Computational Commutative Algebra 1 – Lecture Notes

2004-04-20

- Einheiten sind nichts anderes als die Elemente, die invertierbar sind.
- Anmerkung zur Definition 'irreduzibel':
  - Hier wird nur $R\setminus(\{0\}\cup R^\times)$ statt $R\setminus(\{0\})$ betrachtet, weil die Irreduziblität von Einheiten (diese werden ja von der Definition ausgenommen) nicht interessiert.
  - Betrachte den Polynomring $R[x]$ über den reellen Zahlen. Man will sagen, das Polynome wie '$x+1$' irreduzibel sind (Es gibt zwar die Zerlegung $x+1=\frac{1}{2}(2x+2)$, aber '$\frac{1}{2}$' ist eine Einheit.), aber nicht, dass Polyome wie '2' (also konstante Polynome) irreduzibel sind.
- Ein Modul für einen Ring ist das Analogen zu einem Vektorraum zu einem Körper (gleiche Axiome).
- Ein Ideal unterscheidet sich von einem Unterring darin, dass sogar $R\cdot I\subseteq I$ statt nur $I\cdot I\subseteq I$ gefordert wird.
- Beispiel für ein Ideal, das kein Primideal ist:
  - $R=Z$; $I=\{4,8,12,\ldots\}$; $r=12\in I$; $r=r_1r_2=2\cdot 6$
  - Es müsste folgen $2\in I\vee 6\in I$, stimmt aber nicht.

2004-04-27

- Eine R-Algebra S ist ein Ring, der zugleich R-Modul ist, wenn man als Skalarprodukt $R\times S\to S$ mit $(r,s)\mapsto\varphi(r)\cdot s$ wählt.
- Eine R-Algebra S heißt 'endlich erzeugt', wenn es $\{s_1,\ldots,s_n\}\in S$ gibt, so dass die Potenzprodukte $s_1^{\alpha_1}\ldots s_n^{\alpha_n}$ mit $\alpha_i\geq 0$ S als R-Modul erzeugen.
  - bedeutet: Jedes $s\in S$ lässt sich als Linearkombination von verschiedenen $s_1^{\alpha_1}\ldots s_n^{\alpha_n}$ schreiben, also $s=\sum_{i\geq 1}\lambda_i\cdot s_1^{\alpha_{1.i}}\ldots s_n^{\alpha_{n.i}}$ bzw. $s=\sum_{i\geq 1}c_{1.i}\ldots c_{n.i}\cdot s_1^{\alpha_{1.i}}\ldots s_n^{\alpha_{n.i}}$.
  - Bezug zur Realität: Oft betrachtet man Polynomringe, welche ja R-Algebren sind. Der Polynomring wird 'erzeugt' durch die Potenzprodukte $x_1^{\alpha_1}\ldots x_n^{\alpha_n}$ mit $\alpha_i\geq 0$, weil sich ja jedes Polynom schreiben lässt als $p(x)=\sum_{i\geq 1}c_{1.i}\ldots c_{n.i}\cdot x_1^{\alpha_{1.i}}\ldots x_n^{\alpha_{n.i}}$. Da es nun nach der universellen Eigenschaft genau einen Ringhomomorphismus $R[x_1,\ldots,x_n]\to S$ (mit u. a. der Eigenschaft $\psi(x_i)=s_i$) gibt, entsprechen sich $p(x)=\sum_{i\geq 1}c_{1.i}\ldots c_{n.i}\cdot x_1^{\alpha_{1.i}}\ldots x_n^{\alpha_{n.i}}$ und $s=\sum_{i\geq 1}c_{1.i}\ldots c_{n.i}\cdot s_1^{\alpha_{1.i}}\ldots s_n^{\alpha_{n.i}}$.
  - Siehe auch Definition 1.1.13 im Buch.
- Bei '$S\cong R[x_1,\ldots,x_n]/I$' steht nichts anderes, als dass das Bild (hier: S) isomorph zum

Ganzen (hier: $R[x_1,\ldots,x_n]$) ohne den Kern (hier: I) ist.

2004-04-29

- Spezielle Ringelemente im Polynomring:
  - Einheiten: $P^\times = \left\{ \sum_{(i_1,\ldots,i_n)\in\mathbb{N}_0^n} c_{(i_1,\ldots,i_n)} \cdot x_1^{i_1} \ldots x_1^{i_n} \middle| c_{(0,\ldots,0)} \in R^\times \wedge \text{alle anderen } c_{(i_1,\ldots,i_n)} \text{ nilpotent} \right\}$:
    - siehe Tafelbild 'University; Computational Commutative Algebra 1 (Algebra 2); SS 2004; 2004-05-06; 13-20'
- R Ring, $r \in R$: r Primelement $\Rightarrow$ r irreduzibel:
  - r prime: $r \mid r_1 r_2 \Rightarrow r \mid r_1 \vee r \mid r_2$
  - r irreduzibel: $r \neq r_1 r_2$
  - Angenommen, r prime und nicht r irreduzibel (also r reduzibel): $\underbrace{r = r_1 r_2}_{\text{da reduzibel}} \wedge \underbrace{\left(r \mid r_1 \vee r \mid r_2\right)}_{\text{da prime}}$
  - r_1 und r_2 sind 'kleiner' als r, weil r ja das Produkt der beiden ist. Da r aber auch prime ist, gilt aber auch $r \mid r_1 \vee r \mid r_2$. Also muss r_1 oder r_2 'größer' als r sein ('8' kann nicht '6' teilen, sondern frühestens '8'.). Dann muss aber r 'gleich' r_1 xoder r_2 sein ('Größer' als '8' kann weder r_1 noch r_2 sein, denn $8 = r_1 r_2$. Also muss $r_1 = 8$ xor $r_2 = 8$ und das jeweils andere muss gleich 1 sein ('1' ist jedoch eine Einheit.). Bei Polynomen bedeutet das, dass r_1 xoder r_2 den gleichen Grad wie r haben muss und das jeweils andere eine Zahl sein muss (eigentlich auch immer eine Einheit).).
  - Also ist r doch nicht reduzibel. Widerspruch.
  - siehe Tafelbild 'University; Computational Commutative Algebra 1 (Algebra 2); SS 2004; 2004-05-06; 12-20'

2004-05-25

- Die minimale Erzeugendenzahl von $I = (x_1,\ldots,x_n)^2$ ist $\frac{n(n+1)}{2}$ weil: Man überzeugt sich durch Nachdenken, dass $\left\{ \underbrace{x_1x_1, x_1x_2, \ldots, x_1x_n}_{n \text{ Stück}}, \underbrace{x_2x_2, x_2x_3, \ldots, x_2x_n}_{n-1 \text{ Stück}}, \ldots, \underbrace{x_nx_n}_{1 \text{ Stück}} \right\}$ ein minimales Erzeugendensystem für I ist. Die Anzahl der Elemente ist die Summe der ersten n natürlichen Zahlen. Nach Gauß ist das $\frac{n(n+1)}{2}$.
- Ergänzung zu Tafelbild 'University; Computational Commutative Algebra 1 (Algebra 2); SS 2004; 2004-05-25; 08-14':
  - M wird disjunkt zerlegt in homogene Komponenten vom Grad 0 und 1 – andere gibt es nicht –, nämlich $M = M_0 \oplus M_1$.
  - Die Herleitung des minimalen Erzeugendensystems für M_0 dürfte klar sein.
  - Für das minimale Erzeugendensystem für M_1 wird Nakayama's Lemma verwendet. Dazu wird von M zu $M / P_+ M$ übergegangen. Uns interessiert nur noch die homogene Komponente vom Grad 1 von M (d. h. M_1). Also interessiert uns die homogene

Komponente vom Grad 1 von M/P_+M, also $(M/P_+M)_1$. Es gilt (siehe 1.7.9 im Buch): $(M/P_+M)_1 = M_1/(P_+M)_1$.

- $(P_+M)_1$ sind Monome n vom Grad 1, die sich als Produkt von 2 Monomen schreiben lassen ($n = pm$). Dazu muss $\deg(p)=0 \wedge \deg(m)=1 \vee \deg(p)=1 \wedge \deg(m)=0$ sein. Doch da p aus P_+ kommt, hat p mindestens Grad 1 und somit bleibt nur noch $\deg(p)=1 \wedge \deg(m)=0$ übrig. Dies entspricht also P_1M_0. Mit anderen Worten: $(P_+M)_1 = P_1M_0$.
- Insgesamt kriegt man also $(M/P_+M)_1 = M_1/P_1M_0$.

- Ergänzung zu Tafelbild 'University; Computational Commutative Algebra 1 (Algebra 2); SS 2004; 2004-05-25; 14-14.jpg':
  - Es gilt $t \cdot LT(f_i) = LT\left(\left(\tilde{h}_i + \frac{LC(f)}{LC(f_i)}t\right)f_i\right)$, denn:

$$LT\left(\left(\tilde{h}_i + \frac{LC(f)}{LC(f_i)}t\right)f_i\right) = LT\left(\tilde{h}_i f_i + \frac{LC(f)}{LC(f_i)}tf_i\right) = \max\left\{LT\left(\tilde{h}_i f_i\right), LT(tf_i)\right\}$$

$$= \max\left\{LT\left(\tilde{h}_i f_i\right), t \cdot LT(f_i)\right\} = t \cdot LT(f_i)$$

weil $\underbrace{LT(f)}_{=t\cdot LT(f_i)} > LT\left(\tilde{h}_i f_i\right)$ für alle f_i, als ins Besondere für dieses f_i mit $t \cdot LT(f_i) = LT(f)$

2004-06-03

- Ergänzung zu Tafelbild 'University; Computational Commutative Algebra 1 (Algebra 2); SS 2004; 2004-06-03; 03-29':
  - $g_1 = y\tilde{g}_1$ und $g_2 = x\tilde{g}_2$, weil:
    - $g_1 x = -g_2 y$
    - Weil die rechte Seite durch x teilbar ist, muss es auch die linke sein.
    - Weil y nicht durch x teilbar ist (klar), muss zwangsläufig g_2 durch x teilbar sein.
    - Analoges gilt für y.
    - also: $g_1 = y\tilde{g}_1$ und $g_2 = x\tilde{g}_2$
  - $\tilde{g}_1 = -\tilde{g}_2$, weil: $g_1 x = -g_2 y \Leftrightarrow y\tilde{g}_1 x = -x\tilde{g}_2 y \Leftrightarrow \tilde{g}_1 = -\tilde{g}_2$
- Ergänzung zu Tafelbild 'University; Computational Commutative Algebra 1 (Algebra 2); SS 2004; 2004-06-03; 07-29' und folgende:
  - Für jedes feste Monom $t \in T^n$ muss der Koeffizient von t 0 ergeben, denn:
    - Muliplizierе $g_1 t_1 + \ldots + g_s t_s = 0$ vollkommen aus und fasse gleiche Terme wie üblich zusammen, wodurch sich ihre Koeffzienten addieren.
    - Mit t sind diese Terme gemeint.
    - Da jeder Term t nur einmal in der sich ergebenden Summe aus Termen auftaucht, kann er sich nicht mit einem anderen wegkürzen.
    - Da die Summe immer noch 0 ergibt, muss vor allen Termen der Koeffizient 0 stehen.
  - In der Darstellung $g_i = \sum_j c_{ij} m_j$ sind mit m_j die Terme in $\mathrm{Supp}(g_i)$ gemeint. Also sind die m_j-s von einem g_i nicht die gleichen wie von einem anderen. Auch das j ist bei jedem g_i ein anderes.

- Es folgt '$c_{1j_1} m_{j_1} t_1 + \ldots + c_{1j_s} m_{j_s} t_s = 0$', weil:
  - $c_{1j_1} \underbrace{m_{j_1} t_1}_{=t} + \ldots + c_{1j_s} \underbrace{m_{j_s} t_s}_{=t} = 0 \Leftrightarrow (c_{1j_1} + \ldots + c_{1j_s}) t = 0 \Leftrightarrow c_{1j_1} + \ldots + c_{1j_s} = 0$
  - Letzteres wurde ja bereits festgestellt.
  - Also ist auch $(c_{1j_1} m_{j_1}, \ldots, c_{sj_s} m_{j_s})$ eine Syzygie von $(t_1, \ldots, t_s)$.
- $(m_{j_1}, -m_{j_2}) \in \mathrm{Syz}(t_1, t_2)$, weil:
  $m_{j_1} t_1 = m_{j_2} t_2 \Leftrightarrow m_{j_1} t_1 + (-m_{j_2}) t_2 = 0 \underbrace{\Leftrightarrow}_{\text{nach Definition}} (m_{j_1}, -m_{j_2}) \in \mathrm{Syz}(t_1, t_2)$
- Da $\mathrm{Syz}(t_1, t_2) \underbrace{=}_{\text{siehe Tafelbild 'University; Computational Commutative Algebra 1 (Algebra 2); SS 2004; 2004-06-03; 05-29'}} \langle \sigma_{12} \rangle$,
  muss nun $(m_{j_1}, -m_{j_2})$ ein Vielfaches von $\langle \sigma_{12} \rangle$ sein, also $(m_{j_1}, -m_{j_2}) = h\sigma_{12}$.
- $c_{1j_1} h(t_{12}, -t_{21}, 0, \ldots, 0)$ ist nichts anderes als $(c_{1j_1} m_{j_1}, -c_{1j_1} m_{j_2}, 0, \ldots, 0)$. Dies ist überhaupt erstmal eine Syzygie von $(t_1, \ldots, t_n)$, weil:
  $c_{1j_1} m_{j_1} t_1 - c_{1j_1} m_{j_2} t_2 + 0 t_3 + \ldots + 0 t_s = 0$
  $\Leftrightarrow c_{1j_1} m_{j_1} t_1 - c_{1j_1} m_{j_2} t_2 = 0$
  $\Leftrightarrow c_{1j_1} m_{j_1} t_1 = c_{1j_1} m_{j_2} t_2$
  $\Leftrightarrow m_{j_1} t_1 = m_{j_2} t_2$
  (Dies ist ja der Fall (siehe oben).)
- Subtrahiert man diese Syzygie $((c_{1j_1} m_{j_1}, -c_{1j_1} m_{j_2}, 0, \ldots, 0))$ nun von der Syzygie $((c_{1j_1} m_{j_1}, \ldots, c_{sj_s} m_{j_s}))$, so erhält man eine neue (siehe Tafelbild 'University; Computational Commutative Algebra 1 (Algebra 2); SS 2004; 2004-06-03; 02-29')), und zwar $(0, (c_{2j_2} + c_{1j_1}) m_{j_2}, c_{3j_3} m_{j_3}, \ldots, c_{sj_s} m_{j_s})$ mit einem Koeffizienten $\neq 0$ weniger.
- Führt man das Verfahren fort, so kommt man nach *s* Schritten von $(c_{1j_1} m_{j_1}, \ldots, c_{sj_s} m_{j_s})$ durch Subtraktion von anderen Syzygien auf $(0, \ldots, 0)$
- also: $(c_{1j_1} m_{j_1}, \ldots, c_{sj_s} m_{j_s}) - \underbrace{(\ldots) - \ldots - (\ldots)}_{s \text{ Stück}} = (0, \ldots, 0) \Leftrightarrow (c_{1j_1} m_{j_1}, \ldots, c_{sj_s} m_{j_s}) = (\ldots) + \ldots + (\ldots)$
- Da die $(\ldots)$ alle Vielfache von mit 0-en auf die richtige Dimension gebrachte Vielfache von σ_{ij}, liegt $(c_{1j_1} m_{j_1}, \ldots, c_{sj_s} m_{j_s})$ in dem Modul, der von (ebenfalls die richtige Dimension gebrachten) σ_{ij}-s erzeugt wird.
- Die ursprüngliche Syzygie $(g_1, \ldots, g_s)$ ist Summe von $(c_{1j_1} m_{j_1}, \ldots, c_{sj_s} m_{j_s})$-s, denn die g_i-s sind ja $g_i = \sum_j c_{ij} m_j$ und weil zu jedem Term *t* in $g_1 t_1 + \ldots + g_s t_s$ eine Syzygie $(c_{1j_1} m_{j_1}, \ldots, c_{sj_s} m_{j_s})$ von $(t_1, \ldots, t_s)$ gebildet wird, was dafür sorgt, dass auch jeder Term m_j jedes g_i's genau einmal drankommt und somit:
  $(c_{1j_1} m_{j_1}, \ldots, c_{sj_s} m_{j_s})_1$
  $+ (c_{1j_1} m_{j_1}, \ldots, c_{sj_s} m_{j_s})_2$
  $+ \ldots$
  $+ \underline{(c_{1j_1} m_{j_1}, \ldots, c_{sj_s} m_{j_s})_k}$
  $= (g_1, \ldots, g_s)$
  (*k* = Anzahl der (verschiedenen) Terme *t* in $g_1 t_1 + \ldots + g_s t_s$)

- Beispiel zur λ-Funktion (Definition siehe Tafelbild 'University; Computational Commutative Algebra 1 (Algebra 2); SS 2004; 2004-06-03; 17-29'):
  - $$\lambda\left(\begin{pmatrix} f_1 \\ \vdots \\ f_s \end{pmatrix}\right) = \lambda\left(f_1 \underbrace{\begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}}_{=\varepsilon_1} + \ldots + f_s \underbrace{\begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}}_{=\varepsilon_s} \right) = \lambda\left(f_1 \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}\right) + \ldots + \lambda\left(f_s \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}\right)$$
  - $$= f_1 \cdot \lambda\begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} + \ldots + f_s \cdot \lambda\begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix} = f_1 v_1 + \ldots + f_s v_s$$
  - daher: $\text{Kern}(\lambda) = \left\{ \begin{pmatrix} f_1 \\ \vdots \\ f_s \end{pmatrix} \middle| \underbrace{\lambda\left(\begin{pmatrix} f_1 \\ \vdots \\ f_s \end{pmatrix}\right)}_{=f_1 v_1 + \ldots + f_s v_s} = 0 \right\} = \text{Syz}(v_1, \ldots, v_s)$
- $T^n\langle e_1, \ldots, e_r \rangle$-Graduierung von P^s (siehe Tafelbild 'University; Computational Commutative Algebra 1 (Algebra 2); SS 2004; 2004-06-03; 20-29'):
  - $$\deg\left(\underbrace{\begin{pmatrix} v_1 \\ \vdots \\ v_s \end{pmatrix}}_{\in P^s}\right) = \underbrace{\begin{pmatrix} 0 \\ \vdots \\ 0 \\ \underbrace{t}_{i\text{-te Stelle}} \\ 0 \\ \vdots \\ 0 \end{pmatrix}}_{\substack{=te_i \\ \in T^n\langle e_1, \ldots, e_r \rangle}} \Leftrightarrow \begin{pmatrix} v_1 \\ \vdots \\ v_s \end{pmatrix} = \underbrace{\begin{pmatrix} c_1 t_1 \\ \vdots \\ c_s t_s \end{pmatrix}}_{=\sum_{j=1}^{s} c_j t_j \varepsilon_j} \middle| \forall j : t_j \cdot LT\left(\underbrace{\begin{pmatrix} g_{j.1} \\ \vdots \\ g_{j.r} \end{pmatrix}}_{\substack{=g_j \\ \in P^r}}\right) = t_j \cdot \underbrace{\begin{pmatrix} 0 \\ \vdots \\ 0 \\ LT(g_{j.k}) \\ 0 \\ \vdots \\ 0 \end{pmatrix}}_{\text{für ein } 1 \le k \le r} = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ \underbrace{t}_{i\text{-te Stelle}} \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$
    (also falls $k = i$ ist).
  - v muss kein Mehrdimensionen-Term sein um einen Grad zu haben, darf aber auch kein Vektor von beliebigen Polynomen sein, sondern nur ein Vektor, der in jeder Komponente ($c_i t_i$) ein Monom (oder 0) stehen hat.
- Liften von Syzygien (vgl. Tafelbild 'University; Computational Commutative Algebra 1 (Algebra 2); SS 2004; 2004-06-03; 28-29'):
  - $\text{Syz}(G)$ wird berechnet wie folgt:
    1. Berechne $\text{Syz}(\text{LM}(G))$, was möglich ist, weil in $\text{LM}(G)$ ja nur Terme (mit Koeffizienten) stehen. Also setzt sich $\text{Syz}(\text{LM}(G))$ aus den fundamentalen Syzygien σ_{ij} zusammen und lässt sich, wie auf den vorherigen Tafeln gezeigt, berechnen.
    2. Sei $(f_1, \ldots, f_s) \in \text{Syz}(\text{LM}(G))$. Berechne $\lambda((f_1, \ldots, f_s))$.
    3. Ist $\lambda((f_1, \ldots, f_s)) = 0$, so ist nach Definition von λ $(f_1, \ldots, f_s)$ eine Syzygie von G.
    4. Ist $\lambda((f_1, \ldots, f_s)) \neq 0$, so gibt es für $\lambda((f_1, \ldots, f_s)) = f_1 g_1 + \ldots + f_s g_s$ eine Darstellung

$h_1 g_1 + \ldots + h_s g_s$, weil $f_1 g_1 + \ldots + f_s g_s \in G$ und weil G ein Gröbner-Basis ist.

5. Dann ist

$$\underbrace{f_1 g_1 + \ldots + f_s g_s}_{=\lambda((f_1,\ldots,f_s))} = \underbrace{h_1 g_1 + \ldots + h_s g_s}_{=\lambda((f_1,\ldots,f_s))}$$

$$\Leftrightarrow f_1 g_1 + \ldots + f_s g_s - h_1 g_1 + \ldots + h_s g_s = 0$$

$$\Leftrightarrow (f_1 - h_1) g_1 + \ldots + (f_s - h_s) g_s = 0$$

Also ist $((f_1 - h_1),\ldots,(f_s - h_s))$ eine Syzygie von G.

