Lineare Schieberegisterfolgen

Sei K ein endlicher Körper. Man nehme zwei Vektoren $\begin{pmatrix} x_0 \\ \vdots \\ x_{n-1} \end{pmatrix}, \begin{pmatrix} a_0 \\ \vdots \\ a_{n-1} \end{pmatrix} \in K^n$, berechne $x_n := \sum_{i=0}^{n-1} a_i x_i$ und betrachte die lineare Abbildung $\Phi : K^n \to K^n$, die durch $\begin{pmatrix} x_0 \\ \vdots \\ x_{n-1} \end{pmatrix} \to \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ gegeben ist. Man kann sich dabei vorstellen, daß nach der Berechnung von x_n die Vektorkomponenten nach oben verschoben werden, wobei x_0 herausfällt und x_n unten nachrückt. Die zu dieser „Schiebeabbildung“ gehörige „Schiebematrix“ ist offenbar

$$A = \begin{pmatrix} 0 & 1 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 0 & \ddots & \cdots & \vdots \\ \vdots & \vdots & \vdots & \ddots & \ddots & 0 \\ 0 & 0 & 0 & & 0 & 1 \\ a_0 & a_1 & & \cdots & & a_{n-1} \end{pmatrix} .$$ Man beweist induktiv, daß $\chi_A = X^n - \sum_{i=0}^{n-1} a_i X^i$.

Durch wiederholte Anwendung der Schiebeabbildung, ausgehend von einem Startvektor $0 \neq v_0 \in K^n$, also durch die Rekursion $v_k = \Phi(v_{k-1})$ für $k > 0$, erhält man eine Folge (v_k) in K^n . Indem man nur die ersten Komponenten dieser Vektorfolge betrachtet, ergibt sich eine Folge in K , welche man auch als *Schieberegisterfolge* bezeichnet.

Die Vektorfolge und damit auch die Schieberegisterfolge wird periodisch, sobald sich in der Sequenz $\begin{pmatrix} x_0 \\ \vdots \\ x_{n-1} \end{pmatrix} \to \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \to \cdots \to \begin{pmatrix} x_k \\ \vdots \\ x_{k+n-1} \end{pmatrix}$ ein Vektor wiederholt, was ja wegen der Endlichkeit von K nach spätestens $|K|^n - 1$ Iterationen geschehen muß.

Eine endliche Folge $v_0 \to \ldots \to v_k \to \ldots \to v_{N-1}$ mit $v_{N-1} \to v_N = v_0$ nennt man einen *Zykel* , bzw. einen *N*-Zykel.

Für Anwendungen wichtig ist die Frage, ob man den „Steuervektor“ $a \in K^n$ so wählen kann, daß man einen Zykel der maximal möglichen Länge $|K|^n - 1$ erhält[1] .

Wir illustrieren die Möglichkeiten am Beispiel $K = \mathbb{Z}_2$ und zunächst *n*=3:

a) Mit $a = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$ erhält man als charakteristisches Polynom $\chi_A = X^3 + X^2 + X + 1 = (X+1)^3$ sowie die Zykel $\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \to \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$, $\begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} \to \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \to \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}$ und $\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \to \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \to \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} \to \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} \to \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$.

1 Der Nullvektor darf dabei natürlich nicht vorkommen: er bildet für sich einen Zykel der Länge 1.

b) Wählt man dagegen $a=\begin{pmatrix}1\\1\\0\end{pmatrix}$, so ergibt sich $\begin{pmatrix}1\\0\\1\end{pmatrix}\to\begin{pmatrix}0\\1\\1\end{pmatrix}\to\begin{pmatrix}1\\1\\1\end{pmatrix}\to\begin{pmatrix}1\\1\\0\end{pmatrix}\to\begin{pmatrix}1\\0\\0\end{pmatrix}\to\begin{pmatrix}0\\0\\1\end{pmatrix}\to\begin{pmatrix}0\\1\\0\end{pmatrix}\to\begin{pmatrix}1\\0\\1\end{pmatrix}$,
so daß die Periode hier maximal ist und die Schieberegisterfolge (x_n) , die man aus den ersten Komponenten abliest, die Werte 1 0 1 1 1 0 0 besitzt, bevor sie sich wiederholt.

