Ladislav Skula

Special invariant subspaces of a vector space over $\mathbf{Z}/l\mathbf{Z}$

Archivum Mathematicum, Vol. 25 (1989), No. 1-2, 35--46

Persistent URL: http://dml.cz/dmlcz/107337

ARCHIVUM MATHEMATICUM (BRNO)
Vol. 25, No. 1–2 (1989), 35–46

SPECIAL INVARIANT SUBSPACES OF A VECTOR SPACE OVER $\mathbf{Z}/l\mathbf{Z}$

LADISLAV SKULA

(Received April 7, 1988)

Dedicated to the memory of Milan Sekanina

Abstract. This article deals with a special linear operator S on the vector space $\mathbf{V}$ over the Galois field $\mathbf{Z}/l\mathbf{Z}$ of dimension $\frac{l-1}{2}$ (l an odd prime). All invariant subspaces are described in three ways. The background of this theme is found in the area of the *Stickelberger ideal* mod l. It is shown that the matrices of the *Stickelberger ideals* have a very convenient form for $l < 1{,}000$.

Key words. Invariant subspaces, Stickelberger ideal, group ring of a cyclic group over the Galois field, Bernoulli numbers, index of irregularity of a prime.

MS Classification. 10 M 20, 12 A 80

In this paper the vector space $\mathbf{V}$ over the Galois field $\mathbf{Z}/l\mathbf{Z}$ is considered (l is an odd prime) with dimension $\frac{l-1}{2}$. For this vector space special linear operators S_z ($1 \leqq z \leqq l-1$) are defined. The main goal of this paper is to describe all invariant subspaces of $\mathbf{V}$ with respect to the operators S_z (Theorem 3.4).

There is defined a special isomorphism F from a group ring $\mathfrak{R}^-(l)$ (considered as a vector space) on $\mathbf{V}$ and the connection is shown between the ideals of $\mathfrak{R}^-(l)$ and invariant subspaces of $\mathbf{V}$ with respect to S_z (4.3.2).

The theme of this paper derives from the area of the *Bernoulli numbers, index of irregularity of the prime* l and the *Stickelberger ideal* mod l (4.3.3).

The final Section 5 deals with the normal matrix of a subspace of $\mathbf{V}$. Especially the normal matrix of an invariant subspace of $\mathbf{V}$ with respect to the operators S_z is investigated and it is mentioned that for each prime $l < 1{,}000$ the normal matrix of the subspace of $\mathbf{V}$ corresponding to the Stickelberger ideal has a very convenient form (5.9.1).

1. NOTATION

Throughout this paper it will be designated by
l an odd prime,

$$N = \frac{l-1}{2},$$

$\mathbf{V} = \{(a(1), a(2), \ldots, a(N)) : a(i) \in \mathbf{Z}/l\mathbf{Z}\} = (\mathbf{Z}/l\mathbf{Z})^{(N)}$ the vector space over the Galois field $\mathbf{Z}/l\mathbf{Z}$ (of residue classes mod l on the ring $\mathbf{Z}$ of integers) with dimension N and with componentwise operations,
$\mathbf{L} = \{1, 2, \ldots, N\}$.

For integers $1 \leqq x, z \leqq l - 1$ put

$$\varepsilon(x, z) = \begin{cases} 1 & \text{if} \quad xz \equiv y(\text{mod } l),\ 0 < y \leqq N, \\ -1 & \text{if} \quad xz \equiv y(\text{mod } l),\ N + 1 \leqq y < l, \end{cases}$$

$$f(x, z) \equiv \varepsilon(x, z)\, xz(\text{mod } l), \qquad f(x, z) \in \mathbf{L},$$

so $f(x, z) \equiv \pm xz(\text{mod } l)$.

For the vector $\mathbf{u} = (u(1), \ldots, u(N)) \in \mathbf{V}$ put

$$S_z(\mathbf{u}) = \mathbf{v} = (v(1), \ldots, v(N)) \in \mathbf{V},$$

where $v(x) = \varepsilon(x, z)\, u(f(x, z))$ $(x \in \mathbf{L})$. Sometimes an integer $x \in \mathbf{Z}$ will be considered as the residue class mod l containing x.

According to ([6], 3.4 and 3.5) it holds

1.1. Proposition. (*a*) *For each* $1 \leqq z \leqq l - 1$ $(z \in \mathbf{Z})$ *the mapping* S_z: $\mathbf{V} \to \mathbf{V}$ *is an automorphism of the vector space* $\mathbf{V}$.

(b) *For* $1 \leqq z, z' \leqq l - 1$ $(z, z. \in \mathbf{Z})$ *we have*

$$S_{z'} = S_z \quad \textit{if and only if } z = z'.$$

(c) *If* $1 \leqq z, z', w \leqq l - 1$ $(z, z', w \in \mathbf{Z})$, $w \equiv z \,.\, z'(\text{mod } l)$, *then* $S_w = S_{z'} \circ S_z$.

(d) *The set* $\{S_z\colon 1 \leqq z \leqq l - 1,\ z \in \mathbf{Z}\}$ *with operation* e *forms a cyclic group of order* $l - 1$. *Generators of this group are the automorphisms* S_R, *where* $1 \leqq R \leqq$ $\leqq l - 1$ *are primitive roots* mod l.