2004-06-08

- Hilbert's Basissatz (Tafelbild 'University; Computational Commutative Algebra 1 (Algebra 2); SS 2004; 2004-06-08; 10-18'):
  - $\mathrm{LC}(I)$ ist ein Ideal in R, weil:
    - Seien $a,b \in \mathrm{LC}(I)$. Dann muss auch $a+b$ auch in $\mathrm{LC}(I)$ liegen.:
      - Seien $a = \mathrm{LC}(f_a)$ und $b = \mathrm{LC}(f_b)$ für $f_a, f_b \in I$.
      - Da I ein Ideal ist, darf man Elemente aus I mit Elementen aus $R[x]$ multiplizieren und bleibt in I. Also sind $\underbrace{\mathrm{LT}(f_b)}_{\in R[x]} \cdot \underbrace{f_a}_{\in I} \in I$ und $\underbrace{\mathrm{LT}(f_a)}_{\in R[x]} \cdot \underbrace{f_b}_{\in I} \in I$. (Warum gerade diese Produkte? Diese beiden Produkte haben den gleichen Leitterm, nämlich $\mathrm{LT}(f_a) \cdot \mathrm{LT}(f_b)$.)
      - Es gilt offensichtlich $\mathrm{LC}\left(\underbrace{\mathrm{LT}(f_b)}_{\text{ist ja nur ein Term und daher } \mathrm{LC}(f_b)=1} \cdot f_a \right) = \mathrm{LC}(f_a) = a$ und $\mathrm{LC}\left(\underbrace{\mathrm{LT}(f_a)}_{\text{ist ja nur ein Term und daher } \mathrm{LC}(f_b)=1} \cdot f_b \right) = \mathrm{LC}(f_b) = b$.
      - Addiere nun $\underbrace{\mathrm{LT}(f_b) \cdot f_a}_{\in I} + \underbrace{\mathrm{LT}(f_a) \cdot f_b}_{\in I} \in I$. Da beide Summanden den gleichen Leitterm haben (siehe oben), addieren sich ihre Leitkoeffizienten, also $\mathrm{LC}(\mathrm{LT}(f_b) \cdot f_a + \mathrm{LT}(f_a) \cdot f_b) = \mathrm{LC}(\mathrm{LT}(f_b) \cdot f_a) + \mathrm{LC}(\mathrm{LT}(f_a) \cdot f_b) = a + b$.
      - Also ist auch $a+b$ in $\mathrm{LC}(I)$, denn $a+b$ ist der Leitkoeffizient vom Element $\mathrm{LT}(f_b) \cdot f_a + \mathrm{LT}(f_a) \cdot f_b$, welches in I liegt.
    - Sei $a \in \mathrm{LC}(I)$. Dann muss auch $r \cdot a \in \mathrm{LC}(I)$ sein mit $r \in R$.:
      - Sei $a = \mathrm{LC}(f_a)$.
      - Da I ein Ideal ist, darf man Elemente aus I mit Elementen aus $R[x]$ multiplizieren und bleibt in I. Also $\underbrace{r}_{\in R[x], \text{ weil} \in R} \cdot \underbrace{f_a}_{\in I} \in I$.
      - Es gilt offensichtlich $\mathrm{LC}(r \cdot f_a) = r \cdot \mathrm{LC}(f_a) = r \cdot a$.
      - Also ist auch $r \cdot a$ in $\mathrm{LC}(I)$, denn $r \cdot a$ ist der Leitkoeffizient vom Element $r \cdot f_a$, welches in I liegt.
  - Die $\mathrm{LC}(I^{(i)})$-s sind Ideale in R, weil:
    - Seien $a,b \in \mathrm{LC}(I^{(i)})$. Dann muss auch $a+b$ auch in $\mathrm{LC}(I^{(i)})$ liegen.:
      - Seien $a = \mathrm{LC}(f_a)$ und $b = \mathrm{LC}(f_b)$ mit $\deg f_a = \deg f_b = i$.

- Da der Grad der beiden Polynome gleich ist und es nur eine Variable (x) gibt, ist $f_a = ax^i + \ldots$ und $f_b = bx^i + \ldots$.
- Dann ist aber auch $\deg(f_a + f_b) = i$, denn $\deg(f_a + f_b) = \deg\left(\underbrace{ax^i + \ldots}_{=f_a} + \underbrace{bx^i + \ldots}_{=f_b}\right) = \deg\left((a+b)x^i + \ldots\right) = i$.
- Also ist auch $a+b$ in $\mathrm{LC}\left(I^{(i)}\right)$, denn $a+b$ ist der Leitkoeffizient vom Element $f_a + f_b$, welches Grad i hat.

- Sei $a \in \mathrm{LC}\left(I^{(i)}\right)$. Dann muss auch $r \cdot a \in \mathrm{LC}\left(I^{(i)}\right)$ sein mit $r \in R$.:
  - Sei $a = \mathrm{LC}(f_a)$ mit $\deg f_a = i$, also $f_a = ax^i + \ldots$.
  - Multipliziere f_a mit r und erhalte $r \cdot f_a = rax^i + \ldots$ mit $\deg(r \cdot f_a) = i$ und $\mathrm{LC}(r \cdot f_a) = r \cdot \mathrm{LC}(f_a) = r \cdot a$.
  - Also ist auch $r \cdot a$ in $\mathrm{LC}\left(I^{(i)}\right)$, denn $r \cdot a$ ist der Leitkoeffizient vom Element $r \cdot f_a$, welches Grad i hat.

- Weil die $\mathrm{LC}\left(I^{(i)}\right)$-s Ideale in R sind und R noetherian ist, sind auch die $\mathrm{LC}\left(I^{(i)}\right)$-s noetherian. Somit werden sie endlich erzeugt: $\mathrm{LC}\left(I^{(i)}\right) = \left\langle r_1^{(i)}, \ldots, r_{s_i}^{(i)} \right\rangle$
- $f_j^{(i)} := r_j^{(i)} x^i + \ldots$, wobei $0 \le i \le k-1$ und $1 \le j \le s_i$ (also $r_j^{(i)} \in \left\{r_1^{(i)}, \ldots, r_{s_i}^{(i)}\right\}$)
- Ergänzungen zum Beweis der Behauptung $I = \left\langle f_1, \ldots, f_s, f_1^{(k-1)}, \ldots, f_{s_{k-1}}^{k-1}, \ldots, f_1^{(0)}, \ldots, f_{s_0}^{(0)} \right\rangle$:
  - Die u_i-s $\in R$ gibt es allgemein, weil $f \in I$ und $\mathrm{LC}(I) = \langle r_1, \ldots, r_s \rangle$, und nicht nur, weil $\deg f \ge k$.
  - Die Bedingung $\deg f \ge k$ wird nur benötigt, damit in $f - \left(u_1 x^{\deg f - \deg f_1} f_1 + \ldots + u_s x^{\deg f - \deg f_s} f_s\right)$ die Exponenten $\deg f - \deg f_i$ nicht negativ werden können, denn der größte Grad der f_i-s ist k (mit anderen Worten: $\max_{1 \le i \le s}\{\deg f_i\} = k$) (siehe Tafelbild 'University; Computational Commutative Algebra 1 (Algebra 2); SS 2004; 2004-06-08; 12-18').
  - $f - \underbrace{\left(u_1 x^{\deg f - \deg f_1} f_1 + \ldots + u_s x^{\deg f - \deg f_s} f_s\right)}_{\in I, \text{ da alle } f_i \in I}$
    $\underset{\text{nach Definition der } f_i}{=} f - \left(\left(u_1 x^{\deg f - \deg f_1} r_1 x^{\deg f_1} + \ldots\right) + \ldots + \left(u_s x^{\deg f - \deg f_s} r_s x^{\deg f_s} + \ldots\right)\right)$
  - $= f - \left(\left(u_1 r_1 x^{\deg f} + \ldots\right) + \ldots + \left(u_s r_s x^{\deg f} + \ldots\right)\right)$
    $= \underbrace{f}_{=\mathrm{LC}(f) x^{\deg f} + \ldots} - \left(\underbrace{\left(u_1 r_1 + \ldots + u_s r_s\right)}_{=\mathrm{LC}(f)} x^{\deg f} + \ldots\right)$
  - Ist $f - \underbrace{\left(u_1 x^{\deg f - \deg f_1} f_1 + \ldots + u_s x^{\deg f - \deg f_s} f_s\right)}_{\in I, \text{ da alle } f_i \in I} = 0$, so ist $f = u_1 x^{\deg f - \deg f_1} f_1 + \ldots + u_s x^{\deg f - \deg f_s} f_s$ und die Behauptung stimmt, da sich f als Linearkombination der $f_1, \ldots, f_s, f_1^{(k-1)}, \ldots, f_{s_{k-1}}^{k-1}, \ldots, f_1^{(0)}, \ldots, f_{s_0}^{(0)}$ schreiben lässt.
  - Ist $f - u_1 x^{\deg f - \deg f_1} f_1 + \ldots + u_s x^{\deg f - \deg f_s} f_s \ne 0$, so ist aber wegen

$$f-\left(u_1x^{\deg f-\deg f_1}f_1+\ldots+u_sx^{\deg f-\deg f_s}f_s\right)=\underbrace{f}_{=\mathrm{LC}(f)x^{\deg f}+\ldots}-\left(\underbrace{\left(u_1r_1+\ldots+u_sr_s\right)}_{=\mathrm{LC}(f)}x^{\deg f}+\ldots\right)$$

$\deg\left(f-\left(u_1x^{\deg f-\deg f_1}f_1+\ldots+u_sx^{\deg f-\deg f_s}f_s\right)\right)<\deg f$ und man mit diesem Elemenent wieder vorne anfangen.

- Ist $\deg f=:g<k$, so ist $\mathrm{LC}(f)=\mathrm{LC}\left(I^{(g)}\right)=\left\langle r_1^{(g)},\ldots,r_{s_g}^{(g)}\right\rangle$, also $\mathrm{LC}(f)=u_1^{(g)}r_1^{(g)}+\ldots+u_{s_g}^{(g)}r_{s_g}^{(g)}$.
- Außerdem gibt es zu den $r_j^{(g)}$-s passende Polynome, nämlich die $f_j^{(g)}$-s mit $f_j^{(g)}=r_j^{(g)}x^g+\ldots.$
- Bilde nun statt $f-\left(u_1x^{\deg f-\deg f_1}f_1+\ldots+u_sx^{\deg f-\deg f_s}f_s\right)$ entsprechend $f-\underbrace{\left(u_1^{(g)}x^{\deg f-\overbrace{\deg f_1^{(g)}}^{=g}}f_1^{(g)}+\ldots+u_s^{(g)}x^{\deg f-\overbrace{\deg f_{sg}^{(g)}}^{=g}}f_{s_g}^{(g)}\right)}_{\in I}$ und gehe analog zum Fall $\deg f\geq k$ vor, wodurch es wieder ein Polynom kleineren Grades gibt oder man die 0 erreicht.
- Erreicht man irgendwann die 0 (muss man zwangsläufig, weil die Grade ja von Schritt zu Schritt immer kleiner werden), so hat man

$$f-\left(u_1x^{\deg f-\deg f_1}f_1+\ldots+u_sx^{\deg f-\deg f_s}f_s\right)-\ldots$$
$$-\left(u_1^{(g)}x^{\deg f-\deg f_1^{(g)}}f_1^{(g)}+\ldots+u_s^{(g)}x^{\deg f-\deg f_{sg}^{(g)}}f_{s_g}^{(g)}\right)-\ldots=0$$
$$\Leftrightarrow f=\left(u_1x^{\deg f-\deg f_1}f_1+\ldots+u_sx^{\deg f-\deg f_s}f_s\right)+\ldots$$
$$+\left(u_1^{(g)}x^{\deg f-\deg f_1^{(g)}}f_1^{(g)}+\ldots+u_s^{(g)}x^{\deg f-\deg f_{sg}^{(g)}}f_{s_g}^{(g)}\right)+\ldots$$

und hat somit f als Linearkombination der $f_1,\ldots,f_s,f_1^{(k-1)},\ldots,f_{s_{k-1}}^{k-1},\ldots,f_1^{(0)},\ldots,f_{s_0}^{(0)}$ dargestellt.

- Hilfssatz 1:
  - $\underbrace{W}_{\text{Untermodul von } M}\overset{\pi'}{\mapsto}\underbrace{W/U}_{\text{Untermodul von } (M/U)}$
  - π' ist in der Tat bijektiv, wenn man es nicht mit π verwechselt, denn $W\overset{\pi'}{\mapsto}W/U$. Kennt man nämlich $\overline{W}:=W/U$, so kann man W eindeutig angeben, nämlich $W=\overline{W}+U$.
- Beispiel zu 'Normalform':
  - Wähle $K[x]$ als P^r und das Ideal $\left(x^2+x\right)$ als M.
  - Dann können in $K[x]/\left(x^2+x\right)$ nur Polynome vom Typ $c_1x^1+c_0x^0$ (eigentlich $\overline{c_1x^1+c_0x^0}$, weil die Elemente von $K[x]/\left(x^2+x\right)$ ja eigentlich Restklassen sind) liegen, wobei $c_i\in K$.
  - Also wird $K[x]/\left(x^2+x\right)$ erzeugt durch $\left(x^1,x^0\right)$. Da die Koeffizienten **nur** aus K kommen, ist $K[x]/\left(x^2+x\right)$ ein K-Vektorraum.
  - Z. B. liegt x^2 in der Restklasse $\overline{-x}$, weil $x^2=\underbrace{1\cdot\left(x^2+x\right)}_{\in\left(x^2+x\right)}+\underbrace{(-1)x}_{K[x]/\left(x^2+x\right)}$.

- Da dieser Rest hier eindeutig ist, gilt: $\mathrm{NF}(x^2) = -x$.
- $\mathrm{NF}^2 = \mathrm{NF}$, weil: $\mathrm{NF}^2(x^2) = \mathrm{NF}(\mathrm{NF}(x^2)) = \mathrm{NF}(-x) = -x = \mathrm{NF}(x^2)$
- $\mathrm{NF}_{|M} = 0$, weil: Elemente aus M sind in $\overline{0}$ und haben damit keinen Rest, also $\mathrm{NF}_{|M} = 0$.
- $\mathrm{NF}_{|\langle B\rangle_K} = \mathrm{id}_{\langle B\rangle_K}$, weil: Elemente aus $\langle B\rangle_K$ gerade die Reste sind und sich daher modulo M nicht mehr verändern.

- Ergänzung zu 'reduzierte Gröbner-Basis':
  - $\tilde{g}_i := \mathrm{LT}(g_1) - \underbrace{\sum_{b\in B} c_{i.b} b}_{=\mathrm{NF}(\mathrm{LT}(g_1))} \in M$, weil:
    - Für jedes (Multidimensionen-)Polynom p gilt: $p = \underbrace{m}_{M\text{-Anteil von } p} + \underbrace{\mathrm{NF}(p)}_{\text{'Divisionsrest'}}$.
    - Also $p - \mathrm{NF}(p) = m \in M$.
    - eigentlich sowieso klar, denn: $\underbrace{7}_{\triangleq p} \bmod 4 = \underbrace{3}_{\triangleq \mathrm{NF}(7)} \Leftrightarrow 7 = \underbrace{1\cdot 4}_{\triangleq M\text{-Anteil von } p} + 3$, also $7 - 3 = 1\cdot 4 \in M$.
  - '$\tilde{g}_i := \mathrm{LT}(g_1)$' reicht nicht, denn dann gilt zwar $\langle \mathrm{LT}(\tilde{g}_1),\ldots,\mathrm{LT}(\tilde{g}_t)\rangle = \mathrm{LT}(M)$, aber nicht $\tilde{g}_i \in M$, was aber auch benötigt wird, damit man sagen kann, dass $\langle \tilde{g}_1,\ldots,\tilde{g}_t\rangle = M$.

2004-06-15

- Ergänzung zu Tafelbild 'University; Computational Commutative Algebra 1 (Algebra 2); SS 2004; 2004-06-15; 02-12':
  - $w - (r_1 w_1 + \ldots + r_l w_l) \in U$, weil:
    - $(r_1 w_1 + \ldots + r_l w_l)$ ist Representant von w in M/U (wegen $\pi(w) = (r_1 w_1 + \ldots + r_l w_l) + U$), liegt also in modulo U in derselben Restklasse wie w.
    - Wenn 2 Elemente in derselben Restklasse liegen, bedeutet dass, ihre Differenz in U liegt.
  - $w - (r_1 w_1 + \ldots + r_l w_l) \in W \cap U$, weil:
    - $w - (r_1 w_1 + \ldots + r_l w_l) \in U$ (siehe gerade eben)
    - $w - (r_1 w_1 + \ldots + r_l w_l) \in W$, weil $\underbrace{\underbrace{w}_{\in W} - \underbrace{\left(\underbrace{r_1 \underbrace{w_1}_{\in W}}_{\in W} + \underbrace{\ldots}_{\in W} + \underbrace{r_l \underbrace{w_l}_{\in W}}_{\in W}\right)}_{\in W}}_{\in W}$
- Ergänzung zum Korollar auf Tafelbild 'University; Computational Commutative Algebra 1 (Algebra 2); SS 2004; 2004-06-15; 03-12':
  - R^k ist noetherian, falls r noetherian ist, weil:
    - Wähle im Hilfsatz von eben $M := R^k$, $U := R^{k-1}$ und somit $M/U = R^k / R^{k-1} = R$.
    - Dann ist (nach Induktion) $U = R^{k-1}$ noetherian und nach Voraussetzung $M/U = R$ noetherian.
    - Laut Hilfssatz ist dann $M = R^k$ noetherian.
- Ergänzung zum Satz auf Tafelbild 'University; Computational Commutative Algebra 1

(Algebra 2); SS 2004; 2004-06-15; 03-12':

- Gerade gezeigt: R^k ist noetherian.
- Außerdem ist $U := \ker(\varphi)$ ein Untermodul von R^k.
- Wähle also im Hilfssatz 2 auf Tafelbild 'University; Computational Commutative Algebra 1 (Algebra 2); SS 2004; 2004-06-08; 15-18' das **dortige** M als R^k und U als $\ker(\varphi)$.
- Erhalte, dass $R^k / \ker(\varphi)$ noetherian ist.
- Nun ist aber das M aus dem Satz auf Tafelbild 'University; Computational Commutative Algebra 1 (Algebra 2); SS 2004; 2004-06-15; 03-12' isomorph zu $R^k / \ker(\varphi)$, also auch noetherian.

- Ergänzung zu Tafelbild 'University; Computational Commutative Algebra 1 (Algebra 2); SS 2004; 2004-06-15; 11-12':
  - $\mathrm{LT}(\tilde{g}_i) = \mathrm{LT}(g_i)$, weil:
    - $\tilde{g}_i := \underbrace{\mathrm{LT}\left(\underbrace{g_i}_{\in M}\right)}_{\in \mathrm{LT}\{M\}} - \underbrace{\sum_{b \in B} c_b^{(i)} b}_{\in B}$
    - Da aber auch $\tilde{g}_i \in M$, ist $\mathrm{LT}(\tilde{g}_i) \in \mathrm{LT}\{M\}$.
    - Da aber $\mathrm{LT}\{M\}$ disjunkt mit B und $\tilde{g}_i$ nur einen Term in $\mathrm{LT}\{M\}$ hat (alle anderen sind in B), so muss dieser Term der Leitterm von $\tilde{g}_i$ sein.
    - Dieser Term ist $\mathrm{LT}(g_i)$.
    - Mit anderen Worten: $\mathrm{LT}(\tilde{g}_i) = \mathrm{LT}(g_i)$.

2004-06-17

- Ergänzung zu Tafelbild 'University; Computational Commutative Algebra 1 (Algebra 2); SS 2004; 2004-06-17; 07-24': Mit '$\mathcal{O}$' ist das gemeint, was bisher B hieß, nämlich $\Pi^n \setminus \mathrm{LT}\{M\}$ bzw. $\Pi^n \setminus \mathrm{LT}\{I\}$.
- Ergänzung zu Tafelbild 'University; Computational Commutative Algebra 1 (Algebra 2); SS 2004; 2004-06-17; 11-24':
  - $\tau_{ij} := \sigma_{ij} - (h_1, \ldots, h_s) \in \mathrm{Syz}(f_1, \ldots, f_s)$, weil:

$$S(f_i, f_j) = \sum_{k=1}^{s} h_k f_k$$

$$\Leftrightarrow \underbrace{S(f_i, f_j)}_{\text{nach Definition } = \lambda(\sigma_{ij})} - \underbrace{\sum_{k=1}^{s} h_k f_k}_{\text{nach Definition von } \lambda \text{ gleich } \lambda(h_1, \ldots, h_s)} = 0$$

$$\Leftrightarrow \lambda(\sigma_{ij}) - \lambda(h_1, \ldots, h_s) = 0$$

$$\Leftrightarrow \lambda\left(\underbrace{\sigma_{ij} - (h_1, \ldots, h_s)}_{=: \tau_{ij}}\right) = 0$$

$$\Leftrightarrow \lambda(\tau_{ij}) = 0$$

$$\underbrace{\Leftrightarrow}_{\lambda \text{ ist gerade so definiert worden}} \tau_{ij} \in Syz(f_1, \ldots, f_s)$$

- $\mathrm{LF}(\tau_{ij}) = \sigma_{ij}$, wegen: $\mathrm{LT}(h_i f_i) \le \mathrm{LT}\left(\underbrace{S(f_i, f_j)}_{=\lambda(\sigma_{ij})}\right)$ bzw. $\mathrm{LT}\left(\underbrace{S(f_i, f_j)}_{=\lambda(\sigma_{ij})}\right) = \max_{1 \le i \le s}(\mathrm{LT}(h_i f_i))$.

