P1

1965-00-00-A

Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal.

D i s s e r t a t i o n

zur Erlangung des Doktorgrades der philosophischen Fakultät an der Leopold-Franzens-Universität Innsbruck.

Eingereicht von Bruno Buchberger, Innsbruck,
Herbst 1965.

Lebenslauf.

Ich wurde am 22.10.1942 in Innsbruck als Sohn des Gendarmeriebeamten Josef Buchberger und dessen Frau Katharina geboren. Ich besuchte die Volksschule und eine Klasse der Hauptschule in Innsbruck, wechselte dann in die zweite Klasse des I. Bundes-Realgymnasiums in Innsbruck über und maturierte dort am 2.6.1960. Seit dem Wintersemester 1960/61 bin ich an der hiesigen Leopold-Franzens-Universität mit den Fächern Mathematik (Hauptfach) und experimentelle Physik (Nebenfach) inskribiert. Meine Ausbildung verdanke ich den Vorlesungen und Anleitungen zur wissenschaftlichen Arbeit des Herrn Professor Gröbner, den mathematischen Vorlesungen der Herren Professoren Schatz und Lochs und den Vorlesungen über Physik bei den Herren Professoren Steinmaurer und Kolb. Seit dem 1.7.1964 bin ich als WHK in der Rechenanlage (Institut für theoretische Physik) beschäftigt.

1. Einleitung.

Der Restklassenring eines nulldimensionalen Polynomideals in $K[x_1, x_2, \ldots, x_n]$ hat die Struktur eines hyperkomplexen Systems mit endlich vielen Basiselementen. In der vorliegenden Arbeit soll ein Algorithmus näher untersucht werden, der von Professor Wolfgang Gröbner in einer wissenschaftlichen Anleitungsstunde im Frühjahr 1964 angegeben wurde, um diese Basiselemente aus den erzeugenden Polynomen eines Polynomideals berechnen zu können. Die Untersuchung des Algorithmus verfolgt zunächst das Ziel, Kriterien für das Abbrechen des Algorithmus zu finden (Abschnitt 4 und 8) und ihn soweit zu systematisieren, daß er für eine Behandlung mit elektronischer Rechenanlage zugänglich ist (Abschnitt 4, 6 und 9). Dabei konnten noch gewisse innewohnenden Gesetzmäßigkeiten herausgestellt werden, die eine Anwendung auf die Berechnung der Hilbertfunktion eines beliebigen Polynomideals nahelegen (Abschnitt 5 und 7).

Mein aufrichtiger Dank gilt Herrn Prof.Dr.Wolfgang Gröbner für die Leitung der Arbeit. Ich danke auch den Mitarbeitern der Rechenanlage der Universität Innsbruck, den Herren Dr.H.Knapp und G.Margreiter für manche wertvolle Ratschläge bei der Programmierung.

2. Verwendete Abkürzungen, Symbole, Begriffe und Sätze.

Abkürzungen:

P-Ring.................Polynomring
P-Ideal................Polynomideal
KGV....................kleinstes gemeinsames Vielfaches
PP.....................Potenzprodukt
PPR....................Restklasse eines Potenzproduktes

Symbole:

$a \in M$....................a ist Element der Menge M
$N \subset M$....................Die Menge N ist Untermenge der Menge M.
$\overset{\mathrm{Df}}{=}$ ....per definitionem gleich
$\overline{x}$....................Restklasse von x
$a \equiv b(\mathfrak{a})$....................a ist kongruent b modulo dem Ideal $\mathfrak{a}$.
$x \to u$....................Das Element x eines Ringes geht bei der Restklassenbildung modulo einem Ideal in das Element u des Restklassenringes über.

Auftretende algebraische Symbole und Begriffe werden genau in dem Sinne verwendet, wie er in [1] durch die entsprechenden Vereinbarungen festgelegt wird. Deshalb werden wir die Definitionen der Begriffe Gruppe, Ring, Körper, Ideal, Kongruenz modulo einem Ideal, Dimension eines P-Ideals und ähnlicher nicht mehr anführen. Wir geben nur zusätzliche Festlegungen an.