(The operations $\circ$ means composition of mappings.)

The aim of this paper is to describe all invariant subspaces of the vector space $\mathbf{V}$ with respect to the group $(\{S_z : 1 \leqq z \leqq l - 1\}, \circ)$.

Choose a primitive root r mod l $(1 < r < l)$ and denote by S the mapping S_r. Then

$$\{S_z : 1 \leqq z \leqq l - 1, z \in \mathbf{Z}\} = \{S^n : 0 \leqq n \leqq l - 2, n \in \mathbf{Z}\}$$

and the S_z-invariant subspaces of $\mathbf{V}$ for each $1 \leqq z \leqq l - 1$, $z \in \mathbf{Z}$ are just the S-invariant subspaces of $\mathbf{V}$.

2. SOME S-INVARIANT SUBSPACES OF $\mathbf{V}$

2.1. Definition. For a subset $A \subseteq \mathbf{L}$ put

$$\mathscr{S}(A) = \{\alpha = (a(1), a(2), \ldots, a(N)) \in \mathbf{V} : \sum_{x=1}^{N} a(x)^{2a-1} = 0 \text{ for each } a \in A\}.$$

2.2. Proposition. (a) *For each subset $A \subseteq \mathbf{L}$ the set $\mathscr{S}(A)$ forms an S-invariant subspace of the vector space $\mathbf{V}$ and* $\dim \mathscr{S}(A) = N - |A|$. ($|A|$ means cardinal of A).

(b) *For $A \subseteq B \subseteq \mathbf{L}$ the relation $\mathscr{S}(A) \supseteq \mathscr{S}(B)$ holds.*

(c) $\mathscr{S}(\emptyset) = \mathbf{V}$, $\mathscr{S}(\mathbf{L}) = 0$. (0 means zero subspace.)

Proof. a) Clearly, $\mathscr{S}(A)$ is a subspace of the vector space $\mathbf{V}$. Let $\mathbf{u} = (u(1), \ldots, \ldots, u(N)) \in \mathscr{S}(A)$, $S(\mathbf{u}) = \mathbf{v} = (v(1), \ldots, v(N)) \in \mathbf{V}$. Then for $a \in A$ we have

$$\sum_{x=1}^{N} v(x)\, x^{2a-1} = \sum_{x=1}^{N} \varepsilon(x, r)\, u(f(x, r))\, x^{2a-1},$$

hence

$$r^{2a-1} \sum_{x=1}^{N} v(x)\, x^{2a-1} = \sum_{x=1}^{N} u(f(x, r)\,(rx)^{2a-1}\, (\varepsilon(x, r) = 1) +$$
$$+ \sum_{x=1}^{N} u(f(x, r))\,(-rx)^{2a-1}\, (\varepsilon(x, r) = -1) =$$
$$= \sum_{y=1}^{N} u(y)\, y^{2a-1}(\varepsilon(y, r_{-1}) = 1) + \sum_{y=1}^{N} u(y)\, y^{2a-1}(\varepsilon(y, r_{-1}) =$$
$$= -1) = \sum_{y=1}^{N} u(y)\, y^{2a-1} = 0,$$

where $r_{-1} \in \mathbf{Z}$, $0 < r_{-1} < l$, $r \,.\, r_{-1} \equiv 1 (\mathrm{mod}\, l)$. Therefore the subspace $\mathscr{S}(A)$ is S-invariant.

(b) The subspace $\mathscr{S}(A)$ is the space of solutions of the system of linear equations

$$\sum_{x=1}^{N} a(x)\, x^{2a-1} = 0 \qquad (a \in A),$$

over the field $\mathbf{Z}/l\mathbf{Z}$ with unknowns $a(1), \ldots, a(N)$. The matrix of this system equals the matrix

$$(x^{2a-1})\ (x \in \mathbf{L},\ a \in A),$$

which is of Vandermond's type, hence its rank is equal to $|A|$. It follows that $\dim \mathscr{S}(A) = N - |A|$.

(c) The assertions (b) and (c) are evident.

2.3. Definition. We denote by $\mathscr{N}$ the set of all non-quadratic residues x mod l $(1 < x < l)$. For $x \in \mathscr{N}$ put

$$\mathbf{u}(x) = (u(1), \ldots, u(N)) \in \mathbf{V},$$

where for $1 \leqq t \leqq N$ we have

$$u(t) = x^{\operatorname{ind} t},$$

(ind t denotes index of t relative to the primitive root r of l.)

The subspace of the space $\mathbf{V}$ generated by the vector $\mathbf{u}(x)$ will be denoted by $\mathbf{U}(x)$. Hence,

$$\mathbf{U}(x) = \{k \,.\, \mathbf{u}(x) : k \in \mathbf{Z}/l\mathbf{Z}\} \qquad \text{and} \qquad \dim \mathbf{U}(x) = 1.$$

Since $S(\mathbf{u}(x)) = x \,.\, \mathbf{u}(x)$, $\mathbf{U}(x)$ is an S-invariant subspace of the space $\mathbf{V}$ and $S(\mathbf{u}) = x \,.\, \mathbf{u}$ for each $\mathbf{u} \in \mathbf{U}(x)$.