- Ergänzung zu Buchberger's Algorithmus (Tafelbild 'University; Computational Commutative Algebra 1 (Algebra 2); SS 2004; 2004-06-17; 12-24' und folgende):
  - Eine Frage, die man sich stellen könnte, ist, wo der Sinn darin liegt, S'_{ij} im Fall $S'_{ij} \neq 0$ dem bisherigen Erzeugendensystem $G = (g_1, \ldots, g_s)$ von I hinzuzufügen (Schritt 4).
  - Dazu erinnere man sich an folgende Charakterisierung eine Gröbner-Basis: G ist eine Gröbner-Basis $\Leftrightarrow \mathrm{LT}\left\{\underbrace{I}_{\text{oder allgemein } M}\right\} = (\mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s))$.
  - Ist nun $S'_{ij} = \underbrace{\mathrm{NR}_{\underbrace{G}_{\text{hier noch} = (g_1, \ldots, g_s)}}\left(\underbrace{S(g_i, g_j)}_{\in I}\right)}_{\in I, \text{ denn } \mathrm{NR}_G(m) = \underbrace{m}_{\in I} - \underbrace{\sum_{i=1}^{s} p_i \underbrace{g_i}_{\in I}}_{\in I} \in I} \neq 0$, so ist, weil der Divisionsalgorithmus hier gestoppt hat, $\mathrm{LT}(S'_{ij})$ durch kein $\mathrm{LT}(g_i)$ mehr teilbar.
  - Mit anderen Worten: $\mathrm{LT}(S'_{ij})$ ist kein Vielfaches eines $\mathrm{LT}(g_i)$ mehr.
  - Mit anderen Worten: $\underbrace{\mathrm{LT}\left(\underbrace{S'_{ij}}_{\in I}\right)}_{\in \mathrm{LT}\{I\}} \notin (\mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s))$.
  - Also ist $\mathrm{LT}\{I\} \neq (\mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s))$ und damit G keine Gröbner-Basis.
  - Fügt man nun $g_{s'} := S'_{ij}$ dem bisherigen G hinzu, so erzwingt man gerade, dass dann $\mathrm{LT}(S'_{ij}) \in (\mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s), \mathrm{LT}(g_{s'}))$, denn es ist ja gerade $\mathrm{LT}(S'_{ij}) = \mathrm{LT}(g_{s'})$, weil ja $g_{s'} := S'_{ij}$.
  - Dann besteht die Chance, dass jetzt $\mathrm{LT}\{I\} = (\mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s), \mathrm{LT}(g_{s'}))$ und somit G eine Gröbner-Basis für I ist.
- Ergänzung zu Tafelbild 'University; Computational Commutative Algebra 1 (Algebra 2); SS 2004; 2004-06-17; 23-24':
  - Wie kommt man auf die angeschriebene, hinzuzufügende Spalte?
  - Man möchte am Ende eine Matrix A haben, so dass $G = FA$. (Beachte: G und F sind Zeilenvektoren. $G = \underbrace{(g_1, \ldots, g_{s'})}_{\text{bisher berechnete Gröbner-Basis}}$ und $F = \underbrace{(f_1, \ldots, f_s)}_{\text{ursprüngliches Erzeugendensystem}}$.)
  - Zu Anfang ist $(g_1, \ldots, g_{s'}) = (f_1, \ldots, f_s)$ (also auch $s' = s$), also $(g_1, \ldots, g_{s'}) = (f_1, \ldots, f_s) \underbrace{\begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & \ddots & & \vdots \\ \vdots & & \ddots & 0 \\ 0 & \cdots & 0 & 1 \end{pmatrix}}_{\text{Einheitsmatrix } I_s \text{ (mit } s \text{ Zeilen und } s' \text{ Spalten)}}$.
  - Diese Gleichheit soll nach jedem Iterationsschritt des Algorithmus wiederhergestellt werden. Da einerseits in jedem Iterationsschritt ein p zu G hinzukommt, muss die

bisherige Matrix A angepasst werden.

- Da $p = \underbrace{S(g_i, g_j)}_{=\frac{1}{c_i}t_{ij}g_i - \frac{1}{c_j}t_{ji}g_j} - q_1 g_1 - \ldots - q_{s'} g_{s'}$ (siehe vorheriges Tafelbild) und $g_i = (f_1, \ldots, f_s)\underbrace{\vec{a}_i}_{i\text{-te Spalte der Matrix}}$ (für alle g_i) gilt, ist

$$p = (f_1, \ldots, f_s)\underbrace{\left(\frac{1}{c_i}t_{ij}\vec{a}_i - \frac{1}{c_j}t_{ji}\vec{a}_j - q_1\vec{a}_1 - \ldots - q_{s'}\vec{a}_{s'}\right)}_{\text{Dies ist ein Spaltenvektor der Länge } s.}.$$

- Hängt man diesen Spaltenvektor an A an, so erhält man gerade: $\underbrace{(g_1, \ldots, g_{s'}, p)}_{=G}$

$$= \underbrace{(f_1, \ldots, f_s)}_{=F}\underbrace{\left(\underbrace{\underbrace{\begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & \ddots & & \vdots \\ \vdots & & \ddots & 0 \\ 0 & \cdots & 0 & 1 \end{pmatrix}}_{\substack{\text{Einheitsmatrix } I_s \\ \text{vom Anfang}}} \underbrace{\vec{a}_{s+1} \quad \cdots \quad \vec{a}_{s'}}_{\substack{\text{bisher hinzugefügte} \\ \text{Spaltenvektoren}}}}_{\text{bisherige Matrix } A} \underbrace{\left(\frac{1}{c_i}t_{ij}\vec{a}_i - \frac{1}{c_j}t_{ji}\vec{a}_j - q_1\vec{a}_1 - \ldots - q_{s'}\vec{a}_{s'}\right)}_{\text{neuer Spaltenvektor für } p}\right)}_{\text{neue Matrix } A}$$

- Also $\left(\frac{1}{c_i}t_{ij}\vec{a}_i - \frac{1}{c_j}t_{ji}\vec{a}_j - q_1\vec{a}_1 - \ldots - q_{s'}\vec{a}_{s'}\right)$.

- Ergänzung zu Tafelbild ‘University; Computational Commutative Algebra 1 (Algebra 2); SS 2004; 2004-06-17; 24-24’:
  - $h_i = (g_1, \ldots, g_{s'})\begin{pmatrix} b_{1,i} \\ \vdots \\ b_{s',i} \end{pmatrix}$
  - Wie fährt man nun fort, wenn man die Matrix B hat?
  - Ziel ist es ja, $h = \underbrace{(h_1, \ldots, h_t)}_{H}\begin{pmatrix} c_1 \\ \vdots \\ c_t \end{pmatrix}$ als $h = (f_1, \ldots, f_s)\begin{pmatrix} d_1 \\ \vdots \\ d_s \end{pmatrix}$ auszudrücken. d. h. man will $\begin{pmatrix} d_1 \\ \vdots \\ d_t \end{pmatrix}$ kennen.
  - Nun gilt: $H = GB = \underbrace{FA}_{=G}B$.

- also: $h = \underbrace{(h_1,\ldots,h_t)}_{H}\begin{pmatrix} c_1 \\ \vdots \\ c_t \end{pmatrix} = \underbrace{(f_1,\ldots,f_s)}_{F}\underbrace{\underbrace{A}_{s\times s'}\underbrace{B}_{s'\times t}\underbrace{\begin{pmatrix} c_1 \\ \vdots \\ c_t \end{pmatrix}}_{s\times 1}}_{=:\begin{pmatrix} d_1 \\ \vdots \\ d_s \end{pmatrix}}$

2004-06-22

- Ergänzungen zu Tafelbild 'University; Computational Commutative Algebra 1 (Algebra 2); SS 2004; 2004-06-22; 01-18':
  - In dieser Definition fällt ein wesentlicher Teil nicht auf, nämlich, dass die g_i-s aus M sein müssen.
  - Die Definition im Buch (Definition 2.4.2) ist natürlicher.
- Ergänzung zu Bemerkung 2 auf Tafelbild 'University; Computational Commutative Algebra 1 (Algebra 2); SS 2004; 2004-06-22; 02-18':
  - Je nachdem, welche Definition für 'Gröbner-Basis' man benutzt ist entweder nichts zu zeigen (Definition aus dem Buch) oder es ist was zu beweisen (Definition auf Tafelbild 'University; Computational Commutative Algebra 1 (Algebra 2); SS 2004; 2004-06-22; 01-18'). Im letzteren Fall Fall ist der Beweis ab Tafelbild 'University; Computational Commutative Algebra 1 (Algebra 2); SS 2004; 2004-06-08; 07-18' zu finden.
- Ergänzungen zu Tafelbild 'University; Computational Commutative Algebra 1 (Algebra 2); SS 2004; 2004-06-22; 03-18':
  - $v'-v'' \in M$, weil $v'-v'' = \underbrace{\left(\underbrace{v-v''}_{\in M}\right)-\left(\underbrace{v-v'}_{\in M}\right)}_{\in M}$.
  - "Insbesondere gilt $v'-v''=0$ oder ...": Hier wird eine Fallunterscheidung gemacht. 1. Fall: $v'-v''=0$, daher ohne Leitterm, weil kein Grad. Dann gilt offensichlich $v'=v''$. 2. Fall: Es gibt einen Grad, somit einen Leitterm. Dieser ist dann in $\mathrm{LT}(M)$, weil $v'-v'' \in M$.
- Beispiel zu Tafelbild 'University; Computational Commutative Algebra 1 (Algebra 2); SS 2004; 2004-06-22; 16-18':
  - Sei $f(x_1x_2) := x_1^2 + x_1x_2 - x_2 - 1$.
  - Dann ist $\deg(f) = 2$.
  - Dann ist:

$$f^{\mathrm{hom}}\left(\underbrace{x_0}_{\text{neue Variable}}, x_1, x_2\right) = x_0^{\overset{=\deg(f)}{\widehat{2}}} \cdot f\left(\frac{x_1}{x_0}, \frac{x_2}{x_0}\right) = x_0^2 \cdot \left(\left(\frac{x_1}{x_0}\right)^2 + \left(\frac{x_1}{x_0}\right)\left(\frac{x_2}{x_0}\right) - \left(\frac{x_2}{x_0}\right) - 1\right)$$

$$= x_1^2 + x_1x_2 - x_0x_2 - x_0^2$$

  - In f^{hom} hat jeder Term Grad 2, also ist f^{hom} homogen vom Grad 2.
  - Das kommt dadurch, weil f^{hom} sich aus f ergibt, indem diejenigen Terme, die in f einen zu kleinen Grad haben mit einer zusätzlichen Variable (x_0) aufgefüllt werden, bis sie denselben Grad haben, wie die Terme, die den größten Grad haben, also $\deg(f)$.

- Ergänzung zu Tafelbild ‘University; Computational Commutative Algebra 1 (Algebra 2); SS 2004; 2004-06-22; 18-18’:
  - Wenn $\frac{\mathrm{LCM}(t_i,t_j,t_k)}{t_{ik}}=1$ ist, so ist $\sigma_{ik}=\frac{\mathrm{LCM}(t_i,t_j,t_k)}{t_{ij}}\sigma_{ij}+\frac{\mathrm{LCM}(t_i,t_j,t_k)}{t_{jK}}\sigma_{jK}$.
  - Dann aber ist σ_{ik} im Erzeugendensystem von $\mathrm{Syz}(\mathrm{LM}(G))$ (welcher ja auf jeden Fall von der Menge aller σ_{ij} erzeigt wird) überflüssig.

2004-06-24

- Ergänzungen zum Beispiel auf Tafelbild ‘University; Computational Commutative Algebra 1 (Algebra 2); SS 2004; 2004-06-22; 05-18’:
  - Die eigentlich Aussage des Beispiels ist, dass, wenn man I als Gröbner-Basis gegeben hat, man sofort sehen kann, ob $P=I$ und damit , ob $\mathrm{Z}(I)=\{\}$, nämlich genau dann, wenn in der Gröbner-Basis eine Kostante steht.
  - $\mathrm{NF}(1)=0 \Leftrightarrow$ In der Gröbner-Basis gibt es eine Konstante, weil:
    - Der Leitterm von 1 lässt sich unter der Voraussetzung $\mathrm{NF}(1)=0$ durch ein g_i aus der Gröbner-Basis teilen.
    - Dazu muss der Leitterm von g_i aber kleiner oder gleich dem von 1 sein.
    - Da es nicht echt kleiner geht, bleibt nur gleich.
    - Da nur Konstanten den Grad 0 haben, ist g_i also eine Kosntante.
    - Da man durch g_i teilen kann, ist g_i nicht 0.

2004-06-29

- Ergänzung zur Bemerkung auf Tafelbild ‘University; Computational Commutative Algebra 1 (Algebra 2); SS 2004; 2004-06-29; 08-10’:
  - $I\subseteq\sqrt{I}$, weil $\sqrt{I}=\left\{f\middle|f^i\in I\right\}\supseteq\left\{f\middle|f^1\in I\right\}=I$
  - $\mathrm{Z}(I)\supseteq\mathrm{Z}\left(\sqrt{I}\right)$, weil:
    - $\vec{a}\in\mathrm{Z}\left(\sqrt{I}\right)\Rightarrow f(\vec{a})=0\forall g\in\sqrt{I}$
    - Da $I\subseteq\sqrt{I}$, gilt insbesondere $f(\vec{a})=0\forall f\in I$.
    - Dann aber ist $\vec{a}\in\mathrm{Z}(I)$.
    - Also $\vec{a}\in\mathrm{Z}\left(\sqrt{I}\right)\Rightarrow\vec{a}\in\mathrm{Z}(I)$.
    - Das ist genau dann der Fall, wenn $\mathrm{Z}(I)\supseteq\mathrm{Z}\left(\sqrt{I}\right)$ (einfache Mengentheorie).
- Ergänzung zu Tafelbild ‘University; Computational Commutative Algebra 1 (Algebra 2); SS 2004; 2004-06-29; 10-10’:

$$Z(I \cap J) = Z(I) \cup Z(J)$$
$$\Leftrightarrow \{\vec{a} | h(\vec{a}) = 0 \forall h \in I \cap J\} = \{\vec{a} | f(\vec{a}) = 0 \forall f \in I\} \cup \{\vec{a} | g(\vec{a}) = 0 \forall g \in J\}$$

- $$\Leftrightarrow \{\vec{a} | h(\vec{a}) = 0 \forall h \in I \cap J\} = \{\vec{a} | f(\vec{a}) = 0 \forall f \in I \vee g(\vec{a}) = 0 \forall g \in J\}$$

$$\Leftrightarrow \left(h(\vec{a}) = 0 \forall h \in I \cap J \underbrace{\Leftrightarrow}_{\substack{\text{'}\Rightarrow\text{' entspricht } \subseteq \\ \text{'}\Leftarrow\text{' entspricht } \supseteq}} f(\vec{a}) = 0 \forall f \in I \vee g(\vec{a}) = 0 \forall g \in J \right)$$
$$\Leftrightarrow (\exists h \in I \cap J : h(\vec{a}) \neq 0 \Leftrightarrow \exists f \in I : f(\vec{a}) \neq 0 \wedge \exists g \in J : g(\vec{a}) \neq 0)$$

- '$\Rightarrow$':
  - Wähle das existierende $h \in I \cap J$, so dass $h(\vec{a}) \neq 0$.
  - Da $h \in I \cap J$, ist $h \in I$ und $h \in J$.
  - Wähle das zu findende $f := h$ und das zu findende $g := h$.
  - Dann gilt $f(\vec{a}) \neq 0 \wedge g(\vec{a}) \neq 0$.
- '$\Leftarrow$':
  - Wähle die existierenden $f \in I$ und $g \in J$ mit: $f(\vec{a}) \neq 0 \wedge g(\vec{a}) \neq 0$.
  - Dann ist $h := fg \in I \cap J$, denn $fg \in I$, weil $f \in I$, und $fg \in J$, weil $g \in J$.
  - Dann ist $h(\vec{a}) = \underbrace{f(\vec{a})}_{\neq 0} \cdot \underbrace{g(\vec{a})}_{\neq 0} \neq 0$.

2004-07-01

- Ab Tafelbild 'University; Computational Commutative Algebra 1 (Algebra 2); SS 2004; 2004-07-01; 03-18' ist das Liften von Syzygien sehr schön erklärt.
- Ergänzung zu Tafelbild 'University; Computational Commutative Algebra 1 (Algebra 2); SS 2004; 2004-07-01; 08-18' und 'University; Computational Commutative Algebra 1 (Algebra 2); SS 2004; 2004-07-01; 09-18':
  - Bisher ist nur bekannt, wie man Sysygien für Gröbner-Basen berechnet, nicht aber für beliebige Erzeugendensystem.
  - Daher wird das beliebige Erzeugendensystem zunächst in eine Gröbner-Basis konvertiert und *dafür* $Syz(G)$ berechnet (Schritt 3).
- Ergänzungen zu Tafelbild 'University; Computational Commutative Algebra 1 (Algebra 2); SS 2004; 2004-07-01; 14-18':
  - Man kann f_i weglassen, wenn es einen Spaltenvektor $\begin{pmatrix} h_1 \\ \vdots \\ h_s \end{pmatrix}$ in M gibt mit $h_i \in K \setminus \{0\}$

    (also eine $h_i = const$), denn:
    - Die Spaltenvektoren von M erzeugen nach Definition den Syzygienmodul von $(f_1, \ldots, f_s)$.
    - Insbesondere ist jeder Spaltenvektoren von M selbst eine Syzygie von $(f_1, \ldots, f_s)$.
    - Also $(f_1, \ldots, f_s) \begin{pmatrix} h_1 \\ \vdots \\ h_s \end{pmatrix} = f_1 h_1 + \ldots + f_s h_s = 0$.
    - Ist ein $h_i = const$, so gilt:

$$f_1 h_1 + \ldots + f_s h_s = 0$$
$$\Leftrightarrow f_1 h_1 + \ldots + f_{i-1} h_{i-1} + f_{i+1} h_{i+1} + \ldots + f_s h_s = -f_i \underbrace{h_i}_{=const}$$
$$\Leftrightarrow f_i = f_1 \frac{h_1}{-h_i} + \ldots + f_{i-1} \frac{h_{i-1}}{-h_i} + f_{i+1} \frac{h_{i+1}}{-h_i} + \ldots + f_s \frac{h_s}{-h_i}$$

- Also lässt sich f_i durch die übrigen f_j-s ausdrücken und kann demnach im Erzeugendensystem von weggelassen werden.

- Man kann f_i genau dann weglassen, wenn die *i*-te Zeile von *M* das Ideal (1) erzeugt, denn:
  - Zeige hier eigentlich nur die Rückrichtung, aber die Hinrichtung wird einem klar, wenn man die Rückrichtung verstanden hat.
  - Wenn die *i*-te Zeile von *M* das Ideal (1) erzeugt, dann gibt es $p_1,\ldots,p_{\underbrace{u}_{\text{Breite der Matrix}}}$, so dass $1 = p_1 \underbrace{h_{1.i}}_{i\text{-tes Element des 1. Spaltenvektors}} + \ldots + \underbrace{p_u h_{u.i}}_{i\text{-tes Element des } u\text{-ten Spaltenvektors}}$.
  - Ziel ist es nun, *M* eine neue Spalte hinzufügen zu können, in der an der *i*-ten Stelle eine Konstante steht.
  - Da in *M* nur Syzygien stehen dürfen, muss diese neue Spalte eine Syzygie sein.
  - Man darf beliebige Syzygien *M* hinzufügen, denn *M* soll ja ein Erzeugendensystem des Syzygienmoduls sein und einem Erzeugendensystem darf man beliebige Elemente des Moduls hinzufügen, ohne dass die Eigentschaft 'erzeugend' verloren geht.
  - Da man eine Spalte mit einer Konstanten an der *i*-ten Position haben will und $1 = p_1 h_{1.i} + \ldots + p_u h_{u.i}$, ist es nahe liegend, die neue Spalte so zu bilden: $$\left(p_1 \begin{pmatrix} h_{1.1} \\ \vdots \\ h_{1.s} \end{pmatrix} + \ldots + p_u \begin{pmatrix} h_{u.1} \\ \vdots \\ h_{u.s} \end{pmatrix} \right) = \begin{pmatrix} p_1 h_{1.1} + \ldots + p_u h_{u.1} \\ \vdots \\ p_1 h_{1.s} + \ldots + p_u h_{u.s} \end{pmatrix}.$$
  - Dass diese neue Spalte auch wirklich eine Syzygie von $f_1,\ldots,f_s$ ist, sieht man eigentlich schon daran, dass sie im Erzeugnis der alten Spalten liegt. Es lässt sich aber auch leicht direkt nachrechnen:
$$(f_1,\ldots,f_s) \begin{pmatrix} p_1 h_{1.1} + \ldots + p_u h_{u.1} \\ \vdots \\ p_1 h_{1.s} + \ldots + p_u h_{u.s} \end{pmatrix}$$
$$= f_1 (p_1 h_{1.1} + \ldots + p_u h_{u.1}) + \ldots + f_s (p_1 h_{1.s} + \ldots + p_u h_{u.s})$$
$$= f_1 p_1 h_{1.1} + \ldots + f_1 p_u h_{u.1} + \ldots + f_s p_1 h_{1.s} + \ldots + f_s p_u h_{u.s}$$
$$= \underbrace{f_1 p_1 h_{1.1} + \ldots + f_s p_1 h_{1.s}}_{=0,\text{ weil } \begin{pmatrix} h_{1.1} \\ \vdots \\ h_{1.s} \end{pmatrix} \text{ Syzygie ist}} + \underbrace{\ldots}_{=0} + \underbrace{f_1 p_u h_{u.1} + \ldots + f_s p_u h_{u.s}}_{=0,\text{ weil } \begin{pmatrix} h_{u.1} \\ \vdots \\ h_{u.s} \end{pmatrix} \text{ Syzygie ist}}$$
$$= 0$$
  - In der *i*-ten Zeile dieser Spalte steht nun $p_1 h_{1.i} + \ldots + p_u h_{u.i} = 1$ und mit der Überlegung von vorhin folgt, dass man f_i weglassen kann.

