \cong R[x]/(c(x), p^{d-1}x^\rho), \quad n = (d-1)\varepsilon + \rho, \quad 1 \leq \rho \leq \varepsilon. \quad (1)$$

In view of (1) we call commutative finite chain ring also **Galois-Eisenstein ring** or **GE-ring**.

Corollary 2.8. *Any GE-ring can be presented as a quotient ring of some commutative local principal ideal domain.*

A GE-ring S is called a **week ramification** if $(\varepsilon, p) = 1$. in this case there exists element $\pi \in \mathfrak{N} \setminus \mathfrak{N}^2$ such that polynomial (1) has a form $c(x) = x^\varepsilon - c_0$.

A GE-ring S is defined by parameters q, n, ε unique up to isomorphism exactly in the following cases [6]:

- (a) $n = \varepsilon$, i.e. $d = 1$, $S \cong GF(q)[x]/(x^n)$;
- (b) $n = \varepsilon + 1$, $(\varepsilon, q - 1) = 1$, $S \cong GR(q^2, p^2)[x]/(x^2 - pe, px)$;
- (c) $(\varepsilon, q - 1) = 1$, $(\varepsilon, p) = 1$, $S \cong GR(q^d, p^d)[x]/(x^\varepsilon - pe, p^{d-1}x^p)$.

Some estimations of a number of classes of isomorphic GE-rings for a fixed parameters q, n, ε was deduced by Clark, Drake (1976).

A pair of GE-rings $\mathbb{Z}_4[x]/(x^2 - 2)$ and $\mathbb{Z}_4[x]/(x^2 - 2x - 2)$ gives the simplest example of a pair of finite non-isomorphic rings with isomorphic additive and multiplicative groups.

A RING $\mathcal{P}(S)$ OF POLYNOMIAL FUNCTIONS $S \rightarrow S$
on GE-ring S has a form

$$\mathcal{P}(S) \cong S[x]/I,$$

where $I \triangleleft S[x]$ is ideal generated by the system of polynomials

$$F_m(x), \pi^{\varepsilon_{m-1}}F_{m-1}(x), \dots, \pi^{\varepsilon_1}F_1(x),$$

which is defined by the following way [5]: $\varepsilon_i = n - \alpha(qi)$, $i \in \overline{1, m-1}$;

$$\alpha(t) = \left[\frac{t}{q} \right] + \left[\frac{t}{q^2} \right] + \dots; \quad m = (1/q) \min\{t : \alpha(t) \geq n\}.$$

If $i = i_0 + qi_1 + \dots + q^h i_h$, $0 \leq i_t \leq q-1$, $t \in \overline{0, h}$, then

$$F_i(x) = \Phi_0(x)^{i_0} \Phi_1(x)^{i_1} \dots \Phi_h(x)^{i_h},$$

where

$$\Phi_0(x) = x^q - x, \quad \Phi_t(x) = \Phi_{t-1}(x)^q - \pi^{q^t-1} \Phi_{t-1}(x).$$

The number of different polynomial function on GE-ring S is

$$|\mathcal{P}(S)| = q^{q(nm - \sum_{i=1}^{m-1} \alpha(qi))}.$$

NONCOMMUTATIVE CHAIN RINGS (Nechaev [7]). Let now S be noncommutative finite chain ring with the pointed above parameters:

$$\mathfrak{N}(S) = S\pi \text{ for some } \pi \in \mathfrak{N}(S), \quad \mathfrak{N}(S)^t = S\pi^t = \pi^t S, t \in \mathbb{N};$$

The lattice of ideals of S :

$$S \triangleright \mathfrak{N}(S) \triangleright \dots \triangleright \mathfrak{N}(S)^{n-1} \triangleright \mathfrak{N}(S)^n = 0, \quad n = \text{ind } \mathfrak{N}(S) \in \mathbb{N};$$

$$\overline{S} = S/\mathfrak{N}(S) = GF(q), \quad q = p^r, \quad |S| = q^n, \quad \text{char } S = p^d, \quad 1 \leq d \leq n;$$

Let $R = GR(q^d, p^d)$ be a Galois subring of S with property $\overline{R} = \overline{S}$, and ε be the ramification index of S : $pS = \mathfrak{N}(S)^\varepsilon$. , By theorem about distinguishing basis of (R, R) -bimodule, there exists a **distinguishing generator** π of $\mathfrak{N}(S)$ such that for some automorphism $\tau \in \text{Aut}(R)$ we have:

$$\forall a \in R. \quad \pi a = \tau(a)\pi.$$

$$\overline{\tau(a)} = \overline{a}^{p^\lambda}, \quad \lambda \in \overline{1, r}, \quad \text{ord } \tau = r/(\lambda, r) = t, \quad t|\varepsilon.$$

If $t = 1$, in particular, if $(r, \varepsilon) = 1$, then S is a GE-ring.

If $t > 1$ the ring S is a quotient ring of the **Ore polynomial ring** $R[x, \tau]$ with $xa = \tau(a)x$, $a \in R$.