2.4. Proposition. *The vectors* $\mathbf{u}(x)$ $(x \in N)$ *form a basis of the space* $\mathbf{V}$.

Proof. As $\dim \mathbf{V} = N$, it is enough to prove that the vectors $\mathbf{u}(x)$ $(x \in \mathcal{N})$ are linearly independent.

Let $c(x) \in \mathbf{Z}/l\mathbf{Z}$ for $x \in \mathcal{N}$ such that

$$\sum c(x)\, \mathbf{u}(x)\, (x \in \mathcal{N}) = \mathbf{o}.$$

($\mathbf{o}$ means zero vector.)
Then

$$\sum c(x)\, x^{\operatorname{ind} v} (x \in \mathcal{N}) = 0 \qquad \text{for each} \qquad 1 \leqq v \leqq N.$$

It follows

$$\sum c(x)\, x^{i} (x \in \mathcal{N}) = 0 \qquad \text{for each} \qquad 0 \leqq i \leqq N - 1.$$

The matrix (x^i) $(x \in \mathcal{N},\ 0 \leqq i \leqq N - 1)$ is of Vandermond's type, hence $c(x) = 0$ for each $x \in \mathcal{N}$. The proposition is proved.

2.5. Definition. For $X \subseteq \mathcal{N}$ let $\mathbf{U}(X)$ mean the subspace of the vector space $\mathbf{V}$ generated by the vectors $\mathbf{u}(x)$ $(x \in X)$, $\mathbf{U}(\emptyset)$ is defined as zero space. Hence $\mathbf{U}(X)$ is the direct sum of the subspaces $\mathbf{U}(x)$ $(x \in X)$:

$$\mathbf{U}(X) = \sum_{\oplus} \mathbf{U}(x)\, (x \in X)$$

and $\dim \mathbf{U}(X) = |X|$.

Since the subspace $\mathbf{U}(x)$ is S-invariant, the subspace $\mathbf{U}(X)$ is also S-invariant.

2.6. Proposition. *Let* $X, Y \subseteq \mathcal{N}$. *Then we have*

(*a*) $\mathbf{U}(X) \subseteq \mathbf{U}(Y)$ *if and only if* $X \subseteq Y$,
(*b*) $\mathbf{U}(X) = \mathbf{U}(Y)$ *if and only if* $X = Y$.

Proof. Clearly, (a) implies (b). Suppose $\mathbf{U}(X) \subseteq \mathbf{U}(Y)$ and $x \in X$. Then $\mathbf{u}(x) \in \mathbf{U}(Y)$ and hence $x \in Y$. Therefore (a) holds and hence (b) as well.

Between the subspaces $\mathbf{U}(X)$ $(X \subseteq \mathcal{N})$ and the subspaces $\mathcal{S}(A)$ $(A \subseteq \mathbf{L})$ the following relation holds.

2.7. Theorem. *Let* $X \subseteq \mathcal{N}$ *and* $A = \mathbf{L} - \left\{N - \frac{1}{2}(\operatorname{ind} x - 1) : x \in X\right\}$. *Then*

$$\mathbf{U}(X) = \mathcal{S}(A).$$

Proof. I. We show that $\mathbf{U}(X) \subseteq \mathcal{S}(A)$. Let $x \in X$ and $\mathbf{u}(x) = (u(1), \dots, u(N))$. Then $x^{\operatorname{ind} v} = u(v)$ for each $1 \leqq v \leqq N$. For $a \in A$ the integer $\operatorname{ind} x + 2a - 1$ is even and $\operatorname{ind} x + 2a - 1 \not\equiv 0(\operatorname{mod} l - 1)$. Therefore we have

$$\sum_{v=1}^{N} x^{\operatorname{ind} v} v^{2a-1} \equiv \sum_{v=1}^{N} (r^{\operatorname{ind} x + 2a - 1})^{\operatorname{ind} v} (\operatorname{mod} l) \equiv$$

$$\equiv \sum_{u=0}^{\frac{l-3}{2}} (r^{\operatorname{ind} x + 2a - 1})^{u} (\operatorname{mod} l) \equiv 0(\operatorname{mod} l).$$

It follows that $\sum_{v=1}^{N} u(v)\, v^{2a-1} = 0$, hence $\mathbf{u}(x) \in \mathcal{S}(A)$.

II. Since $\dim \mathbf{U}(X) = |X| = N - |A| = \dim \mathcal{S}(A)$, we get $\mathbf{U}(X) = \mathcal{S}(A)$.

3. ALL S-INVARIANT SUBSPACES OF $\mathbf{V}$

In this Section we give description of all S-invariant subspaces of the vector space $\mathbf{V}$. The proofs use the known results concerning the structure of a linear operator in an n-dimensional vector spave over a number field that hold also for the field $\mathbf{Z}/l\mathbf{Z}$ as it is possibly easily to see. The notions and these results from this branch are taken from book [2] by *F. R. Gantmacher*, Chapter VII. Especially we use the notion of *minimal polynomial of a vector space* (with respect to a given linear operator) and „*The First Theorem on the Decomposition of a Space into Invariant Subspaces*" ([2], Chapter VII, Theorem 1).

3.1. Proposition. *The polynomial* $\Psi(\lambda) = \lambda^N + 1$ (considered over the field $\mathbf{Z}/l\mathbf{Z}$) *is the minimal polynomial of the space* $\mathbf{V}$ *with respect to the linear operator* S.