- Ergänzung zu Tafelbild 'University; Computational Commutative Algebra 1 (Algebra 2); SS 2004; 2004-07-06; 13-16':
  - $I \cap J = (\mathrm{lcm}(f,g))$, weil: $I \cap J = \left\{ h \in P \middle| h = \underbrace{a}_{\in P} f = \underbrace{b}_{\in P} g \right\}$. Dies ist die Menge **aller** gemeinsamen Vielfachen. Die muss logischer Weise durch das kleinste gemeinsame Vielfache erzeugt werden.

2004-07-08

- Ergänzungen zu Tafelbildern 'University; Computational Commutative Algebra 1 (Algebra 2); SS 2004; 2004-07-08; 02-18' bis 'University; Computational Commutative Algebra 1 (Algebra 2); SS 2004; 2004-07-08; 04-18':
  - Der zentrale Punkt ist der Ansatz $I = J \cap \tilde{J}$. Wüsste man, wie $\tilde{J}$ aussieht, so hätte man das gesuchte $Z(I)$, denn $Z(I) = Z(J) \cup Z(\tilde{J})$. Im Folgenden wird herausgefunden, dass es sich bei $\tilde{J}$ um $I:J$ handelt.
  - $J \cdot \tilde{J} \subseteq J \cap \tilde{J}$, weil:
    - Sei $J = (j_1, \ldots, j_r)$, $\tilde{J} = (\tilde{j}_1, \ldots, \tilde{j}_s)$ und $\hat{j} \in J \cdot \tilde{J}$.
    - Dann ist $\hat{j} = p_{1.1} j_1 \tilde{j}_1 + \ldots + p_{1.s} j_1 \tilde{j}_s + \ldots + p_{r.1} j_r \tilde{j}_1 + \ldots + p_{r.s} j_r \tilde{j}_s$.
    - Es gilt $\hat{j} \in J$, weil $\hat{j} = \underbrace{(p_{1.1} \tilde{j}_1)}_{\in P} j_1 + \ldots + \underbrace{(p_{1.s} \tilde{j}_s)}_{\in P} j_1 + \ldots + \underbrace{(p_{r.1} \tilde{j}_1)}_{\in P} j_r + \ldots + \underbrace{(p_{r.s} \tilde{j}_s)}_{\in P} j_r$.
    - Es gilt $\hat{j} \in \tilde{J}$, weil $\hat{j} = \underbrace{(p_{1.1} j_1)}_{\in P} \tilde{j}_1 + \ldots + \underbrace{(p_{1.s} j_1)}_{\in P} \tilde{j}_s + \ldots + \underbrace{(p_{r.1} j_r)}_{\in P} \tilde{j}_1 + \ldots + \underbrace{(p_{r.s} j_r)}_{\in P} \tilde{j}_s$.
    - Also $\hat{j} \in J \cap \tilde{J}$ und somit $J \cdot \tilde{J} \subseteq J \cap \tilde{J}$.
  - $I = J \cap (I:J)$, weil:
    - '$\subseteq$':
      - $I \subseteq J$ (siehe Tafelbild 'University; Computational Commutative Algebra 1 (Algebra 2); SS 2004; 2004-07-08; 02-18').
      - $I \subseteq I:J$, denn $I:J := \{h \in P | hJ \subseteq I\}$ und $h \in I$ ist auch Element von $\{h \in P | hJ \subseteq I\}$, denn für ein $h \in I$ und ein $j \in J$ ist auf Grund der Definition 'Ideal' auch $hj \in I$, also $hJ \subseteq I$.
      - Also $I \subseteq J \cap (I:J)$.
    - '$\supseteq$':
      - Sei $\tilde{h} \in J \cap (I:J)$, also $\tilde{h} \in J$ und $\tilde{h} \in I:J \Leftrightarrow \tilde{h}J \subseteq I$.
      - Weil $\tilde{h} \in J$ und $\tilde{h}J \subseteq I$, ist $\tilde{h} \underbrace{\tilde{h}}_{\in J} \in I$.
      - Also $\tilde{h}^2 \in I$.
      - Weil I ein Radikalideal ist, gilt $\sqrt{I} = I$. ($\sqrt{I} := \{h \in P | h^i \in I\}$)
      - Da $\tilde{h}^2 \in I$, ist $\tilde{h} \in \sqrt{I}$.
      - Weil $\tilde{h} \in \sqrt{I}$ und $\sqrt{I} = I$, ist $\tilde{h} \in I$.
- Ergänzung zu Tafelild 'University; Computational Commutative Algebra 1 (Algebra 2); SS 2004; 2004-07-08; 05-18':
  - "Für $h \in P$ muss ...": Bessere Formulierung: "Für $h \in I:(g)$ muss ..., weil

$h \in I:(g) \Leftrightarrow h(g) \subseteq I \Rightarrow hg \in I \Leftrightarrow \exists a_i : hg = a_1 f_1 + \ldots + a_s f_s$.

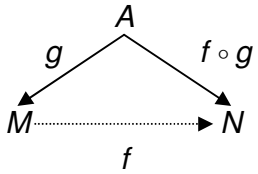
- Ergänzungen zu Tafelbild 'University; Computational Commutative Algebra 1 (Algebra 2); SS 2004; 2004-07-08; 06-18':
  - $I:(g) = (c_{1.0},\ldots,c_{r.0})$, weil die $c_{i.0}$-s in $\mathrm{Syz}(g,f_1,\ldots,f_s)$ zu g gehören, so dass $c_{i.0}g = (-c_{i.1})f_1 + \ldots + (-c_{i.s})f_s$
  - Hat man für alle $g_1,\ldots,g_t$ das zugehörige $I:(g_i) = (c_{1.0},\ldots,c_{r_i.0})_i$ berechnet, so gilt $I:J = \bigcap_{i=1}^{t} I:(g_i) = \bigcap_{i=1}^{t} (c_{1.0},\ldots,c_{r_i.0})_i$.
- Ergänzung zu Tafelbild 'University; Computational Commutative Algebra 1 (Algebra 2); SS 2004; 2004-07-08; 11-18':
  - $M:(w_i)$
  - $= \langle$erste Komponenten der Elemente des Erzeugendensystems von $\mathrm{Syz}(w_i,v_1,\ldots,v_s)\rangle$
- Ergänzungen zu Tafelbild 'University; Computational Commutative Algebra 1 (Algebra 2); SS 2004; 2004-07-08; 13-18':
  - $\mathrm{Ann}_P(M) = U:P^r$, weil:
    - Da $M \cong P^r/U$, kann man die Elemente aus M als Restklassen betrachten, also $\overline{p} \in M$ für $p \in P^r$.
    - Dann ist $\mathrm{Ann}_P(M) = \{f \in P \mid f\overline{p} = \overline{0} \forall \overline{p} \in M\} = \{f \in P \mid fp \in U \forall p \in P^r\} = \{f \in P \mid fP^r \subseteq U\} = U:P^r$.
  - $I \subseteq \mathrm{Ann}_P\left(\underbrace{M}_{=P/I}\right)$, weil:
    - $\mathrm{Ann}_P(M) = \{f \in P \mid f\overline{p} = \overline{0} \forall \overline{p} \in M\} = \{f \in P \mid \overline{fp} = \overline{0} \forall \overline{p} \in M\} = \{f \in P \mid fp \in I \forall \overline{p} \in M\}$
    - $= \{f \in P \mid fp \in I \forall p \in P\}$
    - Die letzte Gleichheit gilt, weil man zu jedem $p \in P$ ein $\overline{p} \in M$ bilden kann und man, wenn man mit den p-s ganz P durchläuft, damit dann auch alle $\overline{p} \in M$ erreicht.
    - Zu zeigen ist also, dass ein $i \in I$ auch in $\mathrm{Ann}_P(M) = \{f \in P \mid fp \in I \forall p \in P\}$ liegt.
    - Sei also $i \in I$. Dann ist $ip \in I \forall p \in P$, weil $IP \subseteq I$, weil I ein Ideal ist.
    - Also ist i auch in $\{f \in P \mid fp \in I \forall p \in P\} = \mathrm{Ann}_P(M)$.
  - Beachte: $\mathrm{Ann}_P(M)$ ist ein Ideal. Denn:
    - Zu zeigen: $P \cdot \mathrm{Ann}_P(M) \subseteq \mathrm{Ann}_P(M)$.
    - Seien $p \in P$ und $f \in \mathrm{Ann}_P(M)$. Dann ist $pf \in \mathrm{Ann}_P(M)$, weil $(pf)M = p(fM) = p \cdot 0 = 0$.
- Ergänzung zu Tafelbild 'University; Computational Commutative Algebra 1 (Algebra 2); SS 2004; 2004-07-08; 14-18':
  - Der Unterschied zwischen 'Colon-Ideal' und 'Colon-Modul ist:
    - Colon-Ideal: $\underbrace{M:\underbrace{N}_{\text{Modul}}}_{\text{Colon-Ideal}} = \left\{ \underbrace{f \in P}_{f \text{ ist Polynom}} \mid fN \subseteq M \right\}$
    - Colon-Modul: $\underbrace{M:\underbrace{I}_{\text{Ideal}}}_{\text{Colon-Modul}} = \left\{ \underbrace{\vec{f} \in P^r}_{\vec{f} \text{ ist Vektor aus Polynomen}} \mid \vec{f}I \subseteq M \right\}$

- Ergänzungen zu Tafelbild 'University; Computational Commutative Algebra 1 (Algebra 2); SS 2004; 2004-07-08; 15-18':
  - Gesucht sind alle $\vec{w} \in P^r$, so dass $\vec{w}f \in M \forall f \in I$, also alle $\vec{w} \in P^r$, so dass es eine Darstellung $\vec{w}f = h_1 v_1 + \ldots + h_s v_s$ gibt.
  - $\underbrace{\vec{w}f}_{f \cdot P^r} = \underbrace{h_1 v_1 + \ldots + h_s v_s}_{\in M} \in f \cdot P^r \cap M$
  - Jedes u_j ist von der Form $u_j = f w_j$, weil $u_j \in f \cdot P^r$.
  - $M:I$ ist dann $M:I = \bigcap_{f \in I} M:(f) = \bigcap_{i=1}^{t} M:(f_i)$
- Ergänzungen zu Tafelbild 'University; Computational Commutative Algebra 1 (Algebra 2); SS 2004; 2004-07-08; 16-18':
  - Nichtnullteiler-Probe: $f \in P$ ist NNT für $M \Leftrightarrow 0 :_M (f) = \{\vec{0}\}$, weil:
    - $0 :_M (f) = \{\vec{m} \in M \mid \vec{m}(f) \subseteq (\vec{0})\} = \{\vec{m} \in M \mid \vec{m}(f) = \vec{0}\}$
    - '$\Rightarrow$':
      - Da f NNT, gilt nur für $\vec{m} = \vec{0}$ $f\vec{m} = \vec{0}$.
      - Somit ist $\{\vec{m} \in M \mid \vec{m}(f) = \vec{0}\} = \{\vec{0}\}$
    - '$\Leftarrow$':
      - Wenn $\{\vec{m} \in M \mid \vec{m}(f) = \vec{0}\} = \{\vec{0}\}$, dann ist nur für $\vec{m} = \vec{0}$ $f\vec{m} = \vec{0}$.
      - Somit ist f NNT von M.

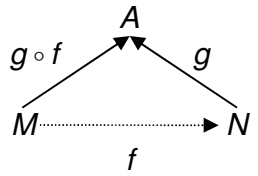
2004-07-13

- Ergänzungen zu Tafelbild 'University; Computational Commutative Algebra 1 (Algebra 2); SS 2004; 2004-07-13; 03-20':
  - $\ker(\varphi)$ soll im 1. Fall als $\tilde{U}/U$ gegeben werden. Die Definitionsmenge von φ ist P^r/U. Also ist $\tilde{U} \subseteq P^r$.
  - Analoges gilt bei $\mathrm{im}(\varphi)$
  - Unter '3' ist das Urbild einer vorgegebenen Menge gesucht.
- Ergänzungen zu Tafelbild 'University; Computational Commutative Algebra 1 (Algebra 2); SS 2004; 2004-07-13; 04-20':
  - $\left\{ \tilde{u} \in P^r \middle| \varphi\left(\underbrace{(\tilde{u} + U)}_{\in P^r/U} \right) = \underbrace{\overline{0}}_{\in P^s/V} \right\} = \{\tilde{u} \in P^r \mid \Phi(\tilde{u}) \in V\}$
  - Die w_i-s sind die von Tafelbild 'University; Computational Commutative Algebra 1 (Algebra 2); SS 2004; 2004-07-13; 02-20'. Daher auch die Beziehung zwischen Φ und φ.
  - $\Phi(\tilde{u}) = \Phi(f_1 e_1 + \ldots + f_r e_r) = \Phi(f_1 e_1) + \ldots + \Phi(f_r e_r) = f_1 \Phi(e_1) + \ldots + f_r \Phi(e_r) = f_1 w_1 + \ldots + f_r w_r$.
- Ergänzung zu Tafelbild 'University; Computational Commutative Algebra 1 (Algebra 2); SS 2004; 2004-07-13; 06-20':
  - $\tilde{V} = \langle w_1, \ldots, w_r, v_1, \ldots, v_\beta \rangle$, weil:

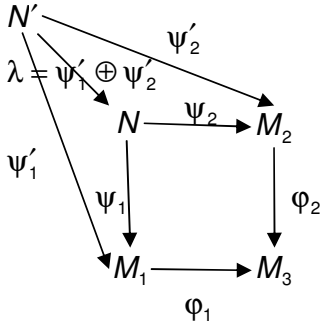
- $\mathrm{im}(\varphi) = \left\langle \underbrace{w_1}_{=\varphi(e_1+U)}, \ldots, \underbrace{w_r}_{=\varphi(e_r+U)} \right\rangle$ und $\mathrm{im}(\varphi) = \tilde{V}/V = \tilde{V}/\langle v_1, \ldots, v_\beta \rangle$
  - also: $\tilde{V} = \mathrm{im}(\varphi) + V = \langle w_1, \ldots, w_r \rangle + \langle v_1, \ldots, v_\beta \rangle = \langle w_1, \ldots, w_r, v_1, \ldots, v_\beta \rangle$
- Ergäzung zu Tafelbild 'University; Computational Commutative Algebra 1 (Algebra 2); SS 2004; 2004-07-13; 07-20':
  - Gesucht ist $\tilde{U}/U := \varphi^{-1}\left(\tilde{V}/V\right)$. Da U ja schon bekannt ist, ist also nur noch das $\tilde{U} \subseteq P^r$ gesucht.
- Ergänzungen zu Tafelbild 'University; Computational Commutative Algebra 1 (Algebra 2); SS 2004; 2004-07-13; 09-20':
  - Die Frage ist, auf was man die $e_i \in P^t$ mit Hilfe von $\overline{\psi}$ abbilden soll, damit $\varphi \circ \overline{\psi} = \psi$ ist, bei gegebenen φ und ψ.
  - Mit $\overline{\psi}(e_i) = (f_{i.1}, \ldots, f_{i.r}) + U$ ist $\overline{\psi}(e_i) = (f_{i.1}e_1 + \ldots, + f_{i.r}e_r) + U$ gemeint, also die Linearzerlegung des Bildes.
  - Es soll also sein $\varphi(\overline{\psi}(e_i)) = \psi(e_i) \Leftrightarrow \varphi((f_{i.1}e_1 + \ldots, + f_{i.r}e_r) + U) = \psi(e_i)$ und gesucht sind also die passenden $f_{i.j}$-s.
- Ergänzung zu Tafelbild 'University; Computational Commutative Algebra 1 (Algebra 2); SS 2004; 2004-07-13; 10-20':
  - Das $B = \langle w_1, \ldots, w_r, v_1, \ldots, v_\beta \rangle \subseteq P^s$ ist das $\tilde{V}$ von Tafelbild 'University; Computational Commutative Algebra 1 (Algebra 2); SS 2004; 2004-07-13; 06-20'.
- Ergänzung zu Tafelbild 'University; Computational Commutative Algebra 1 (Algebra 2); SS 2004; 2004-07-13; 12-20':
  - $Hom(A, f)$:



  - $Hom(f, A)$:

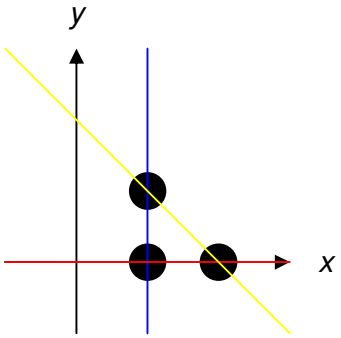


- Ergänzungen zur universelen Eigenschaft (Tafelbilder 'University; Computational Commutative Algebra 1 (Algebra 2); SS 2004; 2004-07-13; 16-20' bis 'University; Computational Commutative Algebra 1 (Algebra 2); SS 2004; 2004-07-13; 18-20'):



2004-07-15

- Ergänzung zu Tafelbild ‘University; Computational Commutative Algebra 1 (Algebra 2); SS 2004; 2004-07-15; 01-14’:
  - Ein Eliminations-Ideal ist nichts anderes als das Teilideal von *I*, das nur die Polyome aus *I* enthält, in denen die Variablen x_i aus *P* nicht vorkommen. Die entsprechenden Polynome verschwinden also.
- Ergänzung zu Tafelbild ‘University; Computational Commutative Algebra 1 (Algebra 2); SS 2004; 2004-07-15; 03-14’:
  - Definition ‘affine variety’: An affine variety over an algebraically closed field *K* is a subset of some affine space K^n over *K* which can be described as the vanishing set of finitely many polynomials in *n* variables with coefficients in *K*, and which cannot be written as the union of two smaller such sets. (http://planetmath.org/encyclopedia/AffineVariety.html)
- ‘iff’ = ‘if and only if’
- Ergänzungen zu Tafelbild ‘University; Computational Commutative Algebra 1 (Algebra 2); SS 2004; 2004-07-15; 04-14’ und ‘University; Computational Commutative Algebra 1 (Algebra 2); SS 2004; 2004-07-15; 05-14’:
  - *V* ist eine affine variety. Nach der Definition kann man hier nun Polynome in 2 Variablen finden, so dass $p_1 = (1;1)$, $p_2 = (1;0)$ und $p_3 = (2;0)$ die Elemente des vanishing sets dieser Polynome sind.
  - Diese Polynome findet man, indem man Geraden durch je 2 Punkte legt:



  - Die Geradengleichungen lauten:
    - blau: $x = 1 \Leftrightarrow x - 1 = 0$
    - rot: $y = 0$
    - gelb: $y = -x + 2 \Leftrightarrow y + x - 2 = 0$
  - Nun bildet man aus je 2 Geradengleichungen das Produkt:
    - blau-rot: $(x-1)y$
    - blau-gelb: $(x-1)(y+x-2)$
    - rot-gelb: $y(y+x-2)$
  - Ein Produkt ist = 0, wenn eine der beiden Geradengleichungen = 0 ist. Logisch ausgedrückt: Die eine **oder** die andere.
  - Also sind alle Produkte = 0 (logische **Und**-Verknüpfung; es ergibt sich der Gesamt-Ausdruck (Geradengleichung 1 = 0 oder Geradengleichung 2 = 0) und (Geradengleichung 1 = 0 oder Geradengleichung 3 = 0) und (Geradengleichung 2 = 0 oder Geradengleichung 3 = 0)), wenn mindestens 2 Geradengleichungen = 0 sind.
  - Wenn 2 Geradengleichungen = 0 sind, so gilt insbesondere, dass sie gleich sind.
  - 2 Geradengleichungen sind dort gleich, wo ihr Schnittpunkt ist.

