UNIVERSITAS COMENIANA
ACTA MATHEMATICA UNIVERSITATIS COMENIANAE
L—LI—1987

ON THE SPECIAL INVARIANT SUBSPACES OF A VECTOR SPACE OVER $\mathbf{Z}/l\mathbf{Z}$ (ABSTRACT)

LADISLAV SKULA, Brno

1. Notation. In this report we design by
l an odd prime
$N = 1/2(l-1)$
$\mathbf{V} = \{(a(1), a(2), \ldots, a(N))\colon a(i) \in \mathbf{Z}/l\mathbf{Z}\} = (\mathbf{Z}/l\mathbf{Z})^{(N)}$ the vector space over the field $\mathbf{Z}/l\mathbf{Z}$ with dimension N,
$\mathbf{L} = \{1, 2, \ldots, N\}$.
For integers $1 \le x, z \le l-1$ put

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

$f(x, z) \equiv \varepsilon(x, z)xz \pmod{l}$, $f(x, z) \in \mathbf{L}$.
For the vector $\boldsymbol{u} = (u(1), \ldots, u(N)) \in \mathbf{V}$ put

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

where $v(x) = \varepsilon(x, z)u(f(x, z))$ $(x \in \mathbf{L})$.

Then we can prove

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

(*b*) *For* $1 \le z, z' \le l-1$ *it holds* $S_z = S_{z'}$ *if and only if* $z = z'$.

(*c*) *For* $1 \le z, z', w \le l-1$, $w \equiv zz' \pmod{l}$ *it holds* $S_w = S_{z'} \circ S_z$.

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

The aim of our report is to describe all invariant subspaces of the vector space $\mathbf{V}$ with respect to the group $\{S_z\colon 1 \le z \le l-1\}$.

Further we denote by
r a primitive root mod l
ind x index of x relative to the primitive root r of l
$S = S_r$

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

where $A \subseteq \mathbf{L}$.

Then $\{S_z\colon 1 \leq z \leq l-1\} = \{S^n\colon 0 \leq n \leq l-2\}$ and the S_z — invariant subspaces of $\mathbf{V}$ for each $1 \leq z \leq l-1$ are just the S invariant subspaces of $\mathbf{V}$. Further we can prove

3. Proposition. (*a*) *It holds for* $A \subsetneq B \subseteq \mathbf{L}$ *the relation* $\mathscr{S}(A) \supsetneq \mathscr{S}(B)$.

(*b*) $\mathscr{S}(\emptyset) = \mathbf{V}$, $\mathscr{S}(\mathbf{L}) = 0$.

(*c*) *For each subset* $A \subseteq \mathbf{L}$ *the set* $\mathscr{S}(A)$ *forms an* S — *invariant subspace of the vector space* $\mathbf{V}$ *and* $\dim \mathscr{S}(A) = l^{N-|A|}$.

The set of all quadratic nonresidues $x \bmod l (1 \leq x \leq l-1)$ we denote by $\mathscr{N}$ and for $x \in \mathscr{N}$ put

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

where for $1 \leq t \in N$

$u(t) = x^{\operatorname{ind} t} \in \mathbf{Z}/l\mathbf{Z}$,considered as an element from $\mathbf{Z}/l\mathbf{Z}$.

The subspace of $\mathbf{V}$ generated by $\boldsymbol{u}(x)$ we denote by $\boldsymbol{U}(x)$, hence

$$\boldsymbol{U}(x) = \{k \cdot \boldsymbol{u}(x) : k \in \mathbf{Z}/l\mathbf{Z}\}.$$

Since

$$S(\boldsymbol{u}(x) = x \cdot \boldsymbol{u}(x),$$

the subspace $\boldsymbol{U}(x)$ is an S-invariant subspace of $\mathbf{V}$. It follows

4. Proposition. *Let* $X \subseteq \mathscr{N}$. *Then*

$$\boldsymbol{U}(X) = \Sigma\, \boldsymbol{U}(x)\, (x \in X) \text{ (the direct sum)}$$

is an S — *invariant subspace of* $\mathbf{V}$.

For the subspaces $\boldsymbol{U}(X)$ and the subspaces $\mathscr{S}(A)$ the following relations hold:

5. Proposition. (*a*) *For* $X, Y \subseteq \mathscr{N}$ *we have* $\boldsymbol{U}(X) \subseteq \boldsymbol{U}(Y)$ *if and only if* $X \subseteq Y$, *hence* $\boldsymbol{U}(X) = \boldsymbol{U}(Y)$ *if and only if* $X = Y$.

(*b*) *Let* $X \subseteq \mathscr{N}$ *and* $A = \mathbf{L} - \{N + 1 - 1/2(\operatorname{ind} x + 1)\colon x \in X\}$. *Then* $\boldsymbol{U}(X) = \mathscr{S}(A)$.

Now we describe all S — invariant subspaces of $\mathbf{V}$.

6. Theorem. *Let* $\boldsymbol{U}$ *be a non-zero S-invariant subspace of* $\mathbf{V}$. *Then there exists a subset* X *of the set* $\mathscr{N}$ *such that* $\boldsymbol{U} = \boldsymbol{U}(X)$.

The subset X is formed by means of the minimal polynómial $G(\lambda)$ of the subspace $\boldsymbol{U}$ with respect to the operator S.

REFERENCES

1. Gantmacher, F. R.: Těorija matric, Moskva 1966 (2nd edition).
2. Skula, L.: A note on index of irregularity, to appear.

3. Skula, L.: Systems of equations depending on certain ideals, Archivum Mathematicum (Brno), vol. 21, no 1 (1985), 23—38.

Author's oddress:
Ladislav Skula
Katedra matematiky PřF UJEP
Janáčkovo nám. 2, 662 95 Brno

Received: 12. 12. 1985

SÚHRN

O SPECIÁLNÍCH INVARIANTNÍCH PODPROSTORECH VEKTOROVÉHO PROSTORU NAD $\mathbf{Z}/l\mathbf{Z}$

Ladislav Skula, Brno

V této přednášce se uvažuje speciální automorfismus S vektorového prostoru $\mathbf{V}$ dimense $1/2 \cdot (l - 1)$ nad tělesem zbytkových tříd $\mathbf{Z}/l\mathbf{Z}$ (l liché prvočíslo). Jsou popsány všechny S-invariantní podprostory prostoru $\mathbf{V}$, ktoré jsou v přirozených korespondencích s podmnožinami množiny $\{1, 2, \ldots, 1/2\,(l - 1)\}$ a s podmnožinami kvadratických nezbytků $x \bmod l\,(1 \leq x \leq l - 1)$.

РЕЗЮМЕ

О СПЕЦИАЛЬНЫХ ИНВАРИАНТНЫХ ПОДПРОСТРАНСТВАХ ВЕКТОРНОГО ПРОСТРАНСТВА НАД $\mathbf{Z}/l\mathbf{Z}$

Ладислав Скула, Брно

В этом докладе изучается специальный линейный оператор S над $\frac{l-1}{2}$-мерном векторным пространством $\mathbf{V}$ над полем $\mathbf{Z}/l\mathbf{Z}$ (l простое число ≥ 3). Пописаны все S-инвариантные подпространства векторного пространства $\mathbf{V}$, которые в естественных кореспонденциях с подмножествами множества $\left\{1, 2, \ldots, \frac{1}{2}(l - 1)\right\}$ и с подмножествами квадратичных невычетов $x \bmod l\,(1 \leq x \leq l - 1)$.