Proof. Recall that the minimal polynomial $\Psi(\lambda)$ is the non-zero monic polynomial over $\mathbf{Z}/l\mathbf{Z}$ of the least degree such that for each $\mathbf{u} \in \mathbf{V}$ we have $\Psi(S)(\mathbf{u}) = \mathbf{o}$.

If $\mathbf{u} \in \mathbf{V}$, then $S^N(\mathbf{u}) = S_r^N(\mathbf{u}) = S_{l-1}(\mathbf{u}) = -\mathbf{u}$, so $\Psi(S)(\mathbf{u}) = \mathbf{o}$.

Let $\mathbf{u}_i = (0, 0, \dots, 0, 1, 0, \dots, 0) \in \mathbf{V}$, where 1 is situated on the ith position. The vectors $\mathbf{u}_i$ $(1 \leqq i \leqq N)$ form a basis of $\mathbf{V}$.

For $0 \leqq n \leqq \frac{l-3}{2}$ let $x(n)$ be the integer, $1 \leqq x(n) \leqq N$, $e_n = \pm 1$ such that $e_n r^n x(n) \equiv 1(\operatorname{mod} l)$. Then $S^n = S_r^n = S_w$ according to 1.1 (c), where w is the integer, $1 \leqq w \leqq l - 1$, $w \equiv r^n(\operatorname{mod} l)$. Hence $S^n(\mathbf{u}_1) = e_n \mathbf{u}_{x(n)}$. Since for $0 \leqq n$, $m \leqq \frac{l-3}{2}$ the equality $x(n) = x(m)$ follows $n = m$, the vectors $S^0(\mathbf{u}_1), S^1(\mathbf{u}_1), \dots,$

$\ldots, S^{\frac{l-3}{2}}(\mathbf{u}_1)$ are linearly independent hence $x(S)(\mathbf{u}_1) \neq \mathbf{o}$ for each non-zero polynomial $x(\lambda)$ over the field $\mathbf{Z}/l\mathbf{Z}$ of degree $< N$. The proposition follows.

3.2. Remark. Clearly

$$\Psi(\lambda) = \lambda^N + 1 = \Pi(\lambda - x) \qquad (x \in \mathcal{N})$$

over the field $\mathbf{Z}/l\mathbf{Z}$. The polynomial $\lambda - x$ is the minimal polynomial of the subspace $\mathbf{U}(x)$ with respect to the operator S for each $x \in \mathcal{N}$. The conversion of this assertion holds as well:

3.3. Proposition. *Let* $\mathbf{U}$ *be an invariant subspace of* $\mathbf{V}$ *with respect to the operator* S *with minimal polynomial* $\lambda - x$ $(x \in \mathcal{N})$ (over $\mathbf{Z}/l\mathbf{Z}$). *Then* $\mathbf{U} = \mathbf{U}(x)$.

Proof. Clearly, $\mathbf{U}$ is a non-zero space. Let $\mathbf{u} = (u(1), \ldots, u(N)) \in \mathbf{U}$, $\mathbf{u} \neq \mathbf{o}$. There exists $1 \leqq i \leqq N$ such that $u(i) \neq 0$. For $1 \leqq j \leqq N$ let $1 \leqq z \leqq l - 1$ with the property $zi \equiv j (\text{mod } l)$. There exists $k \in \mathbf{Z}/l\mathbf{Z}$, $0 \neq k$ such that $k \,.\, \mathbf{u} = S_z(\mathbf{u})$, hence $0 \neq k \,.\, u(i) = \varepsilon(i, z)\, u(f(i, z)) = \pm u(j)$. Thus $u(j) \neq 0$ for each $1 \leqq j \leqq N$.

Put $\mathbf{v} = u(1)^{-1}\mathbf{u} = (v(1), \ldots, v(N)) \in \mathbf{U}$. Then $v(j) \neq 0$ for each $1 \leqq j \leqq N$ and $v(1) = 1$.

a) For $1 \leqq a, b \leqq N$ we have $v(a) \,.\, v(b) = \varepsilon(a, b) \,.\, v(f(a, b))$. Namely, there exists $k \in \mathbf{Z}/l\mathbf{Z}$, $k \neq 0$ such that $k \,.\, \mathbf{v} = S_a(\mathbf{v}) = (w(1), \ldots, w(N))$. Since $1 = v(1)$, we get $k = w(1) = \varepsilon(1, a)\, v(f(1, a)) = v(a)$, thus $v(a) \,.\, v(b) = k \,.\, v(b) = w(b) = \varepsilon(b, a) \,.\, v(f(b, a))$.

b) Let $1 \leqq c, d \leqq N$, $e = \pm 1$, n a positive integer and $c^n \equiv ed (\text{mod } l)$. Then $v(c)^n = ev(d)$.

We prove this assertion by mathematical induction with regard to n. The case $n = 1$ is clear. Let this assertion hold for $n \geqq 1$ and let $1 \leqq C, D \leqq N$, $E = \pm 1$ and let $C^{n+1} \equiv E \,.\, D (\text{mod } l)$.