- Die Schnittpunkte sind p_1, p_2 und p_3.
- Also sind die Polynome an diesen 3 Punkten = 0, also liegen sie im vanishing set dieser Polynome. (Man überlegt sich kurz, dass es auch keine weiteren gibt.)
- Also lässt sich die Koordinaten-Information in diese 3 Polyome codieren. Hat man die 3 Polynome, so kann man die Koordinaten-Information decodieren, indem man das vanishing set dieser 3 Polynome berechnet.
- Das nächste Ziel ist es, wenn man die Polynome gegeben hat, daraus die Polynome der projizierten Punkte zu berechnen. Aus ihnen kann man dann die Koordinaten-Information der projizierten Punkte gewinnen.
- "$q \in A^1$ is a ...":
  - Wenn $(p,q) \in Z(I)$, dann ist $(p,q) \in V$ (I wurde ja gerade so konstruiert.).
  - Da auf die y-Achse projiziert wird, fällt die erste Koordinate eines Punktes aus A^2 beim Projizieren einfach weg; es überlebt also nur das q.
- "$f \in K[y]$ is in ...":
  - Das f hat 2 Argumente (obwohl es $\in K[y]$ ist), weil das f eigentlich aus I kommt.
  - $q \in \pi(V)$ bedeutet, dass q überhaupt erstmal ein projizierter Punkt ist, dass es also einen Punkt $(p,q) \in V$ gibt, der auch tatsächlich auf q abgebildet wird. Dies sorgt dafür, dass die Bedingung $f(p,q) = 0$ nur für projizierte Punkte erfüllt sein muss; bei anderen ist es egal.
  - $(p,q) \in \pi^{-1}(q)$ bedeutet, dass (p,q) der Punkt ist, der auf q abgebildet wird, und nicht z. B. $\left(\underbrace{r}_{\neq p}, q \right)$.
- "Hence $f \in K[y]$ is ...":
  - Wenn f aus dem vanishing ideal $I(\pi(V))$ ist, dann ist f in I, weil $f(p,q) = 0$ für alle $(p,q) \in V$, und in $K[y]$, weil es das vanishing ideal aller Punkte $\underbrace{q}_{\text{hat nur eine Koordinate}} \in \pi(V)$ ist.

- Ergänzung zu Tafelbild 'University; Computational Commutative Algebra 1 (Algebra 2); SS 2004; 2004-07-15; 07-14':
  - Ein Minimalpolynom zu einer Abbildung f ist das normierte, kleinste Polynom, dass, wenn man f in dieses Polynom einsetzt, die 0-Abbildung ergibt. Insbesondere kann f natürlich auch selber ein Polynom sein.
- Ergänzung zu Tafelbild 'University; Computational Commutative Algebra 1 (Algebra 2); SS 2004; 2004-07-15; 10-14':
  - Wenn der Leitterm von f in $\hat{P}$ liegt, dann soll ganz f in $\hat{P}$ liegen.
  - Dazu müssen aber alle, also auch die kleineren Terme von f, in $\hat{P}$ liegen.
  - Also können nur größere Terme als $\mathrm{LT}(f)$ nicht in in $\hat{P}$ liegen.
  - Wenn also ein Term, der ein x_i aus Y enthält (also durch x_i teilbar ist) und somit nicht in $\hat{P}$ liegt, so muss er größer sein als alle Terme aus $\hat{P}$, denn sonst könnte man ein Polynom aus dem größeren Term (aus $\hat{P}$) und dem kleineren Term (aus Ncht-$\hat{P}$) bilden, das dann nach Definition der Elimination-Ordnung zwar in $\hat{P}$ liegen müsste, es aber offensichtlich nicht tut, denn es ist ja ein x_i aus Y enthalten.
- Ergänzung zu Tafelbild 'University; Computational Commutative Algebra 1 (Algebra 2); SS 2004; 2004-07-15; 11-14':
  - Die Terme $x_1, \ldots, x_i$ müssen also größer als die Terme $x_{i+1}, \ldots, x_n$ sein.

- Ergänzung zu Tafelbild ‘University; Computational Commutative Algebra 1 (Algebra 2); SS 2004; 2004-07-15; 14-14’:
  - $I \cap J = U \cap P$, weil:

    $f = c_1 f_1 + \ldots + c_s f_s = d_1 g_1 + \ldots + d_t g_t \quad (\Leftrightarrow f \in I \cap J)$

    $\Leftrightarrow c_1 f_1 + \ldots + c_s f_s - d_1 g_1 - \ldots - d_t g_t = 0$

    $\Leftrightarrow c_1 f_1 + \ldots + c_s f_s - d_1 g_1 - \ldots - d_t g_t + \underbrace{d_1 g_1 y + \ldots + d_t g_t y}_{=fy} = fy$

    $\Leftrightarrow c_1 f_1 + \ldots + c_s f_s + (-d_1 + d_1 y) g_1 + \ldots + (-d_t + d_t y) g_t = fy$

    $\Leftrightarrow c_1 f_1 + \ldots + c_s f_s + (-d_1) g_1 (1-y) + \ldots + (-d_t) g_t (1-y) = fy \in U$

2004-07-20

- Ergänzung zu Tafelbild ‘University; Computational Commutative Algebra 1 (Algebra 2); SS 2004; 2004-07-20; 01-19’:
  - Wäre eine der ersten *i* Komponenten von *v* ungleich 0, z. B. $v_{\underset{\leq i}{j}}$, so wäre, weil σ eine Komponenteneliminationsordnung ist, $\underbrace{\begin{pmatrix} 0 \\ \vdots \\ 0 \\ v_j \\ 0 \\ \vdots \\ 0 \end{pmatrix}}_{=t' e_j} > \underbrace{\begin{pmatrix} 0 \\ \vdots \\ 0 \\ v_\lambda \\ 0 \\ \vdots \\ 0 \end{pmatrix}}_{=te_\lambda} = \mathrm{LT}(v)$, was aber nicht sein kann, weil sonst $\begin{pmatrix} 0 \\ \vdots \\ 0 \\ v_j \\ 0 \\ \vdots \\ 0 \end{pmatrix}$ der Leitterm wäre.
- Ergänzung zu Tafelbild ‘University; Computational Commutative Algebra 1 (Algebra 2); SS 2004; 2004-07-20; 03-19’:
  - $\mathrm{LT}(g) \in F$, weil:

- $\underbrace{\begin{pmatrix} 0 \\ \vdots \\ 0 \\ t \\ 0 \\ \vdots \\ 0 \end{pmatrix}}_{=te_\lambda;\ \in F} = t'\mathrm{LT}(g)$
  - Weil t' nur ein 1-dimensionaler Term ist und $\mathrm{LT}(g)$ und ein Vektor ist, ist $\mathrm{LT}(g)$ dafür verantwortlich, in welcher Zeile der Vektor $t'\mathrm{LT}(g)$ den Eintrag hat.
  - Wegen $t'\mathrm{LT}(g) = \underbrace{\begin{pmatrix} 0 \\ \vdots \\ 0 \\ t \\ 0 \\ \vdots \\ 0 \end{pmatrix}}_{=te_\lambda;\ \in F}$ ist der Eintrag bei $\mathrm{LT}(g)$ auch in Zeile $\lambda > i$ und somit $\mathrm{LT}(g) \in F$.
- Ergänzungen zu Tafelbild 'University; Computational Commutative Algebra 1 (Algebra 2); SS 2004; 2004-07-20; 05-19':
  - $N := \left\langle \underbrace{\begin{pmatrix} \vec{v}_1 \\ -1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}}_{=:\vec{v}_1}, \ldots, \underbrace{\begin{pmatrix} \vec{v}_s \\ 0 \\ \vdots \\ 0 \\ -1 \end{pmatrix}}_{=:\vec{v}_s} \right\rangle$
  - Sei $\vec{a} = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ a_1 \\ \vdots \\ a_s \end{pmatrix} \in \tilde{N}$.
  - Dann ist

$$a_1\begin{pmatrix}\vec{v}_1\\0\\0\\\vdots\\0\end{pmatrix}+\ldots+a_s\begin{pmatrix}\vec{v}_s\\0\\\vdots\\0\\0\end{pmatrix}$$

$$=a_1\begin{pmatrix}\vec{v}_1\\-1\\0\\\vdots\\0\end{pmatrix}+\ldots+a_s\begin{pmatrix}\vec{v}_s\\0\\\vdots\\0\\-1\end{pmatrix}+a_1\begin{pmatrix}\vec{0}\\1\\0\\\vdots\\0\end{pmatrix}+\ldots+a_s\begin{pmatrix}\vec{0}\\0\\\vdots\\0\\1\end{pmatrix}$$

$$=\underbrace{\underbrace{a_1\begin{pmatrix}\vec{v}_1\\-1\\0\\\vdots\\0\end{pmatrix}}_{\in N}+\ldots+\underbrace{a_s\begin{pmatrix}\vec{v}_s\\0\\\vdots\\0\\-1\end{pmatrix}}_{\in N}+\underbrace{\begin{pmatrix}\vec{0}\\a_1\\\vdots\\\vdots\\a_s\end{pmatrix}}_{\in\tilde{N}\Rightarrow\in N}}_{\in N}$$

- Also ist $\vec{z}:=a_1\begin{pmatrix}\vec{v}_1\\0\\\vdots\\\vdots\\0\end{pmatrix}+\ldots+a_s\begin{pmatrix}\vec{v}_s\\0\\\vdots\\\vdots\\0\end{pmatrix}\in N$.
- Dann gibt es $b_1,\ldots,b_s$ mit

$$\vec{z}=\underbrace{\begin{pmatrix}z_1\\\vdots\\z_r\\0\\\vdots\\0\end{pmatrix}}_{\text{mit } s \text{ 0-en unten}}=b_1\underbrace{\begin{pmatrix}\vec{v}_1\\-1\\0\\\vdots\\0\end{pmatrix}}_{\text{Erzeuger von } N}+\ldots+b_s\underbrace{\begin{pmatrix}\vec{v}_s\\0\\\vdots\\0\\-1\end{pmatrix}}_{\text{Erzeuger von } N}=\begin{pmatrix}\vec{v}_1\\-b_1\\0\\\vdots\\0\end{pmatrix}+\ldots+\begin{pmatrix}\vec{v}_s\\0\\\vdots\\0\\-b_s\end{pmatrix}.$$

- Also sind die $b_i=0$.
- Also ist $\vec{z}=\underbrace{\begin{pmatrix}z_1\\\vdots\\z_r\\0\\\vdots\\0\end{pmatrix}}_{\text{mit } s \text{ 0-en unten}}=\vec{0}$.

- Nach Definition von $\vec{z}$ ist also $a_1 \begin{pmatrix} \vec{v}_1 \\ 0 \\ \vdots \\ \vdots \\ 0 \end{pmatrix} + \ldots + a_s \begin{pmatrix} \vec{v}_s \\ 0 \\ \vdots \\ \vdots \\ 0 \end{pmatrix} = \vec{0}$.
- Also ist $a_1\vec{v}_1 + \ldots + a_s\vec{v}_s = \vec{0}$.
- Also ist $(a_1,\ldots,a_s) \in \mathrm{Syz}(V)$.

- Ergänzungen zu Tafelbild 'University; Computational Commutative Algebra 1 (Algebra 2); SS 2004; 2004-07-20; 07-19':
  - Ergänzungen zur 2. Anwendung:
    - $\sum_{i=1}^{s} a_i \begin{pmatrix} \vec{v}_i \\ \vec{0} \end{pmatrix} + \sum_{j=1}^{t} b_j \begin{pmatrix} \vec{w}_j \\ \vec{w}_j \end{pmatrix} \in \hat{L} = L \cap \underbrace{0 \oplus \ldots \oplus 0}_{r \text{ Stück}} \oplus \underbrace{P \oplus \ldots \oplus P}_{r \text{ Stück}}$
    - Weil $u_i :=$ $\underbrace{\begin{pmatrix} 0 \\ \vdots \\ 0 \\ \hat{u}_i \end{pmatrix}}_{i\text{-ter Erzeuger von } \hat{L}}$ $\in \hat{L}$, ist auch $u_i \in L$.
    - Damit gibt es a_i und b_i mit $\sum_{i=1}^{s} a_i \begin{pmatrix} \vec{v}_i \\ \vec{0} \end{pmatrix} + \sum_{j=1}^{t} b_j \begin{pmatrix} \vec{w}_j \\ \vec{w}_j \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ \hat{u}_i \end{pmatrix}$.
    - Wegen der unteren r Zeilen ($\sum_{j=1}^{t} b_j \vec{w}_j = \hat{u}_i$) ist $\hat{u}_i \in N$.
    - Wegen der oberen r Zeilen ist $\sum_{i=1}^{s} a_i \vec{v}_i + \sum_{j=1}^{t} b_j \vec{w}_j = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} \Leftrightarrow \underbrace{\sum_{i=1}^{s} a_i \vec{v}_i}_{\in M} = -\sum_{j=1}^{t} b_j \vec{w}_j = -\hat{u}_i$, also $-\hat{u}_i$ und somit auch $\hat{u}_i \in M$.
    - Also $\hat{u}_i \in M \cap N$.
    - Die Rückrichtung (beliebiges Element aus $M \cap N$ führt zu einem $\begin{pmatrix} 0 \\ \vdots \\ 0 \\ \hat{u}_i \end{pmatrix}$-s in $\hat{L}$) lässt sich analog zeigen.
  - Ergänzungen zur 3. Anwendung:
    - $M :_P \langle w \rangle = \{h \in P \mid hw \in M\} = \left\{ h \in P \;\middle|\; \underbrace{\overline{hw} = \vec{0}}_{\text{modulo } M, \text{ also in } P^r/M} \right\} = \mathrm{Ann}_{P^r/M}(\overline{w})$

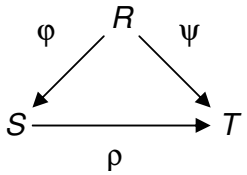
- Weil $u_i = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ f_i \end{pmatrix} \in \hat{N}$, ist auch $u_i \in N$
- Also gibt es a_i und b mit $\sum_{i=1}^{s} a_i \begin{pmatrix} \vec{v}_i \\ 0 \end{pmatrix} + b \begin{pmatrix} \vec{w} \\ 1 \end{pmatrix} = \underbrace{\begin{pmatrix} 0 \\ \vdots \\ 0 \\ f_i \end{pmatrix}}_{=u_i}$.
- Wegen der unteren Zeile ist $f_i = \underbrace{b}_{\in P} \in P$.
- Wegen den oberen r Zeilen ist $\sum_{i=1}^{s} a_i \vec{v}_i + b\vec{w} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} \Leftrightarrow b\vec{w} = -\underbrace{\sum_{i=1}^{s} a_i \vec{v}_i}_{\in M} \in M$.
- Also ist $b \in M :_{\dot{P}} \langle w \rangle$.
- Wegen $f_i = b$ ist $f_i \in M :_{\dot{P}} \langle w \rangle$.
- Die Rückrichtung (beliebiges Element aus $M :_{\dot{P}} \langle w \rangle$ führt zu einem $\begin{pmatrix} 0 \\ \vdots \\ 0 \\ f_i \end{pmatrix}$-s in $\hat{L}$) lässt sich analog zeigen.

- Ergänzungen zu Tafelbild ‘University; Computational Commutative Algebra 1 (Algebra 2); SS 2004; 2004-07-20; 09-19’:
  - $I(M)$ ist ein Ideal (und kein Untermodul), weil $I(M)$ ein Ideal des **Rings** $R \times M$ ist.
  - Man hat also einen Ring gefunden, in dem ein zum Modul M isomorphes Objekt ein Ideal ist. Man hat M gewissermaßen ‘idealisiert’.
- Ergänzungen zu Tafelbild ‘University; Computational Commutative Algebra 1 (Algebra 2); SS 2004; 2004-07-20; 13-19’:
  - $(r,s) \sim (r',s') \Leftrightarrow \frac{r}{s} = \frac{r'}{s'} \Leftrightarrow rs' = r's \Leftrightarrow r's - s'r = 0$
  - Woher das ‘s''’ kommt, ist an dieser Stelle noch nicht offensichlich.
- Ergänzung zu Tafelbild ‘University; Computational Commutative Algebra 1 (Algebra 2); SS 2004; 2004-07-20; 19-19’:
  - $M :_{P^r} (f)^{\infty} = \left(M \cdot P[y] + (fy-1) \cdot P[y]^r\right) \cap P^r$, weil:
    - Nach Satz auf Tafelbild ‘University; Computational Commutative Algebra 1 (Algebra 2); SS 2004; 2004-07-20; 17-19’ gilt $M :_{P^r} (f)^{\infty} = M_f \cap P^r$.
    - Nach Satz auf Tafelbild ‘University; Computational Commutative Algebra 1 (Algebra 2); SS 2004; 2004-07-20; 16-19’ gilt $M_f \cong P[y]/(fy-1)$.

Computational Commutative Algebra 1 – Book Notes

1.1 Polynomial Rings

- Definition 1.1.3:
  - Ein R-Algebren-Homomorphismus ist eine Abbildung $\rho: S \to T$, die, wenn man $r \in R$ und $s \in S$ hat und diese nach T konvertieren will, weil man in T rechnen will, es einem ermöglicht, r nicht erst mit $\varphi: R \to S$ in S umrechnen zu müssen, sondern r mit $\psi: R \to T$ gleich in T umrechnen zu können, die also in gewisser Hinsicht kompatibel mit ψ ist.
  - Mit anderen Worten: $\rho(\varphi(r) \cdot s) = \rho(\varphi(r)) \cdot \rho(s) = \psi(r) \cdot \rho(s)$



- Definition 1.1.4:
  - Ein Körper K hat nur die Ideale K und $\{0\}$, denn:
    - Sei $r \in I$.
    - Wegen $K \cdot I \subseteq I$ und der Existenz von r^{-1} ist auch $r^{-1}r = 1 \in I$.
    - Wieder wegen $K \cdot I \subseteq I$ und $1 \in I$ ist $K \cdot 1 \subseteq I$, also $K \subseteq I$.
    - Da sowieso $I \subseteq K$, ist $I = K$.

1.2 Unique Factorization

- Proposition 1.2.2:
  - Da in $K[x]$ jedes Ideal ein Hauptideal ist, lässt sich ein Element finden, welches das Ideal (a,f) alleine erzeugt, also $(a,f) = (e)$.
  - Weil a und f ganz offensichtlich Elemente dieses Ideals sind, müssen sie Vielfache von e sein, denn nur so kann man sie erreichen.
  - Weil f nach Voraussetzung eine Nicht-Einheit ist und K ein Körper ist, also jedes Element (außer 0) eine Einheit ist, muss f ein echtes Polynom sein.
  - Weil f irreduzibel ist, kann nur eine Zahl aus dem Körper ein Teiler von f sein – oder f.
  - f kann das Ideal nicht erzeugen, denn auch a ist in dem Ideal und a ist kein Vielfaches von f, müsste es aber sein, wenn f der Erzeuger des Ideals ist.
  - Also wird das Ideal durch eine Zahl e (ungleich 0) aus dem Körper erzeugt.
  - Weil I ein Ideal ist ($R \cdot I \subseteq I$, hier $R = K[x]$) ist auch $e^{-1}e \in I \Leftrightarrow 1 \in I$
- Lemma 1.2.11:
  - $1 = cont(f) = g \cdot cont(h)$ ausführlich:
    - $cont(f) = 1$, da f o. B. d. A primitve ist

- $cont(f) = cont\left(\underbrace{gh}_{=f}\right) \underset{\text{Gauß's Lemma}}{=} cont(g)\cdot cont(h) \underset{\substack{\text{weil } \deg(g)=0 \text{ und}\\ \text{somit } g \text{ eine Zahl ist}}}{=} g\cdot cont(h)$
  - also: $g\cdot cont(h)=1$
  - also: $cont(h)=g^{-1}$
  - Also ist g invertierbar und somit eine Einheit. Widerspruch zur Annahme, g sei keine Einheit.

1.3 Monomial Ideals and Monomial Modules

- Proposition 1.3.4:
  - Ergänzung zum Beweis 'b) $\Rightarrow$ c)': Hier sollte erstmal geklärt werden, was 'maximal' überhaupt bedeutet. 'Maximal' bedeutet nämlich nur, dass es kein größeres gibt und nicht, dass es Obermenge von allen anderen sein muss. Sehe auch Tafelbild 'University; Computational Commutative Algebra 1 (Algebra 2); SS 2004; 2004-05-13; 01-10'.
  - Ergänzung zum Beweis 'c) $\Rightarrow$ a)': Angenommen, das maximale Element (nenne es $\tilde{\Delta}$) der erwähnten Menge von Monoidealen ist nicht Δ. Dann gibt es ein Element δ, das in Δ, aber nicht in $\tilde{\Delta}$ liegt. Nehme dieses Element zur endlichen Erzeugermenge von $\tilde{\Delta}$ hinzu und erhalte eine neue Erzeugermenge, die ein Ideal erzeugt, das echt größer als $\tilde{\Delta}$ ist und dennoch durch eine endliche Teilmenge von Elementen aus Δ erzeugt wird, also in der erwähnten Menge von Monoidealen liegt. Doch dann ist $\tilde{\Delta}$ nicht mehr das maximale, denn dieses ist ja größer. Widerspruch. Also ist Δ das maximale Element und somit endlich erzeugt.
- Proposition 1.3.5:
  - Ergänzung zu '$n=1$': Jedes Monoideal ist von der Form (a), denn: Betrachte z. B. das Monoideal $(8,12,15)$. Da die Operation '+' ist und in N die Zahl 1 liegt, gilt für das Monoideal (8), dass $(8)=\{8,9,10,\ldots\}$, denn es muss ja gelten $8+n\in(8)\forall n\in \mathrm{N}$ (siehe Definition 'Monoideal'). Also sind auch $12,15\in(8)$ und somit $(8)=(8,12,15)$.
  - Ergänzungen zu '$n>1$':
    - Die Kette $\begin{pmatrix} v_{1.1}\\ v_{1.2}\\ \vdots\\ v_{1.n}\end{pmatrix}\subseteq\begin{pmatrix} v_{1.1} & v_{2.1}\\ v_{1.2} & v_{2.2}\\ \vdots & \vdots\\ v_{1.n} & v_{2.n}\end{pmatrix}\subseteq\ldots$ wird letztendlich stationär, weil die Kette $\begin{pmatrix} v_{1.2}\\ \vdots\\ v_{1.n}\end{pmatrix}\subseteq\begin{pmatrix} v_{1.2} & v_{2.2}\\ \vdots & \vdots\\ v_{1.n} & v_{2.n}\end{pmatrix}\subseteq\ldots$ nach Induktionsvoraussetzung letztendlich stationär wird und weil die ersten Komponenten $v_{1.1},v_{2.1},\ldots$ nicht fallend sind, also gilt $v_{1.1}\le v_{2.1}\le\ldots$. Wie oben erläutert, gilt dann $(v_{1,1})=(v_{1,1},v_{2,1})=\ldots$, weil die Operation ja '+' ist und $v_{1.1}$ die kleinste Zahl ist. Mit $\begin{pmatrix} v_{1.2}\\ \vdots\\ v_{1.n}\end{pmatrix}\subseteq\begin{pmatrix} v_{1.2} & v_{2.2}\\ \vdots & \vdots\\ v_{1.n} & v_{2.n}\end{pmatrix}\subseteq\ldots$ gilt dann

insgesamt $\begin{pmatrix} v_{1.1} \\ v_{1.2} \\ \vdots \\ v_{1.n} \end{pmatrix} \subseteq \begin{pmatrix} v_{1.1} & v_{2.1} \\ v_{1.2} & v_{2.2} \\ \vdots & \vdots \\ v_{1.n} & v_{2.n} \end{pmatrix} \subseteq \ldots.$

- $v_i = w_{m_i} \notin (w_1,\ldots,w_{m_{i-1}}) \supseteq (v_1,\ldots,v_{i-1})$:
  - $v_i = w_{m_i}$: nach Definition
  - $w_{m_i} \notin (w_1,\ldots,w_{m_{i-1}})$:
    - Angenommen $w_{m_i} \in (w_1,\ldots,w_{m_{i-1}})$.

