FFC 21.4.08

Satz von McCoy

Zutaten: 1) Isomorphismus $M_n(R[x]) \simeq (M_n(R))[x]$ (R komm Ring)

via $\left(\sum_{k\geq 0} a_{ij}^{(k)} x^k\right)_{\substack{1\leq i\leq n\\ 1\leq j\leq n}} \mapsto \sum_{k\geq 0} \left(a_{ij}^{(k)}\right)_{\substack{1\leq i\leq n\\ 1\leq j\leq n}} x^k$

Die Elemente in $R[x]$ sind jeweils eingebettet:

$g \in R[x]$ in $M_n(R[x])$ als „Skalarmatrix" $g(x)\cdot I = \begin{pmatrix} g(x) & & \\ & \ddots & \\ & & g(x) \end{pmatrix}$

$\sum_k a_k x^k$ in $(M_n(R))[x]$ $\quad g(x) = a_0 I + a_1 I x + \dots + a_n I x^n = \begin{pmatrix} a_0 & & \\ & \ddots & \\ & & a_0 \end{pmatrix} + \begin{pmatrix} a_1 & & \\ & \ddots & \\ & & a_1 \end{pmatrix} x + \dots + \begin{pmatrix} a_n & & \\ & \ddots & \\ & & a_n \end{pmatrix} x^n$

Bem: S komm Ring, dann Zentrum (Menge der El, die mit allen El. kommutieren) von $M_n(S)$ ist S eingebettet als Menge der Skalarmatrizen $\{sI \mid s \in S\}$.

2) Zusammenhang (Äquivalenz)

Linearfaktoren - Nullstellen eines Polynoms:

der Zusammenhang gilt auch für nichtkomm. Koeffizientenring (ev. mit Nullteilern).

S Ring mit 1 $\quad g \in S[x]$ $\quad g = \sum_k a_k x^k$, $s \in S$, dann

$\sum_k a_k s^k \Leftrightarrow \exists h \in S[x] \quad g(x) = h(x)(x-s)$ ← Linearfaktor re.

$\sum_k s^k a_k \Leftrightarrow \exists l \in S[x] \quad g(x) = (x-s)\, l(x)$ ← Linearfaktor li.

3) Adjungierte einer Matrix

R komm Ring $A \in M_n(R)$, dann $\exists B \in M_n(R)$, $B = \mathrm{adj}(A)$

sd. $A \cdot B = B \cdot A = (\det A) I = \begin{pmatrix} \det A & & 0 \\ & \ddots & \\ 0 & & \det A \end{pmatrix}$

Nämlich: $B = \left((-1)^{i+j} \det A_j^i\right)_{\substack{1\leq i\leq n\\ 1\leq j\leq n}}$ wobei A_j^i die aus A durch Streichen der i-ten Spalte und j-ten Zeile hervorgehende Matrix bezeichnet.

Bem: Die Einträge der Adjungierten sind bis auf Vorzeichen die $(n-1)\times(n-1)$ Minoren von A.

Def: $A \in M_n(R)$ Ein $k\times k$ Minor von A ist die Determinante einer $k\times k$ Untermatrix von A. (eine Matrix die durch Streichen von $n-k$ Zeilen u. Spalten aus A hervorgeht.)

Spezialfall der Satzes von McCoy: Cayley-Hamilton

$A \in M_n(R)$, $\chi(x) = \det(xI - A)$ dann $\chi(A) = 0$.