There exist integers ε, δ, $\varepsilon = \pm 1$, $1 \leqq \delta \leqq N$ such that $C^n \equiv \varepsilon\delta (\text{mod } l)$. We have $v(C)^n = \varepsilon v(\delta)$ and according to a) $v(\delta) \,.\, v(c) = \varepsilon(\delta, c) \,.\, v(f(\delta, c))$. Further $\varepsilon(\delta, c)\, f(\delta, c) \equiv C\delta \equiv \varepsilon C^{n+1} \equiv \varepsilon E \,.\, D (\text{mod } l)$, hence $f(\delta, c) = D$ and $\varepsilon E = \varepsilon(\delta, c)$, thus $v(C)^{n+1} = \varepsilon v(\delta) \,.\, v(C) = Ev(D)$.

c) It holds $v(t) = x^{\text{ind}\, t}$ for each $1 \leqq t \leqq N$. Put $R = r$, $\varepsilon = 1$ in case $r < l/2$ and $R = l - r$, $\varepsilon = -1$ in case $r > l/2$. There holds $xv(j) = \varepsilon(j, r)\, v(f(j, r))$ $(1 \leqq j \leqq N)$, hence $x = xv(1) = \varepsilon(1, r)\, v(f(1, r)) = \varepsilon v(R)$, which follows $\varepsilon x = v(R)$. Let $1 \leqq t \leqq N$, $n = \text{ind}\, t$. According to b) ($c = R$, $d = t$, $e = \varepsilon^n$) we get $v(t) = \varepsilon^n v(R)^n = x^n$, thus $x^{\text{ind}\, t} = v(t)$.

Assertion c) yields $\mathbf{v} = \mathbf{v}(x)$ and since each vector from $\mathbf{U}$ is a multiple of $\mathbf{v}$, we have $\mathbf{U} = \mathbf{U}(x)$.

3.4. Theorem. *Let* $\mathbf{U}$ *be a non-zero S-invariant subspace of the space* $\mathbf{V}$, $\dim \mathbf{U} = m$ $(1 \leqq m \leqq N)$. *Then there exists* $X \subseteq \mathcal{N}$, $|X| = m$ *such that* $\mathbf{U}(X) = \mathbf{U}$.

Proof. Let $G(\lambda)$ be the minimal polynomial of the space $\mathbf{U}$ with respect to S. Then $G(\lambda)$ divides the polynomial $\Psi(\lambda) = \lambda^N + 1$, hence there exists $X \subseteq \mathcal{N}$ with the property

$$G(\lambda) = \prod (\lambda - x) \qquad (x \in X),$$

(considered as a polynomial over the field $\mathbf{Z}/l\mathbf{Z}$). The First Theorem on the Decomposition *of a Space into Invariant Subspaces* then yields

$$\mathbf{U} = \sum_{\oplus} \mathbf{U}_x \qquad (x \in X),$$

where $\mathbf{U}_x$ is an S-invariant subspace of $\mathbf{V}$ with the minimal polynomial $\lambda - x$. Proposition 3.3 then implies Theorem.

4. CONNECTION WITH THE GROUP RING $(\mathbf{Z}/l\mathbf{Z})[G]$

4.1. Notation. Throughout this Section we shall use the following notation:

G a multiplicative cyclic group of order $l - 1$,

s a generator of G; thus $G = \{1 = s^0, s, \dots, s^{l-2}\}$,

$\mathfrak{R}(l)$ $= (\mathbf{Z}/l\mathbf{Z})[G]$ the group ring of G over the field $\mathbf{Z}/l\mathbf{Z}$; thus $\mathfrak{R}(l) = \{\sum_{i=0}^{l-2} a_i s^i : a_i \in \mathbf{Z}/l\mathbf{Z}\}$,

$\mathfrak{R}^-(l)$ $= \{\alpha = \sum_{i=0}^{l-2} a_i s^i \in \mathfrak{R}(l) : 0 = a_i + a_{i+N}$ for each $0 \leqq i \leqq N - 1\}$,

F the mapping of $\mathfrak{R}^-(l)$ onto $\mathbf{V}$ defined as follows: $F(\alpha) = \mathbf{u} = (u(1), \dots, u(N)) \in \mathbf{V}$, $\alpha = \sum_{i=0}^{l-2} a_i s^i \in \mathfrak{R}^-(l)$ and for $1 \leqq x \leqq N$, $u(x) = a_{l-1-\operatorname{ind} x}$ $(a_{l-1} = a_0)$,

F_n the mapping of $\mathfrak{R}^-(l)$ onto $\mathfrak{R}^-(l)$ for an integer n defined by the formula $F_n(\alpha) = s^n . \alpha (\alpha \in \mathfrak{R}^-(l))$.

We consider the subring $\mathfrak{R}^-(l)$ of the ring $\mathfrak{R}(l)$ as the vector space over the field $\mathbf{Z}/l\mathbf{Z}$. Then F is an isomorphism of the vector space $\mathfrak{R}^-(l)$ onto the vector space $\mathbf{V}$ and the mappings F_n are automorphisms of the vector space $\mathfrak{R}^-(l)$.

