Poly_Smith_neu.mws 12. Juni 2003

Beispiel zur Berechnung der Smith-Form von Polynom-Matrizen.

```
> restart:
> with(linalg):
Warning, the protected names norm and trace have been redefined and
unprotected
```

Definition der Elementarmatrizen als Prozeduren, n gibt die Zeilenanzahl (=Spaltenanzahl) an:

```
> P:=proc(n,i,j) local k;swaprow(diag(seq(1,k=1..n)),i,j);end:
> S:=proc(n,i,l) local k; evalm(mulrow(diag(seq(1,k=1..n)),i,l));end:
> Q:=proc(n,i,j,l) local k; evalm(addrow(diag(seq(1,k=1..n)),i,j,l));end:
```

Festlegung der Matrix:

```
> p:=3: (Festlegung des Koeffizientenkörpers)
M := map(modp,matrix([[x^2-1, x^3+3*x^2-x-3, x^3-3*x^2-x+3], [x^3+3*x^2-x-3, -x^4-x^3-4*x^2-5*x-1, -x^3-x^2-x-1], [x^3+x^2-x-1, x^6+8*x^5+23*x^4+21*x^3-7*x^2-23*x-11, x^5+9*x^4+32*x^3+52*x^2+41*x+13]]),p);
```

$$M := \begin{bmatrix} x^2+2 & x^3+2\,x & x^3+2\,x \\ x^3+2\,x & 2\,x^4+2\,x^3+2\,x^2+x+2 & 2\,x^3+2\,x^2+2\,x+2 \\ x^3+x^2+2\,x+2 & x^6+2\,x^5+2\,x^4+2\,x^2+x+1 & x^5+2\,x^3+x^2+2\,x+1 \end{bmatrix}$$

Abkürzung der stets notwendigen Operationen "Reduzieren modulo p" und "entwickeln nach Potenzen " :

```
> RE:=X->map(sort,map(modp,map(expand,evalm(X)),p));
```

$$RE := X \to \mathrm{map}(\mathit{sort}, \mathrm{map}(\mathit{modp}, \mathrm{map}(\mathit{expand}, \mathrm{evalm}(X)), p))$$

Im <u>ersten Schritt</u> **werden durch elementare Zeilen/Spalten-Umformungen die Einträge modulo M[1,1] reduziert:**

```
> M1:=RE(Q(3,1,2,-quo(M[2,1],M[1,1],x)) &* M);

U:=Q(3,1,2,-quo(M[2,1],M[1,1],x)):
```

$$M1 := \begin{bmatrix} x^2+2 & x^3+2\,x & x^3+2\,x \\ 0 & x^4+2\,x^3+x+2 & 2\,x^4+2\,x^3+2\,x+2 \\ x^3+x^2+2\,x+2 & x^6+2\,x^5+2\,x^4+2\,x^2+x+1 & x^5+2\,x^3+x^2+2\,x+1 \end{bmatrix}$$

```
> M2:=RE(Q(3,1,3,-quo(M1[3,1],M1[1,1],x)) &* M1);

U:=RE(Q(3,1,3,-quo(M1[3,1],M1[1,1],x)) &* U):
```

$$M2 := \begin{bmatrix} x^2+2 & x^3+2\,x & x^3+2\,x \\ 0 & x^4+2\,x^3+x+2 & 2\,x^4+2\,x^3+2\,x+2 \\ 0 & x^6+2\,x^5+x^4+2\,x^3+2\,x+1 & x^5+2\,x^4+x^3+2\,x^2+1 \end{bmatrix}$$

```
> M3:=RE(M2 &* Q(3,2,1,-quo(M2[1,2],M2[1,1],x)));

V:=Q(3,2,1,-quo(M2[1,2],M2[1,1],x)):
```

$$M3 := \begin{bmatrix} x^2+2 & 0 & x^3+2\,x \\ 0 & x^4+2\,x^3+x+2 & 2\,x^4+2\,x^3+2\,x+2 \\ 0 & x^6+2\,x^5+x^4+2\,x^3+2\,x+1 & x^5+2\,x^4+x^3+2\,x^2+1 \end{bmatrix}$$

```
> M4:=RE(M3 &* Q(3,3,1,-quo(M3[1,3],M3[1,1],x)));
V:=RE(V&*Q(3,3,1,-quo(M3[1,3],M3[1,1],x))):
```

$$M4 := \begin{bmatrix} x^2+2 & 0 & 0 \\ 0 & x^4+2x^3+x+2 & 2x^4+2x^3+2x+2 \\ 0 & x^6+2x^5+x^4+2x^3+2x+1 & x^5+2x^4+x^3+2x^2+1 \end{bmatrix}$$

Es lagen (untypischerweise) in der ersten Zeile und in der ersten Spalte nurVielfache von x^2+2 vor. Schön, aber teilt nun der (1,1)-Eintrag auch alle übrigen Einträge von M4 ??