Theorem 2.9. (a) *distinguishing generator* π of $\mathfrak{N}(S)$ is a root of a **special Eisenstein polynomial**:

$$c(x) = x^{tm} - c_{m-1}x^{t(m-1)} - \dots - c_1x^t - c_0 \in R[x; \tau], \quad (2)$$

where $c_i \in pR, i \in \overline{0, m-1}; c_0 \notin p^2R$, if $d > 1$; and either

(a1) $c_i \in R_\tau = \{a \in R : \tau(a) = a\}, i \in \overline{0, m-1}$; or

(a2) $n - (d-1)\varepsilon = tk + 1, \tau(c_k) - c_k \in p^{d-1}R \setminus 0$, and $c_i \in R_\tau$,

for $i \in \overline{0, m-1}, i \neq k$.

(b) Let $\rho = n - (d-1)\varepsilon$. Then there is an isomorphism

$$S \cong R[x; \tau]/I, \text{ where } I = c(x)R[x; \tau] + p^{d-1}x^\rho R[x; \tau], \quad (3)$$

(c) For any special Eisenstein polynomial (2) the ideal I from (3) is a two-sided ideal and the ring (3) is a chain ring with described parameters. The center Z of the ring S is

$$Z = C = R_\tau + R_\tau\pi^t + \dots + R_\tau\pi^{tk} \text{ under the condition (a1),}$$

$$\text{and } Z = C + p^{d-1}R\pi^{tk} \text{ under the condition (b).}$$

In view of this theorem we call such a ring also **Galois-Eisenstein-Ore-** or **GEO-ring** In the case (a2) GEO-ring S cannot be represented as a factor of some prime principal ideals ring (Nechaev 1974).

REFERENCES.:

- [1] Matematicheskaya Enciklopediya (in Russian).
- [2] Herstein I. N. "Proc. Amer. Math. Soc., 1950,v.1, No 3, 370-371.
- [3] McDonald B. R. Finite rings with identity. N-Y, 1974;
- [4] Markov V. T., Nechaev A. A. "Fundamental'naya i Prikladnaya Matematika." (in Russian), CNIT of MSU, 2000.
- [5] Krull W. "Math. Ann.", 1922, B.88, 80-122;
- [6] Arkhipov L. M. "Mathematics Notes", 1976;
- [7] Nechaev A. A. "Math. Sb.", v.91, No 3, 1973, (350-366 Russ.);
- [8] Nechaev A. A. Proc. of All-Un. Alg. Symp., Gomel, 1975, (Russ.).
- [9] Nechaev A. A. "Alg. and Log.", v.18, No 2, 1979, (186-194 Russ.);
- [10] Nechaev A. A. "Uspekhi Mat. Nauk", v. 37, No 5, 1982, (193-194 in Russian);
- [11] Nechaev A. A. "Discrete Math. and Appl.", v.1, iss. 4, 1989, (123-139 in Russian);
- [12] Elizarov V. P. Dep. VINITI USSR, 1472-85, 1985, (in Russian).
- [13] Elizarov V. P. Finite Rings (foundations of the theory),

Moscow 1993 (in Russian);

[14] K r u s e R. L., P r i c e D. T. Nilpotent rings. Gordon and Breach, 1969.

[15] W i e s e n b a u e r J. Monatsh. Math., 78, 1974, No 2, 164-173.

[16] F l o r W., W i e s e n b a u e r J. Oesterr. Acad. Wiss. Sitzungsberichte der mathem. — Natur. Kl. Abt. II 1975, Bd. 183, Hft. 8 - 10, S. 289 — 320.

[17] A n t i p k i n V. G., E l i z a r o v V. P. Siberian Math. Journ., 23, 1982, No 4, (9 — 18 in Russian).

[18] L v o v I. V. "Alg. and Log.", v.12, No 3, 1973, (269-297 in Russian);

[19] L v o v I. V. "Alg. and Log.", v17, No 3, 1978, (282-286 in Russian);

[20] M a l ' c e v J. N. The structure of associative algebras...Barnaul, 1994;

[21] M a l ' c e v J. N. K u z m i n E. N. "Alg. and Log.", v.17, N1. 1978, (28-32 in Russian).

[22] G e n o v G. K. "Alg. and Log.", v. 20, No 4, 1981, (365-388 in Russian);

- [23] Genov G. K., Siderov P. N. "Serdika Bulgar. Mat. spisanie" No 8, 1982, 313-323, 351-366 in Bulgarian;
- [24] Oleksenko A. N. "Fundamental'naya i Prikladnaya Matematika", CNIT of MSU, 2000. in Russian;
- [25] Bakhturin Ju. A., Olshanskii' A. Ju. "Math. Sbornik.", v. 96, No 4, 1975, (543-559 in Russian).
- [26] Medvedev Ju. A. "Alg. and Log.", v. 18, No 6, 1979, (723-758 in Russian);
- [27] Polin S. V. "Siberian Math. Journ.", v. 17, No 6, (1356-1366 in Russian),
- [28] Bakhturin Ju. A, Identities in Algebras. ., "Nauka", 1985, in Russian.
- [29] Albert A. A. "Proc. Amer. Math. Soc.", 1959, v. 9, 928-932;
- [30] Dixon L. E. "Duke Math. J.", 1935, v. 1, 113 - 125;
- [31] Janush G. J. "Trans. Amer. Math. Soc.", 1966, v.122, 461-478;
- [32] Raghavendran R. "Compos. Math.", 1969, v.21, No 2, 195-219;
- [33] Kuzmin A. S., Nechaev . . "Alg. and Log.".34, No 2, 1995, 169-189;