(2.1) Vereinbarung: Der dem P-Ring $K[x_1, x_2, \ldots, x_n]$ zugrundeliegende Konstantenkörper K wird kommutativ vorausgesetzt.

(2.2) Definition des hyperkomplexen Systems: Ein hyperkomplexes System läßt sich kurz als ein endlicher R-Modul ([2], S.46), der gleichzeitig Ring ist, charakterisieren. Wir geben diese Definition hier aber auch ausführlich, weil wir später auf einzelne Teile davon Bezug nehmen werden: Eine nicht leere Menge G heißt hyperkomplexes System (oder Algebra) vom Range m über R, wenn gilt:

(2.2.1) G ist eine additive, abelsche Gruppe.

(2.2.2) R ist ein Ring mit Einselement.

(2.2.3) Es ist eine Multiplikation der Elemente $\alpha, \beta, \gamma, \ldots$ von R mit den Elementen $u, v, w, \ldots$ von G definiert mit den Eigenschaften:

(2.2.3.1) Das Produkt eines Elementes α von R mit einem Element u von G gehört stets zu G.

(2.2.3.2) $\alpha(u+v) = \alpha u + \alpha v$

(2.2.3.3) $(\alpha+\beta)u = \alpha u + \beta u$

(2.2.3.4) $(\alpha\beta)u = \alpha(\beta u)$

(2.2.3.5) Alle Elemente von G sind eindeutig darstellbar als Linearformen $\alpha_1 u_1 + \alpha_2 u_2 + \dots + \alpha_m u_m$ mit Hilfe von m festen Elementen $u_1, u_2, \dots, u_m$ wobei $\alpha_i \in R$, $u_i \in G$ $(i=1,2,\dots,m)$.

(2.2.4) Es ist eine Multiplikation der Elemente u, v, w, ... von G untereinander definiert mit folgenden Eigenschaften:

(2.2.4.1) Das Produkt uv zweier Elemente u und v von G liegt wieder in G.

(2.2.4.2) $(uv)w = u(vw)$

(2.2.4.3) $(u+v)w = uw + vw$

$u(v+w) = uv + uw$

(2.2.4.4) $(\alpha u)v = u(\alpha v) = \alpha(uv)$ für alle $\alpha \in R$

(2.2.5) Definition: Die in (2.2.3.5) auftretenden m Elemente $u_1, u_2, \dots, u_m$ heißen Basiselemente des hyperkomplexen Systems.

Aus (2.2.3.4) und (2.2.4.4) folgt

(2.2.6) $(\alpha u)(\beta v) = (\alpha\beta)(uv)$ und

(2.2.7) $\left(\sum_{j=1}^{m} \alpha_j u_j\right)\left(\sum_{k=1}^{m} \beta_k u_k\right) = \sum_{j=1}^{m}\sum_{k=1}^{m}(\alpha_j \beta_k)(u_j u_k)$

Daher sind alle Produkte uv berechenbar, sobald die Produkte $u_j u_k$ bekannt sind, die als Elemente von G als Linearkombinationen der $u_1, u_2, \dots, u_m$ geschrieben werden können:

(2.2.8) $u_j u_k = \sum_{l=1}^{m} \gamma_{jk}^{l} u_l$ $(j=1,2,\dots,m;\ k=1,2,\dots,m;\ \gamma_{jk}^{l} \in K)$.

(2.2.9) Definition: Die in (2.2.8) auftretenden m^3 Elemente γ_{jk}^{l} aus R heißen Strukturkonstante des hyperkomplexen Systems G.

(2.2.10) Definition: Die Gesamtheit der ausgerechneten Produkte der Art (2.2.8) heißt Multiplikationstafel des hyperkomplexen Systems G.

