Invariants of Semilinear Transformations

U. Dempwolff

ALWAYS: V finite dimensional vector space over the field K

1. REVISION FROM LINEAR ALGEBRA.

$T \in \mathrm{End}_K(V)$, then:

(a) $V = U_1 \oplus \cdots \oplus U_k$, U_i indecomposable T-space.

(b) Each $U = U_i$ is uniserial (i.e. it exists a unique T-composition series $0 = U^0 \subseteq U^1 \subseteq \cdots \subseteq U^m = U$ such that $soc(U) = U^1 \simeq U^{i+1}/U^i$ for all i).

Theorem. *The numbers k, $\dim U_i$, and the isomorphism types $soc(U_i)$ determine T uniquely.*

Description of irreducible operators

(c) Let V be T-irreducible. Then V can be identified with an extension field L of K, $[L : K] = \dim V$ and T with some $a \in L$ such that $L = K[a]$ and $xT = ax$.

Equivalent to: Let f be minimal polynomial of T. Then f is irreducible and $\dim V = \deg f$.

FROM NOW ON: $\sigma \in \mathrm{Aut}(K)$, T is *σ-linear (semilinear)* i.e.

$$(v + w)T = vT + wT, \quad (av)T = a^{\sigma}(vT).$$

PROBLEM: Find – if possible – a similar description of semilinear operators by invariants as above.

2. EXAMPLES OF MÄURER (1988).

$K = \mathbf{R}(t)$, $\sigma \in \mathrm{Aut}(K)$ defined by
$x^\sigma = x$, $x \in \mathbf{R}$ and $t^\sigma = t + 1$.

(a) $V = K^2$, $(x, y)T = (tx^\sigma + \frac{y^\sigma}{t}, y^\sigma)$.

V indecomposable: $0 \subseteq U = K(1, 0) \subseteq V$ unique T-series.

$$xT_U = tx^\sigma, \quad yT_{V/U} = y^\sigma$$

I.e. U and V/U are NOT T-isomorphic.

(b) $V = K^3$, $(x, y, z)T = (x^\sigma + \frac{y^\sigma}{t} + \frac{z^\sigma}{2t-1}, y^\sigma, z^\sigma)$.

V indecomposable: $U = K(1, 0, 0)$ unique minimal T-space.

V NOT uniserial: Set $U_1 = U + K(0, 1, 0)$ and $U_2 = U + K(0, 0, 1)$, then

$$V/U = U_1/U \oplus U_2/U.$$

FROM NOW ON: $|\sigma| = n < \infty$.

Set $K_0 = K_\sigma$. Then $K : K_0$ is a Galois extension with $\text{Gal}(K : K_0) = \langle\sigma\rangle \simeq \mathsf{C}_n$.

3. JACOBSON (1937)

Theorem. *Let T be a σ-linear operator on the finite dimensional K-space V. Then:*

(a) $V = U_1 \oplus \cdots \oplus U_k$, U_i indecomposable T-space.

(b) Each $U = U_i$ is uniserial and each T-composition factor is isomorphic to $soc(U)$.

(c) The numbers k, $\dim U_i$, and the isomorphism types $soc(U_i)$ determine T uniquely.

Method of proof: Theory of noncommutative polynomial rings (initiated by Ore, extended by Jacobson).

D. (1990, 1999) direct, elementary proofs.

REMAINING PROBLEM: Classification and concrete description of *irreducible* T-spaces V.

4. KANTOR-LIEBLER (2008)

Theorem. *Let T be an irreducible, σ-linear operator on the finite K-space V, $K = \mathrm{GF}(q^n)$. Then there is a decomposition*

$$V = U_0 \oplus \cdots \oplus U_{d-1}$$

of V into subspaces U_i permuted cyclically by T such that $T^d_{U_i}$ is a one dimensional affine map over an extension field of K. Moreover, d divides $|\sigma| = n$, and the map $T^d_{U_i}$ uniquely determines T up to $\mathrm{GL}(V)$-conjugacy.