      $w_{m_i} \in \left(\underbrace{w_1}_{\in \Delta_{n_2} \setminus \Delta_{n_1}}, \ldots, \underbrace{w_{m_{i-1}}}_{\in \Delta_{n_{m_{i-1}+1}} \setminus \Delta_{n_{m_{i-1}}}} \right)$

      $\Rightarrow w_{m_i} \in \Delta_{n_{m_{i-1}+1}}$
    - $\Rightarrow w_{m_i} \in \Delta_{n_{m_{i-1}+1}} \subseteq \ldots \subseteq \Delta_{n_{m_i}}$

      $\Rightarrow w_{m_i} \in \Delta_{n_{m_i}}$

      $\Rightarrow w_{m_i} \notin \Delta_{n_{m_i+1}} \setminus \Delta_{n_{m_i}}$
    - Aber w_{m_i} wurde so gewählt, dass $w_{m_i} \in \Delta_{n_{m_i+1}} \setminus \Delta_{n_{m_i}}$. Widerspruch.
  - $(w_1,\ldots,w_{m_{i-1}}) \supseteq (v_1,\ldots,v_{i-1})$: weil $\{v_1,\ldots,v_{i-1}\} \subseteq \{w_1,\ldots,w_{m_{i-1}}\} = \left\{ w_1,\ldots,\underbrace{w_{m_1}}_{=v_1},\ldots,\underbrace{w_{m_{i-1}}}_{=v_{i-1}} \right\}$
  - Der Widerspruch ist nun, dass $v_i = w_{m_i} \notin (w_1,\ldots,w_{m_{i-1}}) \supseteq (v_1,\ldots,v_{i-1})$, also insbesondere $v_i \notin (v_1,\ldots,v_{i-1})$ für alle *i*. Der Widerspruch liegt darin, dass, wie eben gezeigt $(v_1) \subseteq (v_1,v_2) \subseteq \ldots$ irgendwann stationär wird; mit anderen Worten $(v_1) \subseteq (v_1,v_2) \subseteq \ldots \subseteq (v_1,v_2,\ldots,v_{i-1}) = (v_1,v_2,\ldots,v_{i-1},v_k) = \ldots.$ Dann gibt es aber ein *i*, so dass $v_i \in (v_1,v_2,\ldots,v_{i-1})$ im Widerspruch zu '$v_i \notin (v_1,\ldots,v_{i-1})$ für alle *i*'.
- Corollary 1.3.6 (Dickson's Lemma):
  - Die interessante Aussage ist, dass die Aussage nicht nur für Monoideale, die eine echte Teilmenge von T^n sind, gilt, sondern auch für das **Monoideal** T^n selbst.
  - Damit ist auch ganz das **Ideal** $R[x_1,\ldots,x_n]$ durch das endliche Erzeugendensystem von T^n erzeugt, weil man hier zusätzlich die Operation '+' hat und sich jedes Polynom in $R[x_1,\ldots,x_n]$ als Summe von Termen (= Monomen), die ja aus T^n kommen, schreiben lässt. Weil es ein endliches Erzeugendsystem für T^n gibt, kann man jeden Term erzeugen. Weil es '+' gibt, kann man sie so aneinander reihen, dass man die Darstellung für das darzustellende Polynom erzeugen kann.

1.4 Term Orderings

- Definition 1.4.7:
  - $t_1 \geq_{\text{DegRecLex}} t_2$, wenn $\deg(t_1) > \deg(t_2)$ oder wenn in t_1 weniger 'kleine' Variablen vorkommen als in t_2.
  - So ist $x_1x_2 > x_1x_3$, weil zwar $\deg(x_1x_2) = \deg(x_1x_3)$, aber die kleine Variable x_3 in

x_1x_2 0-mal vorkommt, aber in $x_1x_2 > x_1x_3$ 1-mal.

- analog $x_1^2x_2 > x_1x_2^2$, weil die hier kleine Variable x_2 in $x_1^2x_2$ nur 1-mal vorkommt, aber in $x_1x_2^2$ 2-mal.

1.5 Leading Terms

- Theorem 1.5.7 (Macaulay's Basis Theorem):
  - siehe Tafelbilder ab 'University; Computational Commutative Algebra 1 (Algebra 2); SS 2004; 2004-05-11; 14-20'
  - Ergänzung zum Beweis der linearen Unabhängigkeit: Hier steht $\sum_{i=1}^{s} c_i m_i \in M$ und nicht $\sum_{i=1}^{s} c_i m_i = 0$ (der 'normale' Ansatz zum Beweis der linearen Unabhängigkeit), weil M die Restklasse $\overline{0}$ ist.
- Proposition 1.5.10 und 1.5.11:
  - Der Unterschied zwischen $R[x_i,\ldots,x_n]$ und $(x_i,\ldots,x_n)$ ist, dass in $R[x_i,\ldots,x_n]$ nur die Polynome (hier kommt es aber nur auf die Monome an) sind, die nur aus $x_i,\ldots,x_n$ bestehen, während in Polynomen in $(x_i,\ldots,x_n)$ auch die Variablen $x_1,\ldots,x_{i-1}$ vorkommen können ($R[x_1,\ldots,x_n]\cdot I \subseteq I$). Das Besondere an Polynomen in $(x_i,\ldots,x_n)$ ist, dass in jedem ihrer Monome jedoch mindestens eine der Variablen aus $x_i,\ldots,x_n$ liegen muss.

1.6 The Division Algorithm

- Example 1.6.6: $x_1 - x_2 = (2x+1)-(x_1+x_2+1) \in (g_1,g_2)$, weil:
  $\underbrace{(x_1+x_2)g_1+g_2+(x_1+x_2+1)}_{=f} = \underbrace{x_1g_1+(x_1+1)g_2+(2x_1+1)}_{=f}$
  $\Leftrightarrow (x_1+x_2)g_1+g_2-x_1g_1-(x_1+1)g_2 = (2x_1+1)-(x_1+x_2+1)$
  $\Leftrightarrow x_2g_1 - x_1g_2 = x_1 - x_2$
  Es gibt also eine Linearkombination von g_1 und g_2, also $x_1 - x_2 \in (g_1,g_2)$

1.7 Gradings

- Definition 1.7.6.b:
  - Mit $F := \bigoplus_{i\in I} R(\gamma_i)$ ist gemeint: $I = \{1,\ldots r\}$, $F = R^r$ und die Graduierung der i-ten Komponente eines Polynomvektors aus F ist um γ_i verschoben bzgl. der Standard-Graduierung.
  - quasi: $F = \begin{pmatrix} R(\gamma_1) \\ \vdots \\ R(\gamma_r) \end{pmatrix}$

- also ist z. B. $\deg\left(\underbrace{\begin{pmatrix}0\\\vdots\\0\\1\\0\\\vdots\\0\end{pmatrix}}_{=\tilde{e}_i}\right)=\deg\left(1_{R(\gamma_i)}\right)=0+\left(-\gamma_i\right)=-\gamma_i$

- Definition 1.7.8: Der Sinn dieser Definition ist der folgende: Man hat nun Grade für bestimmte Elemente von Moduln definiert (z. B. $\deg\left(\underbrace{\begin{pmatrix}0\\2x_1^2x_2\\0\\0\end{pmatrix}}_{\in P^4}\right)=\underbrace{\left(x_1^2x_2\right)}_{\in T^2}\underbrace{\begin{pmatrix}0\\1\\0\\0\end{pmatrix}}_{=e_2}\hat{=}\underbrace{\begin{pmatrix}2\\1\end{pmatrix}}_{\in N^2}\underbrace{\begin{pmatrix}0\\1\\0\\0\end{pmatrix}}_{=e_2}$). Einige Elemente haben jedoch keinen direkten Grad (z. B. $\begin{pmatrix}0\\2x_1^2x_2\\x_1\\0\end{pmatrix}$), da sie Summe aus 2 Elementen sind, die jedoch dann wieder direkt einen Grad haben (z. B. $\begin{pmatrix}0\\2x_1^2x_2\\x_1\\0\end{pmatrix}=\begin{pmatrix}0\\2x_1^2x_2\\0\\0\end{pmatrix}+\begin{pmatrix}0\\0\\x_1\\0\end{pmatrix}$) und die selber Elemente dieses Moduls sind, also nicht 'außerhalb' liegen ($M=\bigoplus_{s\in\Sigma}M_s$). Dasselbe möchte man jetzt auf Submoduln dieser Moduln übertragen. Dazu sind aber nicht alle Submoduln geeignet, weil ihre erzeugenden Elemente keinen direkten Grad haben (z. B. das Ideal $I:=(x-1)$) und nur im Modul selbst, nicht aber im Submodul in Komponenten mit eigenem Grad zerfallen ($I\cap P_d=(0)$ für alle Grade d). Diese möchte man nicht betrachten. Stattdessen möchte man nur Submoduln betrachten, die diesbezüglich abgeschlossen sind, das heißt deren Elemente im Submodul selber in homogene Komponenten zerfallen ($N=\bigoplus_{s\in\Sigma}(N\cap M_s)$. Solche Submoduln werden also aus Elementen erzeugt, die im Submodul selber liegen und auch direkt einen Grad haben (denn sie liegen in N **und** in M_s). Solche Submoduln sind geeignet um das Grad-Framework für Moduln auf sie zu übertragen, denn jedes Element aus ihnen zerfällt in Elemente, die direkt einen Grad haben und auch im Submodul liegen. Falls der Submodul ein Ideal ist (also $M=R^1$ und $N=I$), so verdient es den Namen 'homogenes Ideal' weil es aus Elementen erzeugt wird, die direkt einen Grad haben, die also homogene Komponenten sind.
- Remark 1.7.9:
  - Verdeutlichung der Definition $(M/N)_s:=M_s/N_s$ am Beispiel $M:=R[x]$ und $N:=(x^2)$
  - Dann haben die Elemente in M/N das Aussehen a_1x+a_0.

- Es ist $M_0 = \{a_0 | a_0 \in R\}$, $M_1 = \{a_1 x | a_1 \in R\}$, ..., $N_0 = \{\}$, $N_1 = \{\}$, $N_2 = \{a_2 x^2 | a_2 \in R\}$, ..., $(M/N)_0 = \{a_0 | a_0 \in R\} = M_0 / N_0$, $(M/N)_1 = \{a_1 x | a_1 \in R\} = M_1 / N_1$, $(M/N)_2 = \{\} = M_2 / N_2$.
- Proposition 1.7.10: Beim Beweis von 'c) $\Rightarrow$ a)' stellt man sich am besten R als den Polynomring (über einem weiteren Ring) vor. Dann wird klar, warum die r_β-s erst noch in ihre homogenen Komponenten zerlegt werden müssen.
- Korollar 1.7.11: $\sum_{\beta \in B} a_\beta' n_\beta - n$ muss gleich 0 sein, weil: n ist homogen vom Grad s. a_β' ist der einzige Anteil von a_β, so dass $\deg\left(a_\beta' n_\beta\right) = s$. Mit anderen Worten: Alle in a_β'' zusammengefassten Komponenten von a_β führen dazu, dass $\deg\left(a_{\beta\,i}'' \cdot n_\beta\right) \neq s$, wobei $a_{\beta\,i}''$ eine dieser Komponenten ist. Betrachte nun $0 = \left(\sum_{\beta \in B} a_\beta' n_\beta - n\right) + \sum_{\beta \in B} a_\beta'' n_\beta$. Wegen der Unterschiedlichen Grade kein Summand in $\sum_{\beta \in B} a_\beta'' n_\beta$ den Teil $\left(\sum_{\beta \in B} a_\beta' n_\beta - n\right)$ wegkürzen. Da aber trotzdem insgesamt 0 rauskommt, muss $\sum_{\beta \in B} a_\beta' n_\beta - n = 0$ sein. Damit ist $n = \sum_{\beta \in B} a_\beta' n_\beta$.
- Proposition 1.7.12:
  - Nach Definition gilt: P ist Primideal $:\Leftrightarrow (fg \in P; f, g \in R \Rightarrow f \in P \vee g \in P)$.
  - Es ist also zu zeigen: $(fg \in P; f, g \in R \Rightarrow f \in P \vee g \in P) \Leftrightarrow (fg \in P; f, g \in R \text{ und homogen} \Rightarrow f \in P \vee g \in P)$, wobei P zusätzlich ein homogenes echtes Ideal in R ist.
  - Im folgenden Beweis wird folgendes Lemma benutzt: Sei I ein homogenes Ideal und $f = f_{\gamma_1} + \ldots + f_{\gamma_s}$ die Decomposition von f in homogene Komponenten in R. Dann gilt: $f \in I \Leftrightarrow \forall i : f_{\gamma_i} \in I$.:
    - '$\Leftarrow$': Klar. Gilt wegen der Abgeschlossenheit von Idealen bzgl. '+'. (Gilt auch bei nicht homogenen Idealen.)
    - '$\Rightarrow$': Weil I homogen ist, gilt nach Definition von 'homogenes Ideal': $I = \bigoplus_{\gamma \in \Gamma} \underbrace{I \cap R_\gamma}_{=: I_\gamma}$.

      Also gibt es eine Decomposition von f in I. Weil $I \subseteq R$ ist und die Decomposition eindeutig ist, muss die Decomposition von f in I die gleiche wie in R sein. Also liegen alle f_{γ_i} nicht nur in R_{γ_i}, sondern auch in I_{γ_i}. Weil $I_{\gamma_i} \subseteq I$ ist (wegen $I_{\gamma_i} = I \cap R_{\gamma_i}$), liegen die f_{γ_i}-s also auch in I, was zu zeigen war.
  - '$\Rightarrow$': Klar. Wenn $fg \in P; f, g \in R \Rightarrow f \in P \vee g \in P$ für beliebige f, g gilt, dann erst recht für homogene.
  - '$\Leftarrow$':
    - Annahme, es gilt $(fg \in P; f, g \in R \text{ und homogen} \Rightarrow f \in P \vee g \in P)$ und $fg \in P; f, g \in R$, aber nicht $f \in P \vee g \in P$. Dann gilt $f \notin P \wedge g \notin P$.
    - Seien $f = f_{\gamma_1} + \ldots + f_{\gamma_s}$ und $g = g_{\gamma_1} + \ldots + g_{\gamma_s}$, wobei $\gamma_1 < \ldots < \gamma_s$

- Laut dem Lemma gilt (setze $I = P$) $f \notin P \Leftrightarrow \exists \tilde{i} : f_{\gamma_{\tilde{i}}} \notin P$ und analog $g \notin P \Leftrightarrow \exists \tilde{j} : g_{\gamma_{\tilde{j}}} \notin P$.
- Wähle aus den $f_{\gamma_{\tilde{i}}} \notin P$ bzw. $g_{\gamma_{\tilde{j}}} \notin P$ jeweils die beiden mit kleinstem Grad aus: $f_{\gamma_i} \notin P$ bzw. $g_{\gamma_j} \notin P$. (Mit anderen Worten: $\forall \gamma_{\tilde{i}} \neq \gamma_i : \gamma_i < \gamma_{\tilde{i}}$. Analoges für bei den g-s.)
- In $fg = (f_{\gamma_1} + \ldots + f_{\gamma_s})(g_{\gamma_1} + \ldots + g_{\gamma_s})$ taucht der Summand $f_{\gamma_i} g_{\gamma_i}$ auf. Dieser hat Grad $\gamma_i + \gamma_j$. Es können aber noch andere Summanden diesen Grad haben.
- Die Summe genau der Summanden mit Grad $\gamma_i + \gamma_j$ ist die homogene Komponente $(fg)_{\gamma_i+\gamma_j}$ vom Grad $\gamma_i + \gamma_j$ vom Element fg. Die Summe/ homogene Komponente sieht so aus: $(fg)_{\gamma_i+\gamma_j} = f_{\gamma_i} g_{\gamma_i} + \sum_{\{(k,l)|(k,l)\neq(i,j)\wedge\gamma_k+\gamma_l=\gamma_i+\gamma_j\}} f_{\gamma_k} g_{\gamma_l}$.
- Die Summanden von $\sum_{\{(k,l)|(k,l)\neq(i,j)\wedge\gamma_k+\gamma_l=\gamma_i+\gamma_j\}} f_{\gamma_k} g_{\gamma_l}$ liegen alle in P, denn:
  - Es muss $\gamma_k < \gamma_i$ oder $\gamma_l < \gamma_j$ gelten, denn wären beide größer, dann wäre auch ihre Summe $\gamma_k + \gamma_l > \gamma_i + \gamma_j$, doch die Summe läuft über $\left\{(k,l)\middle|(k,l) \neq (i,j) \wedge \gamma_k + \gamma_l \overset{!}{=} \gamma_i + \gamma_j\right\}$.
  - Da γ_i und γ_j jeweils minimal gewählt wurden, so dass $f_{\gamma_i} \notin P$ bzw. $g_{\gamma_j} \notin P$, liegt f_{γ_k} oder g_{γ_l} in P (je nachdem, ob $\gamma_k < \gamma_i$ oder $\gamma_l < \gamma_j$).
  - Da P ein Ideal ist und somit gilt $R \times P \subseteq P$, liegt der Summand $f_{\gamma_k} g_{\gamma_l}$ auf jeden Fall in P, da ja f_{γ_k} oder g_{γ_l} in P liegt.
- Da jeder Summand von $\sum_{\{(k,l)|(k,l)\neq(i,j)\wedge\gamma_k+\gamma_l=\gamma_i+\gamma_j\}} f_{\gamma_k} g_{\gamma_l}$ in P liegt, liegt auch die ganze Summe in P.
- Wende nun wieder das Lemma an: Weil $fg \in P$, ist auch jede homogene Komponente in P, insbesondere $(fg)_{\gamma_i+\gamma_j}$.
- $(fg)_{\gamma_i+\gamma_j} = f_{\gamma_i} g_{\gamma_i} + \sum_{\{(k,l)|(k,l)\neq(i,j)\wedge\gamma_k+\gamma_l=\gamma_i+\gamma_j\}} f_{\gamma_k} g_{\gamma_l} \Leftrightarrow f_{\gamma_i} g_{\gamma_i} = \underbrace{\underbrace{(fg)_{\gamma_i+\gamma_j}}_{\in P} - \underbrace{\sum_{\{(k,l)|(k,l)\neq(i,j)\wedge\gamma_k+\gamma_l=\gamma_i+\gamma_j\}} f_{\gamma_k} g_{\gamma_l}}_{\in P}}_{\in P, \text{ wegen Abgeschlossenheit von } P \text{ bzgl. '+'}}$
- Also ist $f_{\gamma_i} g_{\gamma_i} \in P$.
- Wegen der Voraussetzung '$fg \in P; f, g \in R$ und homogen $\Rightarrow f \in P \vee g \in P$' folgt jetzt also $f_{\gamma_i} \in P$ oder $g_{\gamma_i} \in P$. (Setze hier $f = f_{\gamma_i}$ und $g = g_{\gamma_i}$.)
- Aber f_{γ_i} und g_{γ_j} waren ja beide nicht in P.
- Also hat die anfängliche Annahme '$f \notin P \wedge g \notin P$' zu einem Widerspruch geführt und muss daher falsch gewesen sein. Somit gilt das Gegenteil $f \in P \vee g \in P$ und somit
  $(fg \in P; f, g \in R \Rightarrow f \in P \vee g \in P) \Leftarrow (fg \in P; f, g \in R \text{ und homogen} \Rightarrow f \in P \vee g \in P)$.

- Proposition 1.7.15 (Nakayama's Lemma):
  - Es reicht $M_2 \subseteq M_1$ zu zeigen, weil nach Voraussetzung bereits $M_2 \supseteq M_1$ gilt.