Es ist auch eine Verallgemeinerung der hyperkomplexen Systeme zu Systemen mit unendlich vielen Basiselementen möglich. Das Axiom (2.2.3.5) wird dabei umgewandelt zu:

(2.2.3.5a) Alle Elemente von G sind eindeutig darstellbar als Linearkombinationen $\alpha_1 u_1 + \alpha_2 u_2 + \dots + \alpha_k u_k$ aus endlich vielen der unendlich vielen Basiselemente $u_1, u_2, \dots, u_k, \dots$

3. Der Restklassenring eines nulldimensionalen P-Ideals.

Über den Restklassenring $K[x_1,x_2,\dots,x_n]/\mathfrak{a}=\mathfrak{r}$ nach einem nulldimensionalen P-Ideal $\mathfrak{a}\subset K[x_1,x_2,\dots,x_n]$ gilt der folgende Satz:

(3.1) Satz: Der Restklassenring $\mathfrak{r}$ nach einem nulldimensionalen P-Ideal ist ein hyperkomplexes System über dem Grundkörper K, wenn wir als additive Gruppenverknüpfung die in $\mathfrak{r}$ schon definierte Addition zwischen Restklassen nehmen, als multiplikative Verknüpfung (2.2.3) die schon definierte Multiplikation αu zwischen Elementen $\alpha\in K$ und und den Restklassen $u\in\mathfrak{r}$ *) und als multiplikative Verknüpfung (2.2.4) die schon definierte Multiplikation zwischen Restklassen.

Beweis: Wir zeigen nacheinander, daß die Axiome (2.2.1) bis (2.2.4) erfüllt sind.

(2.2.1) ist erfüllt, da $\mathfrak{r}$ als Ring in bezug auf seine Addition eine abelsche Gruppe ist.

(2.2.2): K ist als Körper ein Ring mit Einselement.

(2.2.3.1) bis (2.2.3.4) sind in der Tat Eigenschaften der Multiplikation zwischen Elementen des Grundkörpers K und den Restklassen.

Zum Beweis, daß (2.2.3.5) erfüllt ist, brauchen wir zwei Hilfssätze:

(3.2) Hilfssatz: $u_1,u_2,\dots,u_m$ seien Elemente eines hyperkomplexen Systems G mit der Eigenschaft, daß sich jedes $u\in G$ als

(3.2.1) $u=\sum_{j=1}^{m}\alpha_j u_j \quad (\alpha_j\in K,\ j=1,2,\dots,m)$

darstellen läßt. Dann gilt: Wenn $u_1,u_2,\dots,u_m$ über K linear unabhängig sind, so sind die Darstellungen (3.2.1) eindeutig und umgekehrt.

---

*) Zunächst ist eine Multiplikation $\bar\alpha\cdot u$ definiert als Multiplikation zwischen Restklassen. Da aber die Menge der $\bar\alpha$ isomorph ist dem Grundkörper K, ist damit sofort auch eine Multiplikation $\alpha\cdot u$ festlegbar: $\alpha\cdot u \overset{\text{def}}{=} \bar\alpha\cdot u$

Beweis von (3.2): Wir nehmen an, daß die Darstellungen (3.2.1) nicht eindeutig sind, das heißt es gibt ein u, sodaß einerseits

(3.2.2a) $u = \sum_{j=1}^{m} \alpha_j u_j$

und andererseits

(3.2.2b) $u = \sum_{j=1}^{m} \beta_j u_j$ ($\alpha_j \neq \beta_j$ für mindestens ein j).

Somit ist

(3.2.3) $0 = \sum_{j=1}^{m} (\alpha_j - \beta_j) u_j$ ($\alpha_j - \beta_j \neq 0$ für mindestens ein j).

(3.2.3) drückt aber gerade die lineare Abhängigkeit von $u_1, u_2, \ldots, u_m$ aus.

Nehmen wir nun an, daß $u_1, u_2, \ldots, u_m$ linear abhängig sind, also zum Beispiel

(3.2.4) $u_1 = \sum_{j=2}^{m} \gamma_j u_j$,

dann hat ein $u \in G$ mit einer Darstellung (3.2.1), wo $\alpha_1 \neq 0$, sicher noch eine Darstellung

(3.2.5) $u = \sum_{j=1}^{m} \alpha_j u_j = \alpha_1 u_1 + \sum_{j=2}^{m} \alpha_j u_j = \sum_{j=2}^{m} (\alpha_1 \gamma_j + \alpha_j) u_j$,

was der Eindeutigkeit widerspricht.