Ich berechne die Divisionsreste:

```
> RE(map(u->rem(u,M4[1,1],x),M4));
```

$$\begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & x+1 \\ 0 & 0 & 2x+2 \end{bmatrix}$$

Entsprechend addiere ich bei M4 die zweite Zeile zur ersten. Dadurch wandert der (2,3)-Eintrag von M4 in die (1,3)-Position:

```
> M5:=RE(Q(3,2,1,1)&*M4);
U:=RE(Q(3,2,1,1)&*U):
```

$$M5 := \begin{bmatrix} x^2+2 & x^4+2x^3+x+2 & 2x^4+2x^3+2x+2 \\ 0 & x^4+2x^3+x+2 & 2x^4+2x^3+2x+2 \\ 0 & x^6+2x^5+x^4+2x^3+2x+1 & x^5+2x^4+x^3+2x^2+1 \end{bmatrix}$$

Nun wird wie im ersten Schritt weiterverfahren:

```
> M6:=RE(M5&*Q(3,2,1,-quo(M5[1,2],M5[1,1],x))&*Q(3,3,1,-quo(M5[1,3],M5[1,1],x)));
V:=RE(V&*Q(3,2,1,-quo(M5[1,2],M5[1,1],x))&*Q(3,3,1,-quo(M5[1,3],M5[1,1],x))):
```

$$M6 := \begin{bmatrix} x^2+2 & 0 & x+1 \\ 0 & x^4+2x^3+x+2 & 2x^4+2x^3+2x+2 \\ 0 & x^6+2x^5+x^4+2x^3+2x+1 & x^5+2x^4+x^3+2x^2+1 \end{bmatrix}$$

Nun müssen 1. und 3. Spalte vertauscht werden:

```
> M7:=RE(M6&*P(3,1,3));
V:=RE(V&*P(3,1,3)):
```

$$M7 := \begin{bmatrix} x+1 & 0 & x^2+2 \\ 2x^4+2x^3+2x+2 & x^4+2x^3+x+2 & 0 \\ x^5+2x^4+x^3+2x^2+1 & x^6+2x^5+x^4+2x^3+2x+1 & 0 \end{bmatrix}$$

.

.. weiter, wie im ersten Schritt:

```
> M8:=RE(Q(3,1,3,-quo(M7[3,1],M7[1,1],x))&*Q(3,1,2,-quo(M7[2,1],M7[1,1],x))&*M7);
U:=RE(Q(3,1,3,-quo(M7[3,1],M7[1,1],x))&*Q(3,1,2,-quo(M7[2,1],M7[1,1],x))&*U):
```

$$M8 := \begin{bmatrix} x+1 & 0 & x^2+2 \\ 0 & x^4+2x^3+x+2 & x^5+2x^3+x^2+2 \\ 0 & x^6+2x^5+x^4+2x^3+2x+1 & 2x^6+2x^5+x^4+2x^3+2x^2+2x+1 \end{bmatrix}$$

```
> M9:=RE(M8&*Q(3,3,1,-quo(M8[1,3],M8[1,1],x)));
V:=RE(V&*Q(3,3,1,-quo(M8[1,3],M8[1,1],x))):
```

$$M9 := \begin{bmatrix} x+1 & 0 & 0 \\ 0 & x^4+2x^3+x+2 & x^5+2x^3+x^2+2 \\ 0 & x^6+2x^5+x^4+2x^3+2x+1 & 2x^6+2x^5+x^4+2x^3+2x^2+2x+1 \end{bmatrix}$$

Teilt jetzt der (1,1)-Eintrag von M9 auch alle übrigen Einträge von M9 ??

Ich berechne die Divisionsreste:

```
> RE(map(u->rem(u,M9[1,1],x),M9));
```

$$\begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

ja !