Das charakteristische Polynom ist hier $\chi_A=X^3+X+1$, und dies ist irreduzibel in $\mathbb{Z}_2[X]$.

Offenbar hat die Reduzibilität oder Irreduzibilität des charakteristischen Polynoms etwas mit der Periodenlänge zu tun, denn es gilt der **Satz**[2]:

> Ist V ein endlichdimensionaler K-Vektorraum und $\Phi: V\to V$ linear, so ist das charakteristische Polynom $\chi_\Phi\in K[X]$ genau dann irreduzibel[3], wenn es bezüglich Φ keinen nicht-trivialen invarianten Unterraum von K^n gibt.

Ein reduzibles Polynom bedeutet also, daß ein Φ - invarianter Unterraum $U\subset K^n$ existiert – also einer, der durch Φ in sich selbst abgebildet wird. Starten wir daher eine Iterationsfolge mit einem Vektor aus U , so bleiben wir in U und erhalten keine maximale Periode.

c) Es sei diesmal n=4 , und $a=\begin{pmatrix}1\\1\\1\\1\end{pmatrix}$.
Man errechnet $\chi_A=X^4+X^3+X^2+X+1$; dieses Polynom ist ebenfalls irreduzibel, wir haben also keinen invarianten Unterraum, jedoch ergibt sich folgende Iterationsfolge:
$\begin{pmatrix}1\\0\\0\\0\end{pmatrix}\to\begin{pmatrix}0\\0\\0\\1\end{pmatrix}\to\begin{pmatrix}0\\0\\1\\1\end{pmatrix}\to\begin{pmatrix}0\\1\\1\\0\end{pmatrix}\to\begin{pmatrix}1\\1\\0\\0\end{pmatrix}\to\begin{pmatrix}1\\0\\0\\0\end{pmatrix}$ mit der Zykellänge 5 und nicht etwa der maximal möglichen Periode 15. Die fünf Vektoren dieser Folge spannen den gesamten Raum Z_2^4 auf.
Es gibt noch zwei weitere Zykel der Länge 5: schließlich muß ja der gesamte Raum durch Zykel ausgeschöpft werden.

Die Irreduzibilität von χ_A und damit die Nicht-Existenz eines echten invarianten Unterraums ist also nicht hinreichend für eine maximale Zykellänge.

Definition
Ein irreduzibles Polynom $f\in K[X]$ heißt primitiv, wenn die Restklasse $\overline{X}$ im Körper $K[X]/<f>$ dessen multiplikative Gruppe erzeugt.

---

2 Beweis am Ende dieses Artikels
3 Man beachte, daß ein Polynom in $K[X]$ irreduzibel sein kann, während es bezüglich einem Erweiterungskörper von K in nicht-triviale Faktoren zerfällt. Dabei liegen dann einige Koeffizienten der Faktoren nicht mehr in K .

Beispiele:

Im obigen Beispiel b) ist $\chi_A = X^3 + X + 1$ irreduzibel. Die multiplikative Gruppe des Körpers $K[X]/<\chi_A>$ besitzt 7 Elemente, und es ist leicht nachzurechnen, daß $\overline{X}^1 = \overline{X}$ $\overline{X}^2 = \overline{X^2}$, $\overline{X}^3 = \overline{X+1}$, $\overline{X}^4 = \overline{X^2+X}$, $\overline{X}^5 = \overline{X^2+X+1}$, $\overline{X}^6 = \overline{X^2+1}$, $\overline{X}^7 = \overline{1}$. Damit treten alle von Null verschiedenen Elemente des Körpers als Potenzen von $\overline{X}$ auf: Das Polynom χ_A ist also primitiv.

Im Beispiel c) ist $\chi_A = X^4 + X^3 + X^2 + X + 1$ ebenfalls irreduzibel. Jedoch erhält man hier durch Multiplikation mit $\overline{X}$ den 5-Zykel $\overline{X} \rightarrow \overline{X^2} \rightarrow \overline{X^3} \rightarrow \overline{X^4} = \overline{X^3+X^2+X+1} \rightarrow \overline{X^5} = \overline{1} \rightarrow \overline{X^6} = \overline{X}$.
Man sieht deutlich die Analogie zu den 5-Zykeln in Beispiel c) .
Jedenfalls ist das charakteristische Polynom in diesem Beispiel nicht primitiv.