4.2. Proposition. *Let* z *be an integer,* $1 \leqq z \leqq l - 1$, $n = \operatorname{ind} z$. *Then*

$$F \circ F_n \circ F^{-1} = S_z .$$

Thus *the following diagram is commutative*:

$$\begin{tikzcd}
\mathfrak{R}^{-}(l) \arrow[d, "F_n"'] & \mathbf{V} \arrow[l, "F^{-1}"'] \arrow[d, "S_z"] \\
\mathfrak{R}^{-}(l) \arrow[r, "F"] & \mathbf{V}
\end{tikzcd}$$

Proof. Let $\mathbf{u} = (u(1), \ldots, u(N)) \in \mathbf{V}$, $F^{-1}(\mathbf{u}) = \alpha = \sum_{i=0}^{l-2} a_i s^i \in \mathfrak{R}(l)$, $F_n(\alpha) = \beta = \sum_{i=0}^{l-2} b_i s^i \in \mathfrak{R}^{-}(l)$ and $F(\beta) = \mathbf{v} = (v(1), \ldots, v(N)) \in \mathbf{V}$. For each integer j let $a_j = a_i$, where $0 \leqq i \leqq l - 2$, $i \equiv j (\mathrm{mod}\ l - 1)$.

Then for $1 \leqq x \leqq N$ and $0 \leqq i \leqq l - 2$ we have $u(x) = a_{-\mathrm{ind}\, x}$, $b_i = a_{i-n}$ and $v(x) = b_{l-1-\mathrm{ind}\, x} = a_{-\mathrm{ind}\, x - n} = a_{-\mathrm{ind}\, xz} = a_{-\mathrm{ind}\, \varepsilon(x,z) f(x,z)} = a_{-\mathrm{ind}\, \varepsilon(x,z) - \mathrm{ind}\, f(x,z)} = \varepsilon(x, z)\, u(f(x, z)) = u(x)$. It follows $S_z(\mathbf{u}) = \mathbf{v}$ and the proposition is proved.

4.3. Remark. The ideals of the ring $\mathfrak{R}^{-}(l)$ can also be characterized as follows:

4.3.1. *An additive subgroup I of the ring $\mathfrak{R}^{-}(l)$ is an ideal of the ring $\mathfrak{R}^{-}(l)$ if and only if $s \,.\, I \subseteq I$.*

Proof. Clearly, if I has the given property, then it is an ideal of $\mathfrak{R}^{-}(l)$. Let I be an ideal of $\mathfrak{R}^{-}(l)$ and let $\alpha \in I$. Denote by β the element $\frac{l+1}{2} s\,(1 - s^{\frac{l-1}{2}}) \in \mathfrak{R}^{-}(l)$, where 1 is considered as an element of $\mathbf{Z}/l\mathbf{Z}$. Since $\mathfrak{R}^{-}(l) = (1 - s^{\frac{l-1}{2}})\mathfrak{R}(l)$, there exists $\gamma \in \mathfrak{R}(l)$ such that $\alpha = (1 - s^{\frac{l+1}{2}})\,\gamma$. Then $\beta \,.\, \alpha = \frac{l+1}{2} s(1 - s^{\frac{l-1}{2}})^2\, \gamma = s \,.\, (1 - s^{\frac{l-1}{2}})\,\gamma = s \,.\, \alpha$, which implies $s \,.\, \alpha \in I$.

According to 4.3.1 there holds

4.3.2. *A subset I of $\mathfrak{R}^{-}(l)$ is an ideal of the ring $\mathfrak{R}^{-}(l)$ if and only if it forms an F_n-invariant subspace of the vector space $\mathfrak{R}^{-}(l)$ for each integer n.*

According to [5], Proposition 3.9 the ideals of the ring $\mathfrak{R}^{-}(l$ are in the one-to-one correspondence with the subsets X of $\mathcal{N}$ by the formula

$$X \subseteq \mathcal{N} \to \mathcal{J}(X) = \mathfrak{R}^{-}(l) \prod (s - x) \qquad (x \in X),$$

($s - x$ is considered as an element of $\mathfrak{R}(l)$). $\mathcal{J}(X)$ is a subspace of the vector space $\mathfrak{R}^{-}(l)$ and according to [5], Proposition 3.3 the system of elements α_L ($1 \leqq L \leqq$

$\leqq l-2$, L odd, $r_L \notin X$) ($1 \leqq r_n \leqq l-1$, $r_n \equiv r^n (\text{mod } l)$ for an integer n) forms a basis of the subspace $\mathscr{J}(X)$, where $\alpha_L = \sum_{i=0}^{l-2} r_{-iL} s^i$. The image $F(\mathscr{J}(X)$ is then an S-invariant subspace of $\mathbf{V}$, whose basis is formed by the elements $F(\alpha_L) = \mathbf{u}(r_L)$, and then $F(\mathscr{J}(X)) = \mathbf{U}(\mathscr{N} - X)$.

We have got in this way another proof of Theorem 3.4.

The general situation looks like the following:

$$
\begin{array}{ccc}
S\text{-invariant subspaces of } \mathbf{V} \leftrightarrow & \text{subsets of } \mathscr{N} & \leftrightarrow \text{ ideals of } \mathfrak{R}^-(l) \\
\mathbf{U} = \mathbf{U}(X) = \mathscr{S}(A) = & & \\
= F(\mathscr{J}(\mathscr{N} - X)) \leftrightarrow & X = \{r_{-2b+1} : b \in \mathbf{L} - A\} & \leftrightarrow \mathscr{J}(\mathscr{N} - X) = \\
& \updownarrow & = \mathfrak{R}^-(l) \,.\, \prod (s - x)\, (x \in \mathscr{N} - X) \\
& A = \mathbf{L} - \left\{ N - \dfrac{1}{2}(\operatorname{ind} x - 1) : x \in X \right\}, & \\
& \text{subsets of } \mathbf{L} &
\end{array}
$$

4.3.3. *Special case.* If we put $A = \{1 \leqq a \leqq \frac{l-3}{2}\,;\ l/B_{2a}\}$ (B_n means the *Bernoulli number*), then $|A| = \mathrm{i}(l)$ the *index of irregularity of l* and according to [6], Theorem 2.4 (c) $\mathscr{J}(\mathscr{N} - X) = \mathfrak{J}(l)$ is the *Stickelberger ideal* mod l. The set X is then equal to the set $\{r_{-2b+1} : 1 \leqq b \leqq \frac{l-3}{2},\ l \dagger B_{2b}\} \cup \{r\}$.