Nun kann mit der folgenden Teilmatix weitergearbeitet werden:

```
> B:=submatrix(M9,2..3,2..3);
```

$$B := \begin{bmatrix} x^4+2x^3+x+2 & x^5+2x^3+x^2+2 \\ x^6+2x^5+x^4+2x^3+2x+1 & 2x^6+2x^5+x^4+2x^3+2x^2+2x+1 \end{bmatrix}$$

Mit B wird genauso verfahren:

```
> B1:=RE(Q(2,1,2,-quo(B[2,1],B[1,1],x))&*B);
U:=RE(diag(1,Q(2,1,2,-quo(B[2,1],B[1,1],x)))&*U):
```

$$B1 := \begin{bmatrix} x^4+2x^3+x+2 & x^5+2x^3+x^2+2 \\ 2x^3+x^2+x+2 & 2x^7+2x^6+2x^5+2x^2+2x+2 \end{bmatrix}$$

```
> B2:=RE(P(2,1,2)&*B1);
U:=RE(diag(1,P(2,1,2))&*U):
```

$$B2 := \begin{bmatrix} 2x^3+x^2+x+2 & 2x^7+2x^6+2x^5+2x^2+2x+2 \\ x^4+2x^3+x+2 & x^5+2x^3+x^2+2 \end{bmatrix}$$

```
> B3:=RE(Q(2,1,2,-quo(B2[2,1],B2[1,1],x))&*B2);
U:=RE(diag(1,Q(2,1,2,-quo(B2[2,1],B2[1,1],x)))&*U):
```

$$B3 := \begin{bmatrix} 2x^3+x^2+x+2 & 2x^7+2x^6+2x^5+2x^2+2x+2 \\ x^2+2 & 2x^8+2x^7+2x^6+x^5+x^3+2x+2 \end{bmatrix}$$

```
> B4:=RE(P(2,1,2)&*B3);
U:=RE(diag(1,P(2,1,2))&*U):
```

$$B4 := \begin{bmatrix} x^2+2 & 2x^8+2x^7+2x^6+x^5+x^3+2x+2 \\ 2x^3+x^2+x+2 & 2x^7+2x^6+2x^5+2x^2+2x+2 \end{bmatrix}$$

```
> B5:=RE(Q(2,1,2,-quo(B4[2,1],B4[1,1],x))&*B4);
U:=RE(diag(1,Q(2,1,2,-quo(B4[2,1],B4[1,1],x)))&*U):
```

$$B5 := \begin{bmatrix} x^2+2 & 2x^8+2x^7+2x^6+x^5+x^3+2x+2 \\ 0 & 2x^9+2x^7+x^6+x^5+x^4+2x^3+x^2+2x \end{bmatrix}$$

```
> B6:=RE(B5&*Q(2,2,1,-quo(B5[1,2],B5[1,1],x)));

V:=RE(V&*diag(1,Q(2,2,1,-quo(B5[1,2],B5[1,1],x)))):
```

$$B6 := \begin{bmatrix} x^2+2 & 0 \\ 0 & 2\,x^9+2\,x^7+x^6+x^5+x^4+2\,x^3+x^2+2\,x \end{bmatrix}$$

Wir haben Glück und sind bereits so gut wie am Ziel. Nur noch eine Normierung ist vorzunehmen, um Eindeutigkeit zu erreichen:

```
> B7:=RE(S(2,2,2)&*B6);

U:=RE(diag(1,S(2,2,2))&*U):
```

$$B7 := \begin{bmatrix} x^2+2 & 0 \\ 0 & x^9+x^7+2\,x^6+2\,x^5+2\,x^4+x^3+2\,x^2+x \end{bmatrix}$$

Die Smithform von A latet nun:

```
> `Smithform von M`= diag(M9[1,1],B7);
```

$$\mathit{Smithform\ von\ M} = \begin{bmatrix} x+1 & 0 & 0 \\ 0 & x^2+2 & 0 \\ 0 & 0 & x^9+x^7+2\,x^6+2\,x^5+2\,x^4+x^3+2\,x^2+x \end{bmatrix}$$

Zum Vergleich das Ergebnis von Maple:

```
> Smith(M,x) mod p;
```

$$\begin{bmatrix} x+1 & 0 & 0 \\ 0 & x^2+2 & 0 \\ 0 & 0 & x^9+x^7+2\,x^6+2\,x^5+2\,x^4+x^3+2\,x^2+x \end{bmatrix}$$

In Anwendungen ist es häufig notwendig, <u>nicht nur die Smithform</u>**, sondern** <u>auch die Transformationsmatrizen</u> **zu kennen. In unserem Falle sind dies die unterwegs neben der Rechnung her erzeugten Matrizen U und V.**

Die Probe bestätigt dies:

```
> RE(U&*M&*V);
```

$$\begin{bmatrix} x+1 & 0 & 0 \\ 0 & x^2+2 & 0 \\ 0 & 0 & x^9+x^7+2\,x^6+2\,x^5+2\,x^4+x^3+2\,x^2+x \end{bmatrix}$$

.