Satz:

Eine Schieberegisterfolge hat genau dann maximale Länge, wenn das charakteristische Polynom der Schiebeabbildung primitiv ist.

Vor dem Beweis des Satzes ein Beispiel:
Weiter unten soll gezeigt werden, daß das Polynom $X^{127} + X + 1$ primitiv ist. Im „Steuervektor" *a* sind also $a_0 = a_1 = 1$ und alle übrigen $a_k = 0$. Nach obigem Satz erhalten wir eine Schieberegisterfolge maximaler Länge $2^{127} - 1 \approx 10^{38}$, die z.B. durch die ersten 127 Bits festgelegt ist

```
1011010010011010101000100010011011001100011000101011011001011001011110100100010110001100111000111010100000111011101101111100101
```

und dann zunächst so weitergeht:

```
1101110110101111111001100110101101010100101001111101101011101011100011101100111010010101001001001111100001001100110110000101110
0110011011110000000101010101111011111110111101000011011110011110010010011010100111011111101101101000010001101010101101000111001 0
1010101100010000011111111100011000000110001110001011000101000101101101011111010011000001101101110001100101111111101110010010111
1111110100110000100000000100101000000101001001001110100111100111011011110000111010100001011011001001010111000000011001011011100 0
0000011101010001100000001101111000011110110110100111010001010011011000100010011111100011101101011011111001000000101011101100 1000
0000100111110010100000001011000100010001101101111010011100111101011010011001101000010010011011110110000101100000111110010101100 0
0001101000010111100000011101001100110010110110011101001010001111011101010101011100011011010110001101000111010000100001010111101000
0010111000111000100001001110101010101110110101001110111100100011001111111100100101101111010010111001001110001100011111000111000
0111001001001001100011010011111111110011011111010011000101100101010000000101101110110001110111001011010010010100100001001001000
1001011011011010100101110100000000001010110000111010100111010111111000000111011001101001001100101110111011011110110001101101100 1
1011101101101111011100111000000000111110100010011111010011110000010000010011010101110110101011100110011011000110100101101101010
1100110110110000110010100100000000100001110011010000111010001000011000011010111111001101111111001010101011010010111011101101111 11
0101011011010001010111101100000001100010010101110001001110011000101000101111000001010110000001011111111011101110011001101100000 1
1111101101110011110001101000001010011011111001001101001010100111100111000100001111101000011100000000011001100101010101101000010
0000110110010100001001011100001111010110000101101011101111111010001010010011000100001110001001000000001010101011111111101110001 10
0001011010111100011011100100010001111010001110111100110000011100111101101010011000100100110110000000111111111000000000110010010 10
0011101111000100101100101100110010001110010011000101010000100101000110111110101001101101011010000001000000000100000000101011011 110
0100110001001101110101110101010110010010110101001111110001101111001011000011111010110111101110000110000000110000001111101100010
1101010011010110011110011111111010110111011111010000001001011000101110100010000111101100011001000101000000010100000010000110100111
0111110101111010100010100000001111011001100001110000110111010011100111001100010001101001010110011110000011110000110001011101001
1000011110001111100111100000001000110101010001001000101100111010010100101010011001011101111101010001000010001000101001110011 1010
1000100010010000101000100000110010111111100110110011101010011101111011111101010111001100001111100110001100110011110100101001111
1001100110110001111001100001010111000000010101101010011111010011000110000011111100101010001000010101001010101010001110111101 0000
1010101011010010001010100011111001000000111110111111010000111010100101000010000010111111100110001111110111111111100100110001110001
1111111011101100111111001000010110000100001100001110001001111101111000110000111000000101010010000011000000000101101010010010010
0000000110011010100000101100011101000110001010001001001101000011000100101000100100001111110110000101000000000111011111011011 0110
0000001010101111100001110100100111001010011110011011010111000101001101111001101100010000011010001111000000001001100001101101 1010
0000011111110000100010011101101001011110100010101101111001001111010110001010110100110000101110010001000000011010100010110110111 0
0000100000010001100110100110111011100011100111110110001011010001111010011111011101010001110010110011000000101111100111011011001 0
0001100000110010101011101011001100100100101000011010011101110010001110100001100111110010010111010101000011100001010011011010110
0010100001010111111100111101010101101101111000101110100110010110010011100010101000010110111001111111000100100011110101101111010
0111100011111000000010100011111111011011000100111001110101011101011010010011111100011101100101000000100110110010001111011000111 0
1000100100000100000111100100000000110110100110100101001111110011110111011010000001001001101011110000011010110101100100011010010011
1001101100011000010001011000000010110111010111011110100000010100011001101110000110110101111000100000101111011110101100101110110100
1010110100101000110011101000000111011001111001100011100001111001010101100100010110111100010011000111000110001111010111001101110 1
1111011101111001010100111000010011010100010101001001000100010111111110101100111011000100110101001001001010010001111001010110011 0
0001100110001011111101001000110101111100111111011011001100111000000011110101001101001101011111011011011110110010001011111010101 0
0010101010011100000111011001011110000101000001101101010101001000000100011111010111010111100001101101100011010110011100001111111 0
0111111110100100001001101011100010001111000010110111111111011000011001000011110011110001000101101101001011110101001000100000001 0
1000000011101100011010111100100110010001000111011000000000110100010101100010001010001001100111011011101110001111101100110000011 1
1000000100110100101111000101101010110011001001101000000001011100111110100110011110011010101001101100110010010000110101010000100 0
1000001101011101110001001110111111010101011010111000000011100101000011101010100010101111111101011010101011011000101111111000110 01
1000010111100110010011010011000001111111101111001000000100101111000100111111100111100000011101111111101101001110000000100101010
1000111000101010110101110101000010000000110001011000011011100010011010000000101000010000010001100000001101110100100000110111111 1
1001001001111111011110011111000110000001010011101000101100100110101110000011110001100001100101000000010110011101100001011000000 0
1011011010000000110001010000100101000001111010011100111010110101111001000010001001010001010111100000111010100110100011101000000 1
1101101110000001010011110001101111000010001110100101001111011110001011000110011011110011110001000010011111010111001001110000010
0110110010000111101000100101100010001100100111011110100011000100111010010101011000101000010011000110100001111001011010010000110
1011010110001000111001101110100110010101101001100011100101001101001110111111101001111000110101001011100010001011101110110001011
1101111010011001001010110011101010111110111010100100101111010111010011000000111010001001011110111001001100111001100110100111 00
```