Bew: $B = \operatorname{adj}(x \cdot I - A)$; $B(xI - A) = \chi(x) \cdot I$ in $M_n(R[x])$

$B(x - A) = \chi(x)$ in $(M_n(R))[x]$

$\Rightarrow \chi(A) = 0$ $\square$

Zusätzliche Notation: S komm Ring: $A \in M_n(S)$, $F_k(A)$ = das von den $k \times k$ Minoren von A erzeugte Ideal von S

$F_1(A) \supseteq F_2(A) \supseteq \ldots \supseteq F_{n-1}(A) \supseteq F_n(A)$

F_1 ist das von den Eintragungen von A erz. Ideal von S;

F_n ist das von $\det A$ erz. Hauptideal von S, $F_n(A) = (\det(A) \cdot S)$

II: „Idealquotient" $(I :_K J) = \{k \in K \mid \forall j \in J \; kj \in I\}$

wann auch das Sinn hat. Insb. wenn K Ring I, J K-Moduln enthalten in K-Modul $L \supseteq I, J$

Bem: die Eintragungen der Adjungierten von A erzeugen $F_{n-1}(A)$

Def: R komm Ring mit 1, $(M,+)$ komm Gruppe

$(M,+)$ ist R-Modul, wenn Skalarmult

$\cdot \; R \times M \to M$ def, sodass

1) $r(m+n) = rm + rn$ $\forall r \in R$ $\forall m, n \in M$

2) $(r \cdot s)m = r(sm)$ $\forall r, s \in R$, $m \in M$

3) $(r+s)m = rm + sm$ ---

„unitärer Modul" zus 4) $1_R m = m$ $\forall m \in M$

Bem: jeder R-Modul M ist direkte Summe $M = M_0 \oplus M_1$; M_1 unitär

M_0 hat 0-Mult, d.h. $\forall r \in R \; \forall m \in M_0 \; rm = 0$

Bem: wenn M ein R-Modul dann $\operatorname{Ann}_R M := \{r \in R \mid \forall m \in M : rm = 0\}$

Ideal $\trianglelefteq R$. M heißt treuer R-Modul, wenn $\operatorname{Ann}_R M = \{0\}_R$

Def: R komm Rg mit 1, $(M,+,\cdot)$ Rg mit 1 (ev. n. komm)
dann heißt M eine R-Algebra, wenn M ein R-Modul und
sich Mult im Rg M und Skalarmult $\cdot\; R\times M\to M$ vertragen wie folgt:
$r(mn)=(rm)n=m(rn)$ $\forall\, m,n\in M,\ r\in R$.

Bem: $R\subseteq S$ R komm Rg, S Rg $\Rightarrow S$ ist treue R-Algebra
(durch Einschränkung der Mult $S\times S\to S$ auf $R\times S\to S$)
jede treue R-Algebra von dieser Form: M treue R-Algebra, dann
R isomorph eingebettet in M durch $r\mapsto r\cdot 1_M$ und Skalarmult mit
$r\in R$ ist dasselbe wie Mult in M mit $(r\cdot 1_M)$

Satz von McCoy: R komm Rg mit 1 $A\in M_n(R)$ ~~für~~
Sei $N_A:=\{f\in R[x]\mid f(A)=0\}$, sei $C=xI-A$
$N_A=(F_n(C)\ \underset{R[x]}{:}\ F_{n-1}(C))$.

Bew: ang. $g\in R[x]$ ist in $(F_n:F_{n-1})$. Das ist äquivalent zu: für ein
Erzeugendensyst E des Ideals $F_{n-1}(C)$: $\forall e\in E$ $g\cdot e\in \chi(x)\cdot R[x]$
insb. äquivalent zu: für $B=\operatorname{adj}(C)$ gilt: $\exists D\in M_n(R[x])$: $g(x)\cdot B=\chi(x)\cdot D$
Mult mit $C=xI-A$ (kein Nullteiler in $M_n(R[x])$, also kürzbar) ergibt
äquivalente Aussage: $g(x)\chi(x)=\chi(x)\cdot D(xI-A)$ bzw
$\chi(x)g(x)=\chi(x)\,D(xI-A)$ [$\chi(x)$ in Zentrum von $M_n(R[x])$]
Kürze von $\chi(x)$ [kein Nullteiler, kürzbar!] ergibt äquivalente
Aussage: $g(x)=D(xI-A)$ für ein $D\in M_n(R[x])$ in $(M_n(R))[x]$
$g(x)=D(x-A)$ für ein $D\in(M_n(R))[x]$ äquivalent zu: $g(A)=0$