(3.3) Hilfssatz: Wenn das P-Ideal die Dimension o hat, so enthält es Polynome $p_i(x_i)$ ($i=1,2,\ldots,n$), die jeweils nur von einer einzigen Variablen x_i abhängen.

Beweis von (3.3): nach [1], S.98 ist die Dimension eines P-Ideals $\mathfrak{a}$ die maximale Anzahl unabhängiger Variablen in bezug auf $\mathfrak{a}$. Das heißt also: ein nulldimensionales P-Ideal hat keine unabhängigen Variablen in bezug auf $\mathfrak{a}$, oder: alle Variablen sind abhängig in bezug auf $\mathfrak{a}$. Nach der Definition der Abhängigkeit in bezug auf ein P-Ideal ([1], S.97) heißt das weiter: es gibt für jede Variable x_i ein Polynom $p_i(x_i)$, das nur von dieser Variablen abhängt (i=1,2,...,n).

Daß (2.2.3.5) auf $\mathfrak{r}$ zutrifft, kann nun auch dadurch bewiesen werden, daß man zeigt: es gibt endlich viele Restklassen $u_1, u_2, \ldots, u_p$ in $\mathfrak{r}$, durch die sich alle anderen darstellen lassen. Denn aus diesen p Restklassen lassen sich immer m linear unabhängige auswählen, durch die sich alle Restklassen wegen (3.2) eindeutig darstellen lassen.

Zunächst läßt sich jede Restklasse aus $\mathfrak{r}$ durch Linearkombination aus den Restklassen der PP aus n Variablen $x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n}$ darstellen. Da

(3.4.a) $\quad p_i(x_i) \overset{DF}{=} x_i^{k_i} + c_{i,1} x_i^{k_i - 1} + \ldots + c_{i,k_i} \in \mathfrak{a} \qquad (i=1,2,\ldots,n;\ c_{i,j} \in K,\ j=1,2,\ldots,k_i)$

gilt

(3.4.b) $\quad x_i^{k_i} \equiv -c_{i,1} x_i^{k_i-1} - \ldots - c_{i,k_i} \equiv -\sum_{l=1}^{k_i} c_{i,l} x_i^{k_i-l} \ (\mathfrak{a})$

und für die PP $x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n}$ eines Grades $\sigma \geq \tau \quad (\tau = k_1 + k_2 + \ldots + k_n)$

(3.4.c) $\quad x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n} \equiv (x_1^{i_1} \ldots x_j^{i_j - k_j} \ldots x_n^{i_n})\, x_j^{k_j} \equiv -\sum_{l=1}^{k_j} x_j^{k_j - l} \cdot x_1^{i_1} \ldots x_j^{i_j - k_j} \ldots x_n^{i_n}$

$$\equiv -\sum_{l=1}^{k_j} c_{j,l}\, x_1^{i_1} \ldots x_j^{i_j - l} \ldots x_n^{i_n} \ (\mathfrak{a})$$

wenn $i_j \geq k_j$, was bei den PP eines Grades $\sigma \geq \tau$ sicher für ein j der Fall sein muß.

Die PP $x_1^{i_1} \ldots x_j^{i_j - l} \ldots x_n^{i_n}$ lassen sich nun selbst in der Art (3.4.c) weiter bearbeiten, soferne sie einen Grad $\sigma \geq \tau$ haben, solange bis (3.4.c) übergeht in

(3.4.d) $\quad x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n} \equiv \sum c_{j_1, j_2, \ldots, j_n}\, x_1^{j_1} x_2^{j_2} \ldots x_n^{j_n} \ (\mathfrak{a})$,

wobei in der Summe nur mehr PP $x_1^{j_1} x_2^{j_2} \ldots x_n^{j_n}$ eines Grades $< \tau$ auftreten. Aus den PP $x_1^{j_1} x_2^{j_2} \ldots x_n^{j_n}$ effektiv m modulo $\mathfrak{a}$ linear unabhängige zu gewinnen, ist eine Hauptaufgabe des in 4. beschriebenen Algorithmus.