Weil wir die Zeilenlänge dieses Outputs genau auf 127 gesetzt haben, lassen sich Muster in dieser Schieberegisterfolge erkennen: die Struktur des gewählten einfachen Steuervektors führt u.a. dazu, daß unter einer maximalen Gruppe von Einsen oder einer maximalen Gruppe von Nullen eine um ein Element kürzere Gruppe von Nullen stehen muß.

Beweis:

Wir fassen den Körper $E := K[X]/<\chi_A>$ als n-dimensionalen K-Vektorraum auf mit der Basis $e^0 = 1 = X^0, e^1 = X = X^1, e^2 = X^2, \ldots, e^n - 1 = X^{n-1}$, wobei wir verkürzt z.B. X^2 statt $\overline{X}^2$ schreiben.

In E können wir die Multiplikation mit X als lineare Abbildung $\Psi : E \to E$ auffassen.

Ψ hat bezüglich obiger Basis die Matrixdarstellung $B = \begin{pmatrix} 0 & 0 & 0 & \ldots & 0 & a_0 \\ 1 & 0 & 0 & \ldots & 0 & a_1 \\ 0 & 1 & 0 & \ldots & 0 & a_2 \\ 0 & 0 & 1 & \ldots & \vdots & a_3 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & 1 & a_{n-1} \end{pmatrix}$,

und offenbar ist $B = A^t$!!

Die Primitivität von χ_A ist also äquivalent zur folgenden Aussage:

> Die Folge 1, $\Psi(1) = X$, $\Psi^2(1) = X^2, \ldots, \Psi^k(1) = X^k, \ldots$ durchläuft alle von Null verschiedenen Elemente von E.