- Angenommen, $M_2 \subseteq M_1$ gilt nicht.
- Dann gibt es in $M_2 \setminus M_1$ ein homogenes Element, weil:
  - Zunächst einmal gibt es ein Element, weil ja angenommen wird, dass $M_2 \not\subseteq M_1$.
  - Weil M_1 und M_2 Σ-graded sind, lässt sich nach Definition jedes Element aus M_1 bzw. M_2 eindeutig in homogene Elemente, die ebenfalls in M_1 bzw. M_2 liegen, decomposen.
  - Sei nun $\tilde{m} \in M_2 \setminus M_1$ ein (nicht notwendiger Weise homogenes) Element, z. B. $x+1$. (Beachte: $\tilde{m} \in M_2 \setminus M_1 \Rightarrow \tilde{m} \in M_2$.)
  - Dann ist zumindest eine homogene Komponente von $\tilde{m}$ nicht in M_1, denn wären alle homogenen Komponenten von $\tilde{m}$ in M_1, so wäre auch $\tilde{m} \in M_1$, denn $\tilde{m}$ ist ja die Summe seiner homogenen Komponenten.
  - Wenn aber $\tilde{m} \in M_1$, dann kann $\tilde{m}$ nicht in $M_2 \setminus M_1$. Widerspruch.
  - Wähle m als die homogene Komponente von $\tilde{m}$, die nicht in M_1 liegt. Noch zu zeigen: m ist in M_2.
  - Dies ist der Fall, denn $\tilde{m}$ lässt sich in nicht in M_2 decomposen und m ist ja eine homogene Komponente von $\tilde{m}$.
- Weil M_2 Σ-graded ist und $m \in M_2$ ist, lässt sich m nach Corollary 1.7.11 schreiben als $m = \sum_{\beta \in B} r_\beta n_\beta$, wobei $r_\beta \in R$ und $n_\beta \in M_2$ homogene Erzeuger von M_2 und $\deg(r_\beta) * \deg(n_\beta) = \underbrace{\deg(m)}_{=:s}$.
- Betrachte nun den Teil der Summe, mit $\deg(r_\beta) > 0$ (also $r_\beta \in R_+$). Dann ist $m = m' + \sum_{\beta \in B \mid \deg(r_\beta) > 0} r_\beta n_\beta$ mit einem passenden m', dass die Komponenten mit $\deg(r_\beta) = 0$ enthält.
- Wegen $\deg(r_\beta) * \deg(n_\beta) = \deg(m)$ und $\deg(r_\beta) > 0$ ist $\deg(n_\beta) < \deg(m)$.
- Weil m minimalen Grad in $M_2 \setminus M_1$ hatte, können die n_β-s nicht in $M_2 \setminus M_1$ liegen. Weil alle $n_\beta \in M_2$ müssen alle n_β-s auch in M_1 liegen.
- Es ist $\underbrace{m}_{\in M_2} = m' + \underbrace{\sum_{\beta \in B \mid \deg(r_\beta) > 0} \underbrace{r_\beta}_{\in R_+} \underbrace{n_\beta}_{\in M_2}}_{\in R_+ M_2}$. Da $M_2 \subseteq M_1 + R_+ M_2$, besitzt im Besonderen m eine entsprechende Darstellung, das bedeutet, dass man von $m' \in M_1$ ausgehen kann.
- Da außerdem $\underbrace{\underbrace{\sum_{\beta \in B \mid \deg(r_\beta) > 0} \underbrace{r_\beta}_{\in R_+} \underbrace{n_\beta}_{\in M_1}}_{\in M_1, \text{ weil } M_1 \text{ ein Modul ist und somit } R \cdot M_1 \subseteq M_1}}_{\in M_1 \text{ wegen der Abgeschlossenheit von } M_1 \text{ bzgl. '+'}}$, gilt $m = \underbrace{\underbrace{m'}_{\in M_1} + \underbrace{\sum_{\beta \in B \mid \deg(r_\beta) > 0} r_\beta n_\beta}_{\in M_1}}_{\in M_1}$, also $m \in M_1$.
- Dies ist ein Widerspruch, denn wenn $m \in M_1$, kann m nicht in $M_2 \setminus M_1$ liegen, was aber Voraussetzung gewesen ist.
- Also ist $M_2 \setminus M_1$ leer und damit $M_2 \subseteq M_1$.

- Corollary 1.7.16:
  - a):
    - $M \subseteq N + R_+ \cdot M$, weil:

- $\overline{m_i}$ steht für eine Restklasse, nämlich für Menge der Vektoren $m_i + R_+ \cdot M$
- Dann erzeugt $\{m_1,\ldots,m_s\}$ die Menge der Vektoren $N + R_+ \cdot M$. (Daher kommt also '$N + R_+ \cdot M$'.)
- Es gilt nun '$M \subseteq N + R_+ \cdot M$', weil zu *jedem* $m \in M$ seine Restklasse $\overline{m} \in M / R_+ \cdot M$ gebildet werden kann. Weiterhin kann jedes Element aus $M / R_+ \cdot M$ (also insbesondere die $\overline{m}$-s) in eine Menge von Vektoren, nämlich $m + R_+ \cdot M$ verwandelt werden. Insgesamt findet man also *jedes* $m \in M$ in ein $N + R_+ \cdot M$ wieder.

- b):
  - Die entscheidende Frage ist: Warum ist $M/(R_+ \cdot M)$ ein R_0-Modul?:
    - Wie bei einem Vektorraum, hat ein 'Vektor' eines Moduls die Form $\vec{v} = \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix}$, wobei die Komponenten v_i aus dem zu Grunde liegenden Ring sind.
    - Damit $M/(R_+ \cdot M)$ ein R_0-Modul ist, müssen also die Komponenten in R_0 liegen.
    - Dies ist auch der Fall, denn durch '$/(R_+ \cdot M)$' werden in jeder Komponente gerade die Teile, die in $R_1, R_2, \ldots$ liegen, herausgeschnitten, weil sie in der Restklasse $\overline{0}$ liegen. Nur die, die in R_0 liegen, bleiben übrig.
    - Beispiel: $\begin{pmatrix} x^2 \\ x+1 \\ 2x+3 \end{pmatrix}$ wird durch '$/(R_+ \cdot M)$' zu $\begin{pmatrix} \overline{0} \\ \overline{1} \\ \overline{3} \end{pmatrix}$.

2. Gröbner Bases

- "Suppose a vector ...": $g \xrightarrow{g_i} \tilde{g} \Rightarrow g$ und $\tilde{g}$ sind modulo M in derselben Äquivalenzklasse, weil: $\tilde{g} = g - \underbrace{t \underbrace{g_i}_{\in M}}_{\in M} \Leftrightarrow \underbrace{t g_i}_{\in M} = g - \tilde{g} \Rightarrow g - \tilde{g} \in M \Leftrightarrow$ g und $\tilde{g}$ sind modulo M in derselben Äquivalenzklasse.

2.1 Special Generation

- Proposition 2.1.1: Hier ist $M = \langle g_1,\ldots,g_s \rangle$ (siehe Tafelbilder 'University; Computational Commutative Algebra 1 (Algebra 2); SS 2004; 2004-05-25; 10-14' und 'University; Computational Commutative Algebra 1 (Algebra 2); SS 2004; 2004-05-25; 11-14').
- Proposition 2.1.3:
  - $A_2 \Rightarrow B_1$, weil:
  - B_1 bedeutet, dass jeder Leitterm aus M sich darstellen lässt durch $t \cdot g_i$, wobei t ein Monom ist.
  - A_2 sagt aus, dass der Leitterm jedes Elements aus M (also jeder Leitterm von M)

gleich dem $\max\{LT(f_i g_i)\}$ ist, wobei f_i ein Polynom ist.

- Nun ist aber $LT(f_i g_i) = \underbrace{LT(f_i)}_{=:t_i} \cdot LT(g_i)$ (laut Proposition 1.5.3.d).
- Also $\max\{LT(f_i g_i)\} = \max\{t_i \cdot LT(g_i)\} = t \cdot LT(g_i)$, wobei t eines der t_i-s und somit ein Monom ist.
- Dies ist genau die Aussage von B_1.

2.2 Rewrite Rules

- Erläuterungen zur Einleitung:
  - Fernziel der Computeralgebra ist ja im Moment in M/U rechnen zu können.
  - Die Elemente in M/U haben die Form $\overline{m} = m + U$ und für zwei Elemente aus M/U gilt: $\overline{m_1} = \overline{m_2} \Leftrightarrow m_1 \equiv m_2 \bmod U$.
  - Wenn nun $M = P$ (oder auch $M = P^r$) und $U = \langle g_1,\ldots,g_s \rangle$ ist (Stichwort: Polynome), möchten wir für jedes Polynom $f \in M$ (oder auch Polynomvektor) einen 'schönen' Representanten finden, also einen, in dem keine Vielfachen von $g_1,\ldots,g_s$ mehr drin stecken.
  - Eine Methode wäre der Divisionsalgorithmus aus Kapitel 1.6, der ja nach jedem Zwischenschritt folgendes liefert:

    $f : g_i = \underbrace{\underbrace{h_1}_{\text{Monom}} + \ldots + h_t}_{=:h} + \underbrace{Rest}_{=f \bmod g_i}$

    $\underline{-h_1 g_i}$

    $f - h_1 g_i$

    $\vdots$

    $\underline{-h_t g_i}$

    $\underbrace{Rest}_{\substack{=f \bmod g_i \\ =f-hg_i}}$

    wobei der entstandene Rest $f - hg_i$ modulo g_i in der selben Restklasse wie f liegt (d. h./ denn: $\underbrace{f \bmod g_i}_{=f-hg_i,\ \text{s. o.}} = \underbrace{f - hg_i \bmod g_i}_{=f-hg_i,\ \text{weil } f-hg_i \text{ sich ja nicht mehr durch } g_i \text{ teilen lässt}}$), aber schon etwas weniger von den g_i-s enthält als f, also ein schönerer Representant ist.
  - Man stellt jedoch, wenn man einige Beispiele durchrechnet, fest, dass der entstehende Rest $f - hg_i$ immer ein bestimmtes Aussehen hat, welches man, wenn man aus f und g_i direkt angeben kann, ohne den Divisionsalgorithmus benutzen zu müssen.:

    $\overbrace{(x^4 + x^3 - x^2 + 1)}^{=:f} : \overbrace{(x^2 - x + 1)}^{=:g} = x^2 + 2x \text{ Rest } : \underbrace{-2x + 1}_{=f \bmod g}$

    $\underline{-(x^4 - x^3 + x^2)}$

    - $2x^3 - 2x^2 + 1$

      $\underline{-(2x^3 - 2x^2 + 2x)}$

      $-2x + 1$

- Schreibt man nun statt '$x^2 - x + 1$' '$\underbrace{x^2}_{=:a} - \underbrace{(x-1)}_{=:b}$', so stellt man fest, dass man den Rest $-2x+1$ gleich kriegen kann, indem man in f 'x^2' **wiederholt** durch '$(x-1)$' ersetzt:

  $x^4 + x^3 - x^2 + 1 \to (x-1)^2 + (x-1)x - (x-1) + 1$

  $= x^2 - 2x + 1 + x^2 - x - x + 1 + 1$

  $= 2x^2 - 4x + 3 \to 2(x-1) - 4x + 3$

  $= 2x - 2 - 4x + 3$

  $= -2x + 1$

- Woran liegt das?:
  - Man zerlegt g ja in a und b, genauer $g = a - b$. Daher liegen a und b in derselben Äquivalenzklasse bzgl., d. h. modulo g. (Dies wiederum ist der Fall, denn 2 Elemente liegen nach Definition in derselben Äquivalenzklasse, wenn ihre Differenz im 'Unterraum' liegt. Da g im von g aufgespannten 'Unterraum' liegt und $g = a - b$ ist nun $a \equiv b \bmod g$.)
  - Da man $f \bmod g$ (= Rest) betrachten möchte und $a \equiv b \bmod g$, darf man also in f jedes vorkommen von a durch b ersetzen.
  - Da man a als das Leitmonom von g definiert hat und b als 'das Übrige von g', welches vom Grad her echt kleiner ist, konvertiert man f nach und nach in kleiner werdende Polynome, die modulo g alle in derselben Äquivalenzklasse bleiben.
  - Dieses Verfahren muss irgendwann stoppen, so dass man ein 'schönstes', weil kleinstes Polynom findet, mit dem man f modulo g representieren kann.
- Proposition 2.2.2.d):
  - alternativer Beweis:
    - Prinzipiell braucht man die Fallunterscheidung gar nicht machen und kann mit folgenden Überlegungen beweisen:
    - $m_1 \overset{g_i}{\to} m_2 \Leftrightarrow m_2 = m_1 - ctg_i \wedge t \cdot \mathrm{LT}(g_i) \notin \mathrm{Supp}(m_2)$
    - Sei c der Koeffizient von $t \cdot \mathrm{LT}(g_i)$ in m_1, also $m_1 = \ldots + ct\mathrm{LT}(g_i) + \ldots$.
    - Der Koeffizient von $t \cdot \mathrm{LT}(g_i)$ in m_2 ist wegen $t \cdot \mathrm{LT}(g_i) \notin \mathrm{Supp}(m_2)$ gleich 0, also $m_2 = \ldots$.
    - Sei c' der Koeffizient von $t \cdot \mathrm{LT}(g_i)$ in m_3, also $m_3 = \ldots + c't\mathrm{LT}(g_i) + \ldots$.
    - Dann sind $m_1 + m_3 = \ldots + (c + c')t\mathrm{LT}(g_i) + \ldots$ und $m_2 + m_3 = \ldots + c't\mathrm{LT}(g_i) + \ldots$.
    - Wegen $m_1 + m_3 - (c + c')t\mathrm{LT}(g_i) = \underbrace{\qquad\qquad}_{\text{enthält } t\mathrm{LT}(g_i) \text{ nicht mehr}} =: m_4$ gilt $m_1 + m_3 \overset{g_i}{\to} m_4$.
    - Wegen $m_2 + m_3 - c't\mathrm{LT}(g_i) = \underbrace{\qquad\qquad}_{\text{enthält } t\mathrm{LT}(g_i) \text{ nicht mehr}} =: \tilde{m}_4$ gilt $m_2 + m_3 \overset{g_i}{\to} \tilde{m}_4$.
    - Nun ist aber $m_4 = \tilde{m}_4$, denn:

      $m_4 = \underbrace{m_1}_{= m_2 + ct\mathrm{LT}(g_i)} + m_3 - (c + c')t\mathrm{LT}(g_i) = m_2 + ct\mathrm{LT}(g_i) + m_3 - (c + c')t\mathrm{LT}(g_i)$

      $= m_2 + m_3 - c't\mathrm{LT}(g_i) = \tilde{m}_4$

      also: $m_1 + m_3 \overset{g_i}{\to} m_4$ und $m_2 + m_3 \overset{g_i}{\to} m_4$
  - Ergänzung zum Beweis im Buch:
    - $tLT(g_i)$ verschwindet im Fall $c' = -c$ aus $m_2 + m_3 - c'tg_i$, weil $tLT(g_i)$ nicht in m_2

(siehe im Buch 3 Zeilen höher) vorkommt und weil $tLT(g_i)$ in m_3 gerade mit dem Koeffizienten c' vorkommt (siehe im Buch 2 Zeilen höher). Also $m_2 + m_3 - c'tg_i = m_2 + \underbrace{c'tLT(g_i)+\ldots}_{=m_3} - c't\underbrace{(LT(g_i)+\ldots)}_{=g_i}$. Also verschwindet $tLT(g_i)$ aus $m_2 + m_3 - c'tg_i$.

- Weil nun $m_1 + m_3 = m_2 + m_3 - c'tg_i = (m_2 + m_3) - c'tg_i$, bedeutet das, dass $m_2 + m_3 \overset{g_i}{\to} m_1 + m_3$ und somit auch $m_2 + m_3 \overset{G}{\to} m_1 + m_3$.
- Außerdem gilt trivialer Weise: $m_1 + m_3 \overset{G}{\to} m_1 + m_3$.
- Wähle nun $m_4 = m_1 + m_3$, dann gilt $m_1 + m_3 \overset{G}{\to} m_4$ und $m_2 + m_3 \overset{G}{\to} m_4$.
- Bemerkung zum Fall $c' \neq -c$: $m_1 + m_3 \overset{g_i}{\to} m_4$, weil $m_4 = m_1 + m_3 - (c+c')tg_i = \underbrace{\underbrace{m_1 - ctg_i}_{\text{hier wird } tLT(g_i) \text{ ausgelöscht}} + \underbrace{m_3 - c'tg_i}_{\text{hier wird } tLT(g_i) \text{ wird ausgelöscht}}}_{\text{also wird } tLT(g_i) \text{ insgesamt ausgelöscht, kommt also in } m_4 \text{ nicht mehr vor}}$. Also $m_1 + m_3 \overset{g_i}{\to} m_4$. $m_2 + m_3 \overset{g_i}{\to} m_4$ analog.

- Proposition 2.2.5:
  - Ergänzung zum Beweis '$C_2 \Rightarrow C_3$':
    - $m_2 - m_2' \in M$, weil $m_1 \overset{G}{\to} m_2$ und $m_1 \overset{G}{\to} m_2'$.
    - Das heißt, dass sich m_2 schreiben lässt als $m_2 = m_1 - f_1 g_1 - \ldots - f_s g_s$, wobei die f_i die sich aus den jeweiligen Reduktionsschritten ergebenden (angesammelten) Polynome sind. Analoges gilt für m_2'.
    - Etwas umgeschrieben erhält man $m_1 = m_2 + f_1 g_1 + \ldots + f_s g_s$ und $m_1 = m_2' + f_1' g_1 + \ldots + f_s' g_s$, also $m_2 + f_1 g_1 + \ldots + f_s g_s = m_2' + f_1' g_1 + \ldots + f_s' g_s$.
    - Etwas umgeschrieben erhält man $m_2 - m_2' = \underbrace{(f_1' - f_1)g_1 + \ldots + (f_s' - f_s)g_s}_{\in \langle g_1,\ldots,g_s\rangle = M}$.
    - Also $m_2 - m_2' \in M$.
  - Ergänzung zum Beweis '$C_4 \Rightarrow C_1$':
    - gegeben C_4
    - $m \overset{G}{\to} 0 \Rightarrow m \in M$:
      - $m \overset{G}{\to} 0 \Rightarrow m \overset{G}{\leftrightarrow} 0 \underbrace{\Rightarrow}_{\text{nach Proposition 2.2.2.g)}} m \in \underbrace{M}_{=\langle g_1,\ldots,g_s\rangle}$
    - $m \overset{G}{\to} 0 \Leftarrow m \in M$:
      - $m \in M \Rightarrow m \overset{G}{\leftrightarrow} 0$
      - $\underbrace{m}_{=:m_1} \leftrightarrow m_2 \leftrightarrow \ldots \leftrightarrow m_{t-1} \underbrace{\not\to}_{\text{'}\leftarrow\text{' kann an dieser Stelle nicht sein, da sich 0 nicht reduzieren lässt}} \underbrace{0}_{=:m_t}$
      - Sei daher $1 \le l \le t-2$ (statt $1 \le l \le t-1$) der größte Index mit $m_l \leftarrow m_{l+1}$. Oder anders: $m_{l+1} \to m_l$.
      - Dann gilt $m_{l+1} \to m_{l+2} \to \ldots \to 0$, weil ja l die letzte Stelle war, wo der Pfeil nach

links zeigt. Also gilt $m_{l+1} \overset{G}{\to} 0$
- Andererseits gilt $m_{l+1} \to m_l$.
- Nach C_4 gibt es nun ein n, so dass $0 \overset{G}{\to} n$ und $m_l \overset{G}{\to} n$.
- Da sich aber 0 nicht echt reduzieren lässt, ist $n = 0$.
- Also $m_l \overset{G}{\to} 0$.
- Erhalte nun die echt kürzere Sequenz $\underbrace{m}_{=:m_1} \leftrightarrow m_2 \leftrightarrow \ldots \leftrightarrow m_l \overset{G}{\to} 0$.
- Gilt nun überall '$\to$' ist man fertig, ansonsten fängt man mit dieser neuen Sequenz wieder vorne an.
- Auf jeden Fall erhält man am Ende $m \overset{G}{\to} 0$, nämlich dann, wenn es keine '$\leftarrow$' mehr gibt.