(2.2.4.1) bis (2.2.4.4) sind genau Eigenschaften der Multiplikation zwischen Restklassen.

Im Falle eines nicht nulldimensionalen P-Ideals gelten alle Überlegungen des Beweises von (3.1) mit Ausnahme von (3.3) und den Folgerungen aus (3.3). Dementsprechend gilt:

(3.5) Satz: Der Restklassenring nach einem P-Ideal der Dimension $d > 0$ ist ein hyperkomplexes System mit unendlich vielen Basiselementen.

Es gilt auch die Umkehrung von (3.1), die wir in folgender Form schreiben:

(3.6) Satz: Wenn es im Restklassenring $K[x_1, x_2, \ldots, x_n]/\mathfrak{a}$ nur endlich viele linear unabhängige Restklassen gibt, so ist $\mathfrak{a}$ nulldimensional.

Beweis: Angenommen es gäbe m linear unabhängige Restklassen, und m+1 Restklassen wären immer schon linear abhängig, so sind auch die PP $1, x_i, \ldots, x_i^m \ (i=1,2,\ldots,n)$ sicher modulo $\mathfrak{a}$ linear abhängig, es gibt also eine Beziehung:

(3.6.1a) $p_i(x_i) \overset{\mathrm{Df}}{=} \sum_{j=0}^{m} c_{ij} x_i^{m-j} \equiv 0 \ (\mathfrak{a}) \qquad (i=1,2,\dots,n)$

Das heißt aber:

(3.6.1b) $p_i(x_i) \in \mathfrak{a}$

und deshalb: keine Variable ist unabhängig in bezug auf ,
das heißt ist nulldimensional.

4. Ein Algorithmus zum Auffinden einer Basis des hyperkomplexen Systems aus (3.1).

Vorbereitende Überlegungen.

Für die Zwecke des Algorithmus vereinbaren wir zunächst eine eindeutige Anordnung der Potenzprodukte $x_1^{i_1}x_2^{i_2}\dots x_n^{i_n}$ aus n Variablen $x_1, x_2, \dots, x_n$, nämlich die lexikographische:

(4.1) Definition: Ein PP $x_1^{i_1}x_2^{i_2}\dots x_n^{i_n}$ kommt vor einem PP $x_1^{k_1}x_2^{k_2}\dots x_n^{k_n}$ (hat eine niederere Nummer als das PP $x_1^{k_1}x_2^{k_2}\dots x_n^{k_n}$), wenn:
1. $x_1^{i_1}x_2^{i_2}\dots x_n^{i_n}$ den kleineren Grad als $x_1^{k_1}x_2^{k_2}\dots x_n^{k_n}$ hat oder
2. die beiden Grade gleich sind und die erste nicht verschwindende Differenz $i_j - k_j$ positiv ist.

Gegeben sei nun ein nulldimensionales P-Ideal $\mathfrak{a} \subset K[x_1, x_2, \dots, x_n]$ mit einer erzeugenden Basis

(4.2) $\mathfrak{a} = (f_1, f_2, \dots, f_s)$, wobei

(4.3) $f_j \overset{\mathrm{DF}}{=} \sum a^{(j)}_{i_1 i_2 \dots i_n} x_1^{i_1}x_2^{i_2}\dots x_n^{i_n} \quad (j = 1, 2, \dots, s \, ; \; a^{(j)}_{i_1 i_2 \dots i_n} \in K)$

(Die Summation geht über alle Indexkombinationen $(i_1, i_2, \dots, i_n)$ bis zu einer Kombination $(k_1^{(j)}, k_2^{(j)}, \dots, k_n^{(j)})$, wobei $x_1^{k_1^{(j)}}x_2^{k_2^{(j)}}\dots x_n^{k_n^{(j)}}$ unter den PP von f_j mit Koeffizienten $\neq 0$ in der Anordnung (4.1) die höchste Nummer hat. O.B.d.A. können wir $a^{(j)}_{k_1^{(j)} k_2^{(j)} \dots k_n^{(j)}} = 1$ voraussetzen, da K ein Körper ist.)