D.h. wiederholte Anwendung von Ψ erzeugt eine Folge der Länge $N = |K|^n - 1$.

Gleichzeitig sieht man sofort, daß $\Psi^N = id$!! Und außerdem ist offenbar N die kleinste Zahl, für die dieses gilt. Daraus folgt sofort $E = B^N = (A^t)^N = (A^N)^t$, und N ist die kleinste Zahl mit dieser Eigenschaft.

Dieselbe Aussage gilt dann natürlich auch für die Abbildung Φ und die Matrix A.

Iterieren wir also die Abbildung Φ , beginnend mit einem Vektor $0 \neq x_0 \in K^n$, setzen also für $k \geqslant 0$ $x_k = \Phi^k(x_0) = \Phi(x_{k-1})$, so kehren wir nach N Iterationen zum Ausgangsvektor x_0 zurück.

Nehmen wir an, es gäbe eine Periode kürzerer Länge, d.h. einen Vektor $0 \neq y \in K^n$ und $\Phi^M(y) = y$ für $1 \leqslant M < N$.

Sei $U \subset K^n$ der Unterraum, der von den Vektoren $\Phi^i(y)$ $0 \leqslant i \leqslant M$ aufgespannt wird. Weil $\Phi^k(\Phi^i(y)) = \Phi^i(\Phi^k(y)) = \Phi^i(y)$ gilt $\Phi^k = id$ auf diesem Erzeugendensystem von U und damit auf ganz U. Damit ist U ein invarianter Unterraum des K^n und damit schon gleich K^n . Dann gilt aber überhaupt $\Phi^k = id$, damit aber auch $A^k = E$, was wir oben schon ausgeschlossen hatten.

Es ergibt sich, daß die Folge (x_k) , gegeben durch $x_k = \Phi^k(x_0) = \Phi(x_{k-1})$ den gesamten Raum $K^n - \{0\}$ durchläuft.

Beweis daß Reduzibilität des charakteristischen Polynoms äquivalent zur Existenz eines nicht-trivialen invarianten Unterraums ist

Zunächst die einfachere Richtung:
Sei $U \subset V$ ein nicht-trivialer Φ - invarianter Unterraum, $0 < k = \dim U < n = \dim V$.
Dann gibt es eine Basis $u_1, \ldots, u_n$ von V, so daß $u_1, \ldots, u_k$ Basis von U ist.

Bezüglich dieser Basis wird Φ durch eine Blockmatrix der Form $M = \begin{pmatrix} A & B \\ 0 & C \end{pmatrix}$ dargestellt, wobei $A \in M_n(K)$ die Abbildung $\Phi : U \to U$ bezüglich der Basis $u_1, \ldots, u_k$ beschreibt.

Offenbar errechnet sich das charakteristische Polynom von M und damit von Φ als Determinante von $\begin{pmatrix} XE - A & -B \\ 0 & XE - C \end{pmatrix}$, wobei wir es links oben mit einer kxk und rechts unten mit einer (n-k)x(n-k)-Einheitsmatrix zu tun haben. Damit ist $\chi_\Phi = \chi_A \chi_C$ und also reduzibel.

Sei jetzt umgekehrt das charakteristische Polynom χ_Φ reduzibel, also $\chi_\Phi = fg$ mit $f, g \in K[X]$ beide normiert vom Grad $k > 0$. Indem wir f ggf. weiterzerlegen, gehen wir oBdA davon aus, daß f irreduzibel vom Grad k $0 < k < n$ und normiert ist. Mit Hilfe von f müssen wir jetzt irgendwie einen Φ - invarianten Unterraum konstruieren.

Dabei nehmen wir wieder einen Erweiterungskörper $E \supset K$ zu Hilfe, bezüglich welchem f eine Zerlegung $\prod_{i=1}^{k} (X - \zeta_i)$ besitzt.