- Proposition 2.2.6:
  - einfacherer Beweis zu b):
    - $m_1 \overset{g_i}{\to} m_2$ bedeutet $m_2 = m_1 - ctg_i$.
    - Demnach bedeutet $m_1 \overset{G}{\to} m_2 \;\; m_2 = m_1 - \sum_i f_i g_i$.
    - Dann bedeutet $m_1 \overset{G}{\to} 0 \;\; 0 = m_1 - \sum_i f_i g_i \Leftrightarrow m_1 = \sum_i f_i g_i$.
    - Da in $\sum_i f_i g_i$ irgendwo durch ein bestimmtes ctg_α der Leitterm von m zu 0 gemacht wird (wobei natürlich $LT(m) = LT(ctg_\alpha)$), lässt sich dieses aus der Summe herausziehen: $m_1 = \underbrace{\sum_i f_i g_i}_{\text{jetzt ohne den Summanden } ctg_\alpha} + ctg_\alpha$.
    - also: $m_1 - ctg_\alpha = \underbrace{\sum_i f_i g_i}_{\text{jetzt ohne den Summanden } ctg_\alpha}$
    - Dass $LT(m) > LT(f_i g_i)$ für alle $f_i g_i$ in *dieser* Summe, ist offensichtlich.
- Proposition 2.2.8:
  - Ergänzung zum Beweis '$A_2 \Rightarrow C_2$':
    - Angenommen, es gibt ein $m \in M$, dass ungleich 0 ist und trotzdem irreduzibel ist.
    - Der Widerspruch ist $m \overset{G}{\to} m'$, obwohl m irreduzibel angenommen wurde.
  - Ergänzung zum Beweis '$C_1 \Rightarrow A_2$':

$$m \in M \setminus \{0\} \underbrace{\Rightarrow}_{C_1} m \overset{G}{\to} 0 \underbrace{\Rightarrow}_{2.2.6.c)} m = \sum_i f_i g_i \wedge LT(m) = \max_i LT\{f_i g_i\}$$

2.3 Syzygies

- Proposition 2.3.6:
  - Diese recht abstrakt scheinende Proposition hat folgende Aussagen:

- $\mathrm{LT}\left(\lambda\left(\underbrace{(f_1,\ldots,f_s)}_{=m}\right)\right) \leq \deg_G((f_1,\ldots,f_s))$: klar, denn:
  - $\lambda((f_1,\ldots,f_s)) = f_1g_1+\ldots+f_sg_s$
  - $\deg_G((f_1,\ldots,f_s)) = \max\limits_{1\leq i\leq s}\{\mathrm{LT}(f_ig_i)\}$
  - Es ist offensichtlich, dass $\mathrm{LT}(f_1g_1+\ldots+f_sg_s) \leq \max\limits_{1\leq i\leq s}\{\mathrm{LT}(f_ig_i)\}$.
- $\mathrm{LT}(\lambda((f_1,\ldots,f_s))) < \deg_G((f_1,\ldots,f_s))$:
  - bedeutet, dass $\mathrm{LT}(f_1g_1+\ldots+f_sg_s) < \max\limits_{1\leq i\leq s}\{\mathrm{LT}(f_ig_i)\} \underbrace{=}_{\text{für ein oder mehrere } 1\leq k\leq s} \mathrm{LT}(f_kg_k) = \mathrm{LT}(f_k)\cdot\mathrm{LT}(g_k)$
  - Das wiederum bedeutet, dass sich in $f_1g_1+\ldots+f_sg_s$ der größte Term wegkürzt, also der Term $\mathrm{LT}(f_k)\cdot\mathrm{LT}(g_k)$. (Dazu muss es natürlich mindestens 2 solcher *k*-s geben, damit sich die Koeffizienten zu 0 addieren können.)
  - Also ist $\mathrm{LF}(f_1g_1+\ldots+f_sg_s)$, also der Vektor aus den $\mathrm{LM}(f_k)$ dieser *k*-s, eine Syzygie für $(\mathrm{LM}(g_1),\ldots,\mathrm{LM}(g_s))$, weil sich – wie gesagt – die Koeffizienten zu 0 addieren.
- $\mathrm{LT}(\lambda((f_1,\ldots,f_s))) = \deg_G((f_1,\ldots,f_s))$:
  - Hier kürzt sich der größte Term also nicht weg.
  - Also ist $\Lambda(\mathrm{LF}((f_1,\ldots,f_s))) = \sum\limits_{k\text{-s von eben}} \mathrm{LM}(f_k)\cdot\mathrm{LM}(g_k) = \mathrm{LT}(f_1g_1+\ldots+f_sg_s) = \mathrm{LT}(\lambda((f_1,\ldots,f_s)))$.
- Ist $(f_1,\ldots,f_s)\in \mathrm{Syz}(G)$, dann ist auch $\mathrm{LF}(f_1,\ldots,f_s)\in \mathrm{Syz}(\mathrm{LM}(G))$, weil:
  - $f_1g_1+\ldots+f_sg_s = 0$
  - Insbesondere addieren sich die Koeffizienten des größten Terms zu 0.
  - Also ist $\mathrm{LF}(f_1,\ldots,f_s)\in \mathrm{Syz}(\mathrm{LM}(G))$, denn nur $\mathrm{LF}(f_1,\ldots,f_s)$ ist verantwortlich für das 0-Werden des größten Terms von $f_1g_1+\ldots+f_sg_s$

- Proposition 2.3.11:
  - Ergänzung zum Beweis:
    - Angenommen, es gibt *m*-s in $\mathrm{Syz}(G)$, die nicht als Linearkombination der m_i-s dargestellt werden können. Wähle ein kleinstes *m*.
    - Weil $(\overline{m}_1,\ldots,\overline{m}_t)$ $\mathrm{Syz}(\mathrm{LM}(G))$ erzeugt und $\mathrm{LF}(m)\in \mathrm{Syz}(\mathrm{LM}(G))$ (weil $\mathrm{LF}(m)$ für das 0-Werden der Leitmonome von einigen g_i-s verantwortlich ist und weil $m\in \mathrm{Syz}(G)$, d. h. insbesondere diese Leitmonome werden auch tatsächlich 0),, besitzt $\mathrm{LF}(m)$ eine Darstellung $\mathrm{LF}(m) = \sum c_jt_j\overline{m}_{i_j}$.
    - Dann ist $m' := m - \sum c_jt_jm_{i_j}$ kleiner als *m* und kann somit mit $(m_1,\ldots,m_t)$ dargestelt werden.
    - Dann aber auch $m := m' + \sum c_jt_jm_{i_j}$. Widerspruch.
- Proposition 2.3.12:
  - Ergänzung zum Beweis:
    - $A_2 \Rightarrow D_1$:
      - Sei $\vec{f}\in \mathrm{Syz}(\mathrm{LM}(G))$ homogen. Zu zeigen: Es gibt eine Liftung für $\vec{f}$ in $\mathrm{Syz}(G)$.
      - Bilde $\lambda(\vec{f}) = f_1g_1+\ldots+f_Sg_S$.

- Falls $\lambda(\vec{f}) = 0$ ist $\vec{f} \in \mathrm{Syz}(G)$ und $\vec{f}$ ist seine eigene Liftung.
- Sei also $\lambda(\vec{f}) \neq 0$.
- Wegen $\lambda(\vec{f}) \in M$ gibt es nach A_2 eine (weitere) Darstellung $\lambda(\vec{f}) = h_1 g_1 + \ldots + h_S g_S$.
- Also $\lambda(\vec{f}) = f_1 g_1 + \ldots + f_S g_S = h_1 g_1 + \ldots + h_S g_S \Leftrightarrow (f_1 - h_1) g_1 + \ldots + (f_S - h_s) g_S = 0$, d. h. $((f_1 - h_1), \ldots, (f_S - h_s)) \in \mathrm{Syz}(G)$.
- Wegen
  $\deg_G(\vec{h}) \underbrace{=}_{\substack{\text{wegen Voraussetzung } A_2: \\ \mathrm{LT}(h_1 g_1 + \ldots + h_S g_S) = \max_{1 \le i \le s}\{h_i g_i\} = \deg_G(\vec{h})}} \mathrm{LT}(h_1 g_1 + \ldots + h_S g_S) = \mathrm{LT}(f_1 g_1 + \ldots + f_S g_S)$
  $\underbrace{\leq}_{\substack{\text{weil } \vec{f} \in \mathrm{Syz}(\mathrm{LM}(G)), \\ \text{siehe auch Proposition 2.3.6.b}}} \deg_G(m)$
  ist $\mathrm{LF}(\vec{f} - \vec{h}) = \mathrm{LF}(\vec{f}) \underbrace{=}_{\text{weil } \vec{f} \in \mathrm{Syz}(\mathrm{LM}(G))} \vec{f}$.
- Also ist $\vec{f} - \vec{h}$ die gesuchte Liftung von $\vec{f}$ in $\mathrm{Syz}(G)$.

- $D_1 \Rightarrow A_2$:
  - Sei $m \in M = \langle g_1, \ldots, g_s \rangle$. Angenommen, es gibt keine Darstellung von m mit $m = \sum_{i=1}^{s} f_i g_i \wedge \mathrm{LT}(m) = \max\{\mathrm{LT}(f_i g_i)\}$.
  - Da die g_i-s ein Erzeugendensystem bilden, gibt es aber auf jeden Fall eine Darstellung $m = \sum_{i=1}^{s} f_i g_i$. Also liegt das Problem bei $\mathrm{LT}(m) = \max\{\mathrm{LT}(f_i g_i)\}$.
  - Wähle unter allen Darstellung $m = \sum_{i=1}^{s} f_i g_i$ eine, so dass $\deg_G(\vec{f})$ minimal ist.
  - Wegen $\mathrm{LT}(m) \leq \max\{\mathrm{LT}(f_i g_i)\}$, folgt, dass wegen der Widerspruchs-Annahme $\mathrm{LT}(m) < \max\{\mathrm{LT}(f_i g_i)\}$ sein muss.
  - Dann ist jedoch $\mathrm{LF}(\vec{f}) \in \mathrm{Syz}(\mathrm{LM}(G))$ (nach Proposition 2.3.6.b).
  - Nach Voraussetzung D_1 gibt es nun eine Liftung $\vec{f}'$ von $\mathrm{LF}(\vec{f})$ in $\mathrm{Syz}(G)$. (Liftung bedeutet – wie immer – $\mathrm{LF}(\vec{f}') = \mathrm{LF}(\vec{f})$.)
  - Deswegen ist $\deg_G(\vec{f} - \vec{f}') < \deg_G(\vec{f})$.
  - Nach Wahl von $\vec{f}$ dürfte $\vec{f} - \vec{f}'$ keine Darstellung $m = \sum_{i=1}^{s} (f_i - f_i') g_i$ erlauben.
  - Tut es aber: $\sum_{i=1}^{s} (f_i - f_i') g_i = \sum_{i=1}^{s} f_i g_i - \underbrace{\sum_{i=1}^{s} f_i' g_i}_{=0, \text{ weil } \vec{f}' \in \mathrm{Syz}(G)} = \sum_{i=1}^{s} f_i g_i = m$. Widerspruch.

2.4 Gröbner Bases of Ideals and Modules

2.4.2 Normal Forms

- Proposition 2.4.10.d):
  - $\mathrm{Supp}(\mathrm{NF}_N(m)) \cap \mathrm{LT}\{N\} = \{\ \}$, weil: Gäbe es in $\mathrm{NF}_N(m)$ noch einen Term, der in $\mathrm{LT}\{N\} = (\mathrm{LT}(h_1),\ldots,\mathrm{LT}(h_t))$ liegt, so wäre dieser Term ein Vielfaches des Leitterms eines h_i's und der Divisionsalgorithmus zur Berechnung der Normalform hätte noch nicht gestoppt.
  - $\mathrm{NF}_N(m) \in M$, denn $m = f_1 h_1 + \ldots + f_t h_t + \mathrm{NF}_N(m) \Leftrightarrow \mathrm{NF}_N(m) = \underbrace{m}_{\in M} - \underbrace{\underbrace{(f_1 h_1 + \ldots + f_t h_t)}_{\in N \Rightarrow \in M, \text{ denn } N \subseteq M}}_{\in M}$
  - Wegen $\mathrm{Supp}(\mathrm{NF}_N(m)) \cap \mathrm{LT}\{M\} = \{\ \}$ ist $\mathrm{NF}_N(m)$ irreduzibel bzgl. $\overset{(g_1,\ldots,g_s)}{\rightarrow}$.
  - Wegen $\mathrm{C}_2 : n \in M$ irreduzibel bzgl. $\overset{G}{\rightarrow} \Rightarrow n = 0$ (Kapitel 2.2) folgt $n := \underbrace{\mathrm{NF}_N(m)}_{\in M} = 0$.
  - Also $m = \underbrace{\underbrace{f_1 h_1 + \ldots + f_t h_t}_{\in N} + \underbrace{0}_{=\mathrm{NF}_N(m)}}_{\in N}$.

2.5 Buchberger's Algorithm

- Proposition 2.5.2:
  - Der Beweis ist dem von 'Proposition 2.3.12, $\mathrm{A}_2 \Rightarrow \mathrm{D}_1$ sehr ähnlich.:
    - Zu zeigen: Es gibt eine Liftung für $\sigma_{ij} \in \mathrm{Syz}(\mathrm{LM}(G))$ in $\mathrm{Syz}(G)$.
    - Bilde

$$S_{ij} = \lambda(\sigma_{ij}) = \lambda\left(\begin{pmatrix} 0 \\ \vdots \\ 0 \\ \frac{1}{c_i} t_{ij} \\ 0 \\ \vdots \\ 0 \\ -\frac{1}{c_j} t_{ji} \\ 0 \\ \vdots \\ 0 \end{pmatrix}\right)$$

$$= 0g_1 + \ldots + 0g_{i-1} + \frac{1}{c_i} t_{ij} g_i + 0g_{i+1} + \ldots + 0g_{j-1} + \left(-\frac{1}{c_j} t_{ji}\right) g_j + 0g_{j+1} + \ldots + 0g_s$$

    - Falls $\lambda(\sigma_{ij}) = 0$ ist $\sigma_{ij} \in \mathrm{Syz}(G)$ und σ_{ij} ist seine eigene Liftung.
    - Sei also $\lambda(\sigma_{ij}) \neq 0$.
    - Weil G eine Gröbner-Basis ist und $S_{ij} = \lambda(\sigma_{ij}) \overset{G}{\rightarrow} 0 \Rightarrow \lambda(\sigma_{ij}) \in M$ gibt es nach A_2 eine (weitere) Darstellung $\lambda(\sigma_{ij}) = h_1 g_1 + \ldots + h_S g_S$.

- Also

$$\lambda(\sigma_{ij}) = 0g_1 + \ldots + 0g_{i-1} + \frac{1}{c_i} t_{ij} g_i + 0g_{i+1} + \ldots + 0g_{j-1} + \left(-\frac{1}{c_j} t_{ji} \right) g_j + 0g_{j+1} + \ldots + 0g_s$$

$$= h_1 g_1 + \ldots + h_S g_S$$

$$\Leftrightarrow (-h_1)g_1 + \ldots + (-h_{i-1})g_{i-1} + \left(\frac{1}{c_i} t_{ij} - h_i \right) g_i + (-h_{i+1})g_{i+1} + \ldots \quad ,$$

$$+ (-h_{j-1})g_{j-1} + \left(-\frac{1}{c_j} t_{ji} - h_j \right) g_j + (-h_{j+1})g_{j+1} + \ldots + (-h_s)g_s = 0$$

d. h. $(\sigma_{ij} - \vec{h}) \in \mathrm{Syz}(G)$.

- Wegen

$$\deg_G(\vec{h}) \underbrace{\leq}_{\substack{\text{wegen Voraussetzung } A_2: \\ \mathrm{LT}(h_1 g_1 + \ldots + h_S g_S) = \max_{1 \le i \le s} \{h_i g_i\} = \deg_G(\vec{h})}} \mathrm{LT}(h_1 g_1 + \ldots + h_S g_S)$$

$$= \mathrm{LT}\left(0g_1 + \ldots + 0g_{i-1} + \frac{1}{c_i} t_{ij} g_i + 0g_{i+1} + \ldots + 0g_{j-1} + \left(-\frac{1}{c_j} t_{ji} \right) g_j + 0g_{j+1} + \ldots + 0g_s \right)$$

$$\underbrace{\leq}_{\substack{\text{weil } \sigma_{ij} \in \mathrm{Syz}(\mathrm{LM}(G)), \\ \text{siehe auch Proposition 2.3.6.b}}} \deg_G(\sigma_{ij})$$

ist $\mathrm{LF}(\sigma_{ij} - \vec{h}) = \mathrm{LF}(\sigma_{ij}) \underbrace{=}_{\text{weil } \sigma_{ij} \in \mathrm{Syz}(\mathrm{LM}(G))} \sigma_{ij}$.

- Also ist $\sigma_{ij} - \vec{h}$ die gesuchte Liftung von σ_{ij} in $\mathrm{Syz}(G)$.

3.2 Elementary Operations on Modules

- Proposition 3.2.15:
  - Beweis von a):
    - $N :_P M = \{r \in R \mid r \cdot M \subseteq N\}$
    - $\bigcap_{i=1}^{s} (N :_P \langle g_i \rangle) = \bigcap_{i=1}^{s} \{r \in R \mid r \cdot \langle g_i \rangle \subseteq N\}$
    - also zu zeigen $\{r \in R \mid r \cdot M \subseteq N\} = \bigcap_{i=1}^{s} \{r \in R \mid r \cdot \langle g_i \rangle \subseteq N\}$
    - '$\subseteq$':
      - Seien $g_i' \in \langle g_i \rangle$ für beliebiges i und $r \in \{r \in R \mid r \cdot M \subseteq N\}$.
      - Da auch $g_i' \in M$, ist $rg_i' \subseteq N$, also (weil i beliebig war) $r \in \bigcap_{i=1}^{s} \{r \in R \mid r \cdot \langle g_i \rangle \subseteq N\}$.
    - '$\supseteq$':
      - Seien $m = f_1 g_1 + \ldots + f_s g_s$ und $r \in \bigcap_{i=1}^{s} \{r \in R \mid r \cdot \langle g_i \rangle \subseteq N\}$.
      - Dann ist $rm = \underbrace{r f_1 \underbrace{g_1}_{\in \langle g_1 \rangle}}_{\in N, \text{ weil } r \in \{r \in R \mid r \cdot \langle g_1 \rangle \subseteq N\}} + \ldots + \underbrace{r f_s \underbrace{g_s}_{\in g_s}}_{\in N, \text{ weil } r \in \{r \in R \mid r \cdot \langle g_s \rangle \subseteq N\}} \in N$, also

$$r \in \{r \in R \mid r \cdot M \subseteq N\}.$$

- Proposition 3.2.22:
  - Der Beweis verläuft analog zum Beweis von 3.2.15.

3.4 Elimination

- Theorem 3.4.5:
  - Beweis:
    - '$\subseteq$': $te_i \in \mathrm{LT}_{\hat{\sigma}}(M \cap \hat{P}^r) \Rightarrow te_i \in \underbrace{\mathrm{LT}_\sigma(M)}_{\supseteq \mathrm{LT}_{\hat{\sigma}}(M \cap \hat{P}^r)} \wedge te_i \in \hat{P}^r \Rightarrow \mathrm{LT}_\sigma(M) \cap \hat{P}$
    - '$\supseteq$':
      $te_i \in \mathrm{LT}_\sigma(M) \cap \hat{P} \Rightarrow te_i \in \mathrm{LT}_\sigma(M) \wedge te_i \in \hat{P}^r \underbrace{\Rightarrow}_{\text{da } \sigma \text{ Eliminationsordnung}} \exists g_i \in \hat{P}^r : te_i = \mathrm{LT}_{\sigma^r}(g_i)$
      $\Rightarrow \mathrm{LT}_{\hat{\sigma}}(M \cap \hat{P}^r)$

3.5 Localization and Saturation

- Proposition 3.5.12:
  - Beweis:
    - '$\subseteq$':
      $v \in (N :_M I^\infty) \cap (N :_M J^\infty) \Leftrightarrow \exists i, j : I^i v \subseteq N \wedge J^j v \subseteq N$
      $\Leftrightarrow \exists i, j : f^i v \in N \wedge g^j v \in N \forall f \in I, g \in J \Rightarrow (f+g)^{i+j} v \in N \forall f \in I, g \in J,$
      $\Rightarrow v \in N :_M (I+J)^\infty$
      wobei die letzte Folgerung gilt, weil
      $(f+g)^{i+j} v \underbrace{=}_{\substack{\text{bis auf Konstanten} \\ \text{bei den Summanden}}} \underbrace{f^{i+j} g^0 v + f^{i+j-1} g^1 v + \ldots}_{\in N \text{ wegen } f^k \underbrace{(f^i v)}_{\in N} \in N \text{ für } 1 \le k \le j} + \underbrace{f^i g^j v}_{\text{offensichtlich} \in N} + \underbrace{\ldots + f^1 g^{i+j-1} v + f^0 g^{i+j} v}_{\in N \text{ wegen } g^k \underbrace{(g^i v)}_{\in N} \in N \text{ für } 1 \le k \le j}$
    - '$\supseteq$':
      $v \in N :_M (I+J)^\infty \Leftrightarrow \exists k : (I+J)^k v \subseteq N \Leftrightarrow \exists k : (f+g)^k v \in N \forall f \in I, g \in J$
      $\Rightarrow \left(f + \underbrace{0}_{\in J}\right)^k v \in N \wedge \left(\underbrace{0}_{\in I} + g\right)^k v \in N \forall f \in I, g \in J \Rightarrow f^k v \in N \wedge g^k v \in N \forall f \in I, g \in J$
      $\Rightarrow v \in (N :_M I^\infty) \cap (N :_M J^\infty)$

Remarks

Der erste Teil dieser Datei bezieht sich auf die ‘Computanional Commutative Algebra 1 (Algebra 2)’-Vorlesung von Prof. Martin Kreuzer im Sommersemester 2004. Zu dieser Vorlesung gibt es eine Fotoreihe der Tafeln (Dateien: University; Computational Commutative Algebra 1 (Algebra 2); SS 2004; *).
Der zweite Teil dieser Datei bezieht sich auf das Buch ‘Computanional Commutative Algebra 1’ von Martin Kreuzer und Lorenzo Robbiano (Version vom 2000-07-03).
Außerdem gibt es eine weitere Datei ‘University; Algebra 1 (basics), Computational Commutative Algebra 1; Overview’, welche eine Übersicht über die Grundlagen der ‘Algebra 1’-Vorlesung von Prof. Martin Kreuzer im Wintersemester 2003/2004 und über die ‘Computanional Commutative Algebra 1 (Algebra 2)’-Vorlesung von Prof. Martin Kreuzer im Sommersemester 2004 und das Buch ‘Computanional Commutative Algebra 1’ von Martin Kreuzer und Lorenzo Robbiano (Version vom 2000-07-03) enthält.

http://www.TL-Software.de.tf
thleopold@hotmail.com

Thomas Leopold,
2004-10-13