The images of some concrete elements from the *Stickelberger ideal* $\mathfrak{J}^-(l)$ in the isomorphism F are described in Section 4 and 5 of [6].

5. THE NORMAL MATRIX OF A SUBSPACE OF V

All matrices are considered over the field $\mathbf{Z}/l\mathbf{Z}$.

5.1. Definition. A matrix $M = (m_{ij})$ of size $m \times n$ ($m \leqq n$) is said *to be in normal form* if there exist integers $1 \leqq j_1 < j_2 < \ldots < j_m \leqq n$ with the following property:

$$
m_{ij} = \begin{cases} 1 & \text{for } j = j_i, \\ 0 & \text{for } j < j_i, \\ 0 & \text{for } j = j_k,\ 1 \leqq k \leqq m,\ k \neq i, \end{cases}
$$

$1 \leqq i \leqq m$. Thus the columns with subscriptions $j_1, \ldots, j_m$ form the unit matrix of order m and the elements of M standing in the left of ones of this unit matrix are zeros. The number m is rank of M.

It is clear that any nonzero matrix C can be transformed in a matrix M in normal form by a sequence of elementary row operations (i.e. multiplication of a row by a nonzero element from $\mathbf{Z}/l\mathbf{Z}$ and addition to a row another one) and omitting rows containing only zeros.

This matrix M ir defined uniquely by this property and we will call it *the normal form of the matrix C.*

5.2. Definition. Let $0 \neq \mathbf{U}$ be a subspace of the vector space $\mathbf{V}$. The coordinates of vectors of a basis $\mathscr{B}$ of $\mathbf{U}$ form a nonzero matrix

$$U = (u(1), \dots, u(N))\ (\mathbf{u} = (u(1), \dots, u(N)) \in \mathscr{B})$$

of size $\dim \mathbf{U} \times N$. We call the normal form M of the matrix U *the normal matrix of the subspace* $\mathbf{U}$.

Clearly, M doesn't depend on the basis $\mathscr{B}$, size of M equals $\dim \mathbf{U} \times N$ and the row vectors of M form a basis of $\mathbf{U}$. The normal matrix of the whole space $\mathbf{V}$ is the unit matrix of order N.

5.3. Let $\emptyset \neq \mathbf{U} \neq \mathbf{V}$ be an S-invariant subspace of $\mathbf{V}$, let $A \subseteq \mathbf{L}(\emptyset \neq A \neq \mathbf{L})$ and $\mathbf{U} = \mathscr{S}(A)$, and let $r = |A|$ $(0 < r < N)$.

There exist uniquely determined integers

$$0 = \xi_0 < 2 \leqq \xi_1 < \xi_2 < \dots < \xi_{r-1} < \xi_r = N,$$

such that for $x \in \mathbf{L}$, $\xi_k < x \leqq \xi_{k+1} (0 \leqq k < r - 1)$ rank of the matrix

$$(x^{2a-1}, \xi_{k+1}^{2a-1}, \xi_{k+2}^{2a-1}, \dots, \xi_r^{2a-1}) \qquad (a \in A)$$

of size $r \times (r - k + 1)$ equals $r - k$. (Since rank of the matrix (t^{2a-1}) $(a \in A, t \in \mathbf{L})$ of size r/N equals r (Vandermond's type)).

Let $1 \leqq i \leqq N$, $i \notin \{\xi_1, \xi_2, \dots, \xi_r\}$. Then there exists $0 \leqq k \leqq r - 1$ such that $\xi_k < i < \xi_{k+1}$. Since ranks of matrices

$$(i^{2a-1}, \xi_{k+1}^{2a-1}, \dots, \xi_r^{2a-1}) \qquad (a \in A),$$
$$(\xi_{k+1}^{2a-1}, \dots, \xi_r^{2a-1}) \qquad (a \in A)$$

equal one another and equal $r - k$, there exist uniquely determined integers $0 \leqq x_{i\gamma} < l (1 \leqq \gamma \leqq r - k)$ such that

$$(*) \qquad i^{2a-1} + \sum_{\gamma=1}^{r-k} \xi_{k+\gamma}^{2a-1} x_{i\gamma} \equiv 0 (\mathrm{mod}\ l).$$

Put for $1 \leqq j \leqq N (i \notin \{\xi_1, \dots, \xi_r\})$:

$$m_{ij} = \begin{cases} 1 & \text{for } j = i, \\ x_{i\gamma} & \text{for } j = \xi_{k+\gamma} (1 \leqq \gamma \leqq r - k), \\ 0 & \text{otherwise.} \end{cases}$$

5.3.1. Theorem. *The matrix* $M = (m_{ij})$ $(1 \leqq i \leqq N, i \in \{\xi_1, \xi_2, \dots, \xi_r\}, 1 \leqq j \leqq \leqq N)$ *is the normal matrix of the subspace* $\mathbf{U}$.