Diesen Erweiterungskörper können wir wie üblich als Restklassenkörper $E = K[X] / < f >$ konstruieren. In diesem Restklassenkörper ist z.B. $\zeta := \overline{X}$ eine Nullstelle von f, denn es ist ja $\overline{0} = \overline{f} = \overline{f(X)} = f(\overline{X})$. Wie man die übrigen Nullstellen findet, sei hier nur für den Fall erklärt, daß $K = \mathbb{Z}_p$; der allgemeine Fall sieht ganz ähnlich aus. K und damit E sind dann von der Charakteristik p, die Abbildung $\sigma : E \to E$, die durch $\sigma(x) = x^p$ gegeben ist, ist ein Körper-automorphismus[4], welcher, eingeschränkt auf K, die Identität ergibt[5]. Damit sind die p Elemente von K Nullstellen des Polynoms $X^p - X$. Da dieses Polynom p-ten Grades aber auch nicht mehr als p Nullstellen besitzen kann, ist $K = \{ x \in E \mid \sigma(x) = x \}$ der sogenannte *Fixkörper* von σ. Da f Koeffizienten in K besitzt, folgt nun sofort $f(\sigma(\overline{X})) = \sigma(f(\overline{X})) = 0$, d.h. $\sigma(\overline{X})$ ist eine weitere Nullstelle von f in E, und genauso sind $\sigma^2(\overline{X}) = \sigma(\sigma(\overline{X})), \ldots, \sigma^k(\overline{X})$ ebenfalls Nullstellen. Man zeigt auch unschwer, daß diese alle verschieden sind.

Nun sind $\zeta_1, \ldots, \zeta_k \in E$ auch Nullstellen des charaktistischen Polynoms χ_Φ von Φ. Wählen wir eine Basis $u_1, \ldots, u_n$ von V, so wird Φ durch eine Matrix $A \in M_n(K)$ dargestellt. Fassen wir nun A als Matrix in $M_n(E)$ auf, die eine lineare Abbildung $E^n \to E^n$ beschreibt, so sind $\zeta_1, \ldots, \zeta_k \in E$ Eigenwerte dieser Matrix. Wählen wir zu jedem dieser Eigenwerte ζ_i einen Eigenvektor v_i und bilden die von diesen aufgespannten E-Unterräume $E_i = < v_i >$, sow

4 Die Verträglichkeit mit der Addition ergibt sich, weil in der binomischen Formel die Binomialkoeffizienten $\binom{p}{k}$ für $0 < k < p$ durch p teilbar sind und damit in E verschwinden.

5 Die multiplikative Gruppe K^* besitzt p-1 Elemente, daher ist für $x \neq 0$ $x^{p-1} = 1$ und daher $x^p = x$. $0^p = 0$ gilt sowieso.

werden diese durch A in sich selbst abgebildet, sind also unter A invariant . Wir bilden die direkte Summe $W:=\left\{x_1+\ldots+x_k \middle| x_i\in E_i\right\}$ invarianten Räume, die dann natürlich auch invariant ist. Dieser invariante E-Unterraum ist offenbar k-dimensional, denn die E_i sind eindimensional. Dazu muß aber noch gezeigt werden, daß die Darstellung eines Vektors $W\ni x=x_1+\ldots+x_k$ eindeutig bestimmt ist. Wäre dies nicht der Fall, so gäbe es eine nicht-triviale Darstellung $0=x_1+\ldots+x_k$. Konstruieren wir nun die Produktmatrix $B=(\zeta_2 E-A)\cdots(\zeta_k E-A)$. Das Besondere an dieser Matrix ist, daß man ihre Faktoren beliebig umordnen kann, wie man sofort nachrechnet. Wir wenden B auf beide Seiten der Gleichung $x_1+\ldots+x_k=0$ an . Man sieht, daß jeder Summand auf der linken Seite außer x_1 von einem der Faktoren von B zum Verschwinden gebracht wird, während Bx_1 nur dann Null sein kann, wenn auch $x_1=0$. Auf analoge Weise zeigt man, daß auch die anderen $x_i=0$ sein müssen.

Jedenfalls ist nun W ein bezüglich E k-dimensionaler A – invarianter Unterraum von E^n .
Der Haken ist, daß W nicht ein K-Unterraum von K^n ist, und so einen suchen wir eigentlich.

Andererseits ist jeder E-Vektorraum auch ein K-Vektorraum, indem wir als Skalare, mit denen wir Vektoren multiplizieren, eben nur solche aus K zulassen.