PROBLEMS LEFT:

1. Understand the role of the extension field.

2. More concrete description and classification.

3. Infinite fields.

FROM NOW ON: T irreducible, $|\sigma| = n < \infty$, $K : K_0$ Galois, and $\mathrm{Gal}(K : K_0) = \langle\sigma\rangle \simeq \mathrm{C}_n$.

5. REDUCTION, TRANSLATION THEOREM

Lemma. *T^n has an irreducible, minimal minimal polynomial f_0 over K_0 and $F = K_0[T^n]$ is a field.*

Let $K = K_0[\omega]$, f the minimal polynomial of ω over K_0 and L the splitting field of f over F. (call L the *composition of* K and F). From Galois theory:

Translation Theorem. *There is an embedding $K \to \widetilde{K} \subseteq L$. Set $d = [\widetilde{K} \cap F : K_0]$ and $n' = n/d$. Then $[L : F] = n'$ and* $\mathrm{Gal}(L : F) = \langle\gamma\rangle = \mathrm{C}_{n'}$, *and $\widetilde{x}^\gamma = \widetilde{x^{\sigma^d}}$ for $x \in K$.*

Reduction Lemma.

(a) $V = U_0 \oplus \cdots \oplus U_{d-1}$ *(as a K-space and as a F-space), and T permutes cyclically the U_i's.*

(b) Each $U = U_i$ has the structure of an $L-$ space and T^d with respect to this structure is an irreducible, γ-linear operator on U.

Remarks. (a) Let $\widetilde{K} \cap F = K_0[\widetilde{\omega_0}]$ and $K_0[\omega_0]$ the counter image in K. Then U_i is the *eigenspace* for the *eigenvalue* $\widetilde{\omega_0^{\sigma^i}}$ for the F*-linear* operator $R(\omega_0)$ defined by

$$vR(\omega_0) = \omega_0 v.$$

(b) Kantor-Liebler situation: the U_i's are *one dimensional* L-spaces.

6. SEPARABILITY

Schur's Lemma: The centralizer S of $K \cup \{T\}$ in $\mathrm{End}_{K_0}(V)$ is a skew field.

Call T *separable* if S is commutative, i.e. a field. Always true if $|K| < \infty$.

Theorem. *Let T be separable. Then:*

(a) $S = F$ and $\dim_F V = n$ (and $\dim_L U_i = 1$).

(b) T is uniquely determined by T^n. I.e. if T' is separable, σ-linear and $T^n \sim (T')^n$ in $\mathrm{GL}(V)$, then $T \sim T'$ in $\mathrm{GL}(V)$.

Remark. There exist irreducible, but not separable, σ-linear operators.

7. DESCRIPTION OF SEPARABLE OPERATORS

Goal: Let K, σ, and $m > 0$ be given. Construct all irreducible, σ-linear operators on an m-dimensional K-space.

Idea: Consider all field extensions $F : K_0$ of degree m and choose u as a generator of F, i.e. $F = K_0[u]$ (u will take the role of T^n).

Necessary: u is an image of the norm map $\mathrm{N}_{L:F} : L \to F$.

CONSTRUCTION I. Let K, m, and u be as above. Set $V = L^d$ and define a K-structure on V by

$$\alpha \cdot (x_0, x_1, \ldots, x_{d-1}) = (\widetilde{\alpha} x_0, \widetilde{\alpha^{\sigma}}, \ldots, \alpha^{\widetilde{\sigma^{d-1}}} x_{d-1}).$$

Pick $w \in L$ with $\mathrm{N}_{L:F}(w) = u$ and define a σ-linear operator $T = T_w$ by

$$(x_0, x_1, \ldots, x_{d-1})T = (x_1, \ldots, x_{d-1}, wx_0^\gamma)$$

(γ as in the Translation Theorem).