Proof. According to definition the matrix M is in normal form and has size $\dim \mathbf{U} \times N$ since $\dim \mathbf{U} = N - r$. It remains to prove that every row vector of M belongs to $\mathbf{U}$. Using (*) and the fact $\mathbf{U} = \mathscr{S}(A)$ we obtain the Theorem.

5.4. Definition. We call a subset $A \subseteq \mathbf{L}$ *normal (for the prime l)* if $A = \varnothing$ or $A = \mathbf{L}$ or $\varnothing \neq A \neq \mathbf{L}$ and the normal matrix M of the subspace $\mathscr{S}(A)$ of $\mathbf{V}$ has the form

$$M = (E, X),$$

where E is the unit matrix of order $N - |A|$ and X is a matrix of size $N - |A| \times \times |A|$.

The following two Propositions are immediate consequences of Theorem 5.3.1.

5.5. Proposition. *Each one-element subset of* $\mathbf{L}$ *is normal for the prime l.*

5.6. Proposition. *Let* $A \subseteq \mathbf{L}, \varnothing \neq A \neq \mathbf{L}, r = |A|$ *and* $B = \{a - a^* : a \in A\}$, *where* a^* *is the least integer in A. Then the following assertions are equivalent:*

(a) *A is normal for the prime l,*

(b) $\det (x^{2b})\ (b \in B,\ N - r + 1 \leqq x \leqq N) \not\equiv 0 (\mathrm{mod}\ l)$,

(c) $\det ((2x - 1)^{2b})\ (b \in B,\ 1 \leqq x \leqq r) \not\equiv 0 (\mathrm{mod}\ l)$.

We can see easily

5.7. Proposition. *Let* $3 \leqq l \leqq 11$. *Then each subset* $A \subseteq \mathbf{L}$ *is normal for the prime l.*

We also obtain by easy computation:

5.8. Proposition. *Let* $l = 13$. *Then each subset* $A \subseteq \{1, 2, \ldots, 6\}$ *is normal for* 13 *except*

(a) $A = \{1, 3, 5\}$ *or* $A = \{2, 4, 6\}$,

(b) $A = \{1, 4\}$ *or* $A = \{2, 5\}$ *or* $A = \{3, 6\}$.

In case (a) the normal matrix M of $\mathscr{S}(A)$ *has the form*

$$M = \begin{bmatrix} 1 & 0 & x_1 & 0 & y_1 & z_1 \\ 0 & 1 & x_2 & 0 & y_2 & z_2 \\ 0 & 0 & 0 & 1 & y_3 & z_3 \end{bmatrix}$$

and in case (b)

$$M = \begin{bmatrix} 1 & 0 & 0 & x_1 & 0 & y_1 \\ 0 & 1 & 0 & x_2 & 0 & y_2 \\ 0 & 0 & 1 & x_3 & 0 & y_3 \\ 0 & 0 & 0 & 0 & 1 & y_4 \end{bmatrix},$$

$(x_i, y_i, z_i \in \mathbf{Z})$.

The numbers x_i, y_i, z_i can be computed by means of the equalities (*). Thus e.g. for $A = \{1, 3, 5\}$ we have

$$M = \begin{bmatrix} 1 & 0 & 0 & 0 & 5 & 0 \\ 0 & 1 & 8 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 8 \end{bmatrix}$$

and for $A = \{2, 5\}$

$$M = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 12 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 12 \end{bmatrix}.$$

5.9. Let $A = \left\{1 \leqq a \leqq \frac{l-3}{2} : l/B_{2a}\right\}$, $\bar{A} = A \cup \left\{\frac{l-1}{2}\right\}$. Using tables of indices ([3]) and tables of irregular primes ([4], s. also [1], Table 9) we can derive:

5.9.1. Proposition. *For each prime l, $3 \leqq l < 1{,}000$ the sets A and $\bar{A}$ are normal for the prime l.*

REFERENCES

[1] Z. I. Borevicz., I. R. Šafarevič, *Number Theory*, Accademic Press, New York, 1966. (Translation from Russian.)

[2] F. R. Gantmacher, *The Theory of Matrices*, Chelsea Publ. Comp., New York, 1960, vol. 1. (Translation from Russian.)

[3] C. G. J. Jacobi, *Canon Arithmeticus*, Akademie-Verlag, Berlin, 1956.

[4] D. H. Lehmer, Emma Lehmer, H. S. Vandiver, *An application of high-speed computing to Fermat's last theorem*, Proc. Nat. Acad. Sci. U.S.A., 40 (1954), Nr. 1, 25–33.

[5] L. Skula, *Systems of equation depending on certain ideals*, Archivum Mathematicum (Brno), 21 (1985), 23–38.

[6] L. Skula, *A note on the index of irregularity*, Journal of Number Theory, 22 (1986), 125–138.

L. Skula
Department of Mathematics
Faculty of Science, J. E. Purkyně University
Janáčkovo nám. 2a, 662 95 Brno
Czechoslovakia