Bem: haben verwendet: im Polynomring $S[x]$ (S Rg mit 1) sind normierte
Polynome (Leitkoeff $=1$) kürzbar, da sicher kein Nullteiler
(Nullteiler im Polynomring haben als Leitkoeff Nullteiler in S)

Kor: R komm Rg mit 1, $f \in R[x]$ f normiert, A die Gefährtenmatrix von f, d.h. $A = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ \vdots & & \ddots & \ddots & \vdots \\ 0 & & & 0 & 1 \\ -a_0 & \cdots & & & -a_{n-1} \end{pmatrix}$ dann ist $N_A = f(x)\, R[x]$

(d.h. $\forall g \in R[x]: g(A) = 0 \iff f \mid g$ in $R[x]$)

$$C = xI - A = \begin{pmatrix} x & -1 & 0 & \cdots & 0 \\ & \ddots & \ddots & & \vdots \\ 0 & & & x & -1 \\ a_0 & & & & (x+a_{n-1}) \end{pmatrix}$$

$F_{n-1}(C) = R[x]$ da ± 1 als $(n-1) \times (n-1)$ Minor auftritt (bei Streichung von letzter Zeile und erster Spalte) $N_A = (\chi(x) R[x] : R[x]) = \chi(x)\, R[x]$ und $\chi(x) = f(x)$ (det $(x-A)$, A Gefährtenm. von f, ist f).

Damit bekommt man eine Matrixdarstellung einer einfachen alg. Erweiterung von R (R kom Rg mit 1) Nämlich: R ~~kommutativ mit 1~~ Körper $\subseteq S$ Rg $s \in S$ fix u. alg. ü. R

$R[s]$ oder von $R \cup \{s\}$ erz. Unterring von S besteht genau aus den Ausdrücken $a_0 + a_1 s + \dots + a_n s^n$ f. $n \in \mathbb{N}$ $s \in S$, $a_i \in R$.

daher Einsetzhom $\varphi: R[x] \to S$ mit $\varphi(x) = s$

$\varphi|_R = id_R$ surjektiv auf $R[s]$, $\ker \varphi = \{f \in R[x] \mid f(s) = 0\} \neq \{0\}$

daher nach 1. Isosatz $R[x]/_{\ker \varphi} \simeq R[x]$

wobei $\ker \varphi$ Hauptideal $= f(x) \cdot R[x]$. Erhalte Isomorphismus zu dem von R und A_f (der Gefährtenmatrix auf f) erzeugt Unterring in $M_n(R)$ $n = \deg f$

$$R[s] \simeq R[x]/(f) \simeq R[A_f] \qquad s \longleftarrow\!\shortmid (x+f) \longmapsto A_f$$
$$r \longleftarrow\!\shortmid (r+f) \longmapsto rI$$

In jedem Fall Einsetzhom mit $x \mapsto s$ bzw. $x \mapsto A_f$ und Einschränkung auf R gleich id_R ist Epimorph mit $\ker = (f)$ zugehörige $\bar{\varphi}$

(1. Isosatz ergibt Isomorphismus)

Bsp: $\mathbb{C} = \mathbb{R}[i]$ als Rg von 2x2 Matrizen über $\mathbb{R}$. Minimalpolynom von i in $\mathbb{R}[x]$ ist $f = x^2+1$ $A_f = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. Jede Matrix in $\mathbb{R}[A_f]$ lässt sich, da $A_f^2 = -1$ darstellen als Polynom von Grad ≤ 1 in $\mathbb{R}[x]$ mit A_f eingesetzt:

$$a \cdot \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + b \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \underset{\text{Isom.}}{\iff} a + bi$$