Theorem. *Every separable (thus irreducible), σ-linear operator is obtained by Construction I.*

Drawback: Artificial definition of the K-structure.

CONSTRUCTION II (for finite fields). Assume now $K_0 = \mathrm{GF}(q)$ and $K = \mathrm{GF}(q^n)$. Then $F = \mathrm{GF}(q^m)$ and $L = \mathrm{GF}(q^{mn/d})$ with $d = (m, n)$. Wlog. $x^\sigma = x^q$.

Set again $V = L^d$ with the natural K-structure. Extend σ to L by $y^\sigma = y^q$, $y \in L$.

For $u \in F$ ($F = K_0[u]$) choose again $w \in L$ with $\mathsf{N}_{L:F}(w) = u$. Define a *second* extension ρ of σ to L by

$$y^\rho = y^{q^{cm-d+1}}$$

where

$$(c, \frac{n}{d}) = 1, \; x^{q^{cm}} = x^{q^d}, \; x \in K.$$

Define a σ-linear operator $T = T_w$ by

$$(x_0, x_1, \ldots, x_{d-1})T = (wx_{d-1}^\rho, x_0^\sigma, \ldots, x_{d-2}^\sigma).$$

Theorem. *Every irreducible, semilinear operator on a finite vector space is obtained by Construction II.*

Note: In general $\sigma \neq \rho$!

Example. Set $K = \mathrm{GF}(2^6)$, σ Frobenius automorphism, and $m = 4$. Then $F = \mathrm{GF}(2^4)$, $L = \mathrm{GF}(2^{12})$, and $V = L^2$. Choose $w \in L$ such that $|\mathrm{N}_{L:F}(w)| = 15$. Define T by

$$(x, y)T = (wy^{2^7}, x^2).$$

Then T has order 90.

On the other hand: Let M be an extension field of K such that $\dim_K M^d = 4$ (i.e. $|M^d| = 2^{24}$). Let $v \in M$ and define T'

$$(x_0, \ldots, x_{d-1})T' = (vx_{d-1}^2, x_0^2, \ldots, x_{d-2}^2).$$

The order $|T'|$ is NOT divisible by 5.

Consequence of the Theorem: T_w and $T_{w'}$ are conjugate under GL(V) iff $\mathsf{N}_{L:F}(w)$ and $\mathsf{N}_{L:F}(w')$ are conjugate under Gal($F : K_0$).

Example. The irreducible, semilinear operators on $V = K^6$, $K = \mathrm{GF}(2^2)$.

$\|\sigma\|$	$\|F\|$	$\|L\|$	$\|K_0\|$	d	$\|\mathsf{N}_{L:F}(w)\| = \|w\|$	classes
2	2^6	2^6	2	2	$9, 21, 63$	9

Example. The irreducible, semilinear operators on $V = K^2$, $K = \mathrm{GF}(2^6)$.

$\|\sigma\|$	$\|F\|$	$\|L\|$	$\|K_0\|$	d	$\|\mathsf{N}_{L:F}(w)\|$	classes
6	2^2	2^6	2	2	3	1
3	2^4	2^{12}	2^2	1	$5, 15$	6
2	2^6	2^6	2^3	2	$3, 9, 21, 63$	28

Altogether $2 \cdot 1 + 2 \cdot 6 + 28 = 42$ classes.

8. FINAL REMARKS

1. ASANO and NAKAYAMA (1938) show in "Über halblineare Transformationen":

T, T' σ-irreducible and $T^n \sim (T')^n \Rightarrow T \sim T'$

Tool: Noncommutative polynomial rings.

2. $S = (S, +, \cdot)$ is a *semifield* if all axioms for a field hold except possibly the associativity of multiplication.

Let T be σ-irreducible on $V = V(m, K)$ and let $\phi : V \to \bigoplus_{i=0}^{m} KT^i$ be a K_0-isomorphism. Then

$$v * w = v\phi(w)$$

defines a semifield multiplication on V.