Wichtig im Folgenden ist noch, daß σ^k auf E die Identität ist.
Dies ist richtig, denn $\sigma^k(x)=\underbrace{x^p\cdots x^p}_{k\text{- mal}}=x^{pk}$. Weil pd die Elementezahl von E ist, also pk-1 die Elementezahl der multiplikativen Gruppe von E , gilt für $x\neq 0$ $x^{pk-1}=1$ und somit für alle $x\in E$ $x^{pk}=x$.

Betrachten wir nun die Abbildung $\sigma: E^n\to E^n$, die gegeben ist durch $\sigma\begin{pmatrix}x_1\\ \vdots\\ x_n\end{pmatrix}=\begin{pmatrix}\sigma(x_1)\\ \vdots\\ \sigma(x_n)\end{pmatrix}$.
Offenbar gilt für $x, y\in E^n$ $\sigma(x+y)=\sigma(x)+\sigma(y)$ und für $\lambda\in E$ $\sigma(\lambda x)=\sigma(\lambda)\sigma(x)$ und für $\mu\in K$ $\sigma(\mu x)=\sigma(\mu)\sigma(x)=\mu\sigma(x)$. σ ist also K-linear!!

Die K-lineare Abbildung σ wirkt auf dem Unterraum $K^n\subset E^n$ offenbar als die Identität.

Ist $x\in E^n$ ein Eigenvektor von A zum Eigenwert ζ_1 , gilt also $x\in E_1$ bzw. $Ax=\zeta_1 x$, so ist $A(\sigma(x))=\sigma(A(x))=\sigma(\zeta_1 x)=\sigma(\zeta_1)\sigma(x)=\zeta_2\sigma(x)$, so daß $\sigma(x)\in E_2$!

Wir bilden jetzt die Menge $U:=\left\{x_1+\ldots+x_k\in W\subset E^n \middle| x_1\in E_1, x_2=\sigma(x_1),\ldots, x_k=\sigma(x_{k-1})\right\}$ und sehen sofort, daß es sich um einen K-Unterraum von W handelt, der sicher nicht der Nullraum ist. Ist also $x_1+\ldots+x_k\in U$, so ist auch $\sigma(x_k)=x_1$, da ja $\sigma(x_k)=\sigma^k(x_1)=x_1$ nach obiger Bemerkung.

Offenbar gilt jetzt für $x\in U$ $\sigma(x)=\sigma(x_1)+\ldots+\sigma(x_k)=x_2+\ldots+x_k+x_1=x$, so daß U ein Unterraum von K^n ist. Andererseits ist auch U invariant unter A , denn für $x\in U$ gilt $A(x)=A(x_1+\ldots+x_k)=Ax_1+\ldots+Ax_k$ und $Ax_1\in E$ und $Ax_2=A(\sigma(x_1))=\sigma(Ax_1)$, ... , $Ax_k=A(\sigma(x_{k-1}))=\sigma(Ax_{k-1})$, so daß tatsächlich $Ax\in U$.

Damit haben wir einen nicht-trivialen A-invarianten Unterraum von $U\subset K^n$ gefunden.

(Man überlegt sich leicht, daß U k-dimensional ist.) Dieses Ergebnis müssen wir jetzt nur bezüglich V und Φ ausdrücken.

Eigentlich wollten wir aber einen nicht-trivialen Φ - invarianten Unterraum von V finden.

Die Beziehung zwischen V und K^n und Φ und A läßt sich über das folgende kommutative Diagramm ausdrücken: $\begin{array}{ccc} V & \stackrel{\Phi}{\rightarrow} & V \\ \uparrow X & & \uparrow X \\ K^n & \stackrel{A}{\rightarrow} & K^n \end{array}$. Dabei ist X der Isomorphismus, der die kanonische Basis $e_1,\ldots,e_n$ von K^n auf die Basis $u_1,\ldots,u_n$ von V abbildet. Weil nun der oben konstruierte Unterraum $U \subset K^n$ invariant unter A ist und weil $\Phi \circ X = X \circ A$, folgt sofort, daß der Unterraum $W := X(U) \subset V$ invariant unter Φ ist, denn $\Phi(W) = \Phi(X^{-1}(U)) = X(A(U)) \subset X(U) = W$.