Damit ergibt sich:

(4.4a) $\sum a^{(j)}_{i_1 i_2 \dots i_n} x_1^{i_1}x_2^{i_2}\dots x_n^{i_n} \equiv 0 \, (\mathfrak{a}) \quad , \quad (j = 1, 2, \dots, s)$

oder

(4.4b) $x_1^{k_1^{(j)}}x_2^{k_2^{(j)}}\dots x_n^{k_n^{(j)}} \equiv -\sum a^{(j)}_{i_1 i_2 \dots i_n} x_1^{i_1}x_2^{i_2}\dots x_n^{i_n} \, (\mathfrak{a}) \quad , \quad (j = 1, 2, \dots, s)$

(Die Summation geht über alle Indexkombinationen $(i_1, i_2, \dots, i_n) \neq (k_1^{(j)}, k_2^{(j)}, \dots, k_n^{(j)})$)

und

(4.4c) $x_1^{k_1^{(j)}+l_1} x_2^{k_2^{(j)}+l_2} \dots x_n^{k_n^{(j)}+l_n} \equiv -\sum a^{(j)}_{i_1 i_2 \dots i_n} x_1^{i_1+l_1} x_2^{i_2+l_2} \dots x_n^{i_n+l_n} \, (\mathfrak{a})$

$(j = 1, 2, \dots, s \, ; \; l_i = 0, 1, 2, \dots \text{ für } i = 1, 2, \dots, n)$

Sämtliche mögliche Beziehungen zwischen den PPR erhält man, wenn man sämtliche Polynome $f \in \mathfrak{a}$, das sind die Polynome der Form

$$(4.5) \qquad f = \sum_{j=1}^{s} d_j(x_1, x_2, \ldots, x_n)\, f_j = \sum a_{i_1 i_2 \ldots i_n} x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n} \;,\quad d_j(x_1, x_2, \ldots, x_n) \in K[x_1, x_2, \ldots, x_n] \quad (j = 1, 2, \ldots, s)$$

im Restklassenring $\mathfrak{R}$ betrachtet:

$$(4.6) \qquad \sum a_{i_1 i_2 \ldots i_n} x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n} \equiv 0 \;(\mathfrak{a})$$

(4.6) ist eine lineare Gleichung zwischen PPR. Aus jeder solchen Kongruenz (4.6) kann man nun unter den mit Koeffizienten $\neq 0$ vorkommenden PP z.B. das PP mit der höchsten Nummer ausrechnen, das heißt durch PP mit niedererer Nummer ausdrücken. Es bleiben (im Falle eines nulldimensionalen P-Ideals endlich viele) PP übrig, die in keiner Beziehung (4.6) als PP mit höchster Nummer vorkommen. Ihre Restklassen bilden eine linear unabhängige Basis von $\mathfrak{R}$.

Um schrittweise zum Algorithmus zu kommen, der die Aussonderung einer <u>solchen</u> Basis leistet, müssen wir noch eine Überlegung anstellen. Wir nehmen an, wir hätten ausgehend von den schon vorhandenen Beziehungen (4.4b) gewisse PPR $u_1, u_2, \ldots, u_m$ gefunden, sodaß sich die Restklassen aller PP $x_1^{k_1} x_2^{k_2} \ldots x_n^{k_n}$ aus ihnen linear kombinieren lassen:

$$(4.7) \qquad x_1^{k_1} x_2^{k_2} \ldots x_n^{k_n} \equiv \sum_{i=1}^{m} \alpha_i^{(k_1, k_2, \ldots, k_n)} u_i \;(\mathfrak{a}) \;,\; (\alpha_i^{(k_1, k_2, \ldots, k_n)} \in K)$$

(Spezialfall $x_1^{k_1} x_2^{k_2} \ldots x_n^{k_n} \equiv u_i(\mathfrak{a})$ für ein bestimmtes i eingeschlossen).

Weiters lasse sich für jedes PP $x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n}$ zeigen, daß man durch Zerlegung von $x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n}$ in t Teilprodukte

$$(4.8) \qquad x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n} = x_1^{i_1^{(1)}} x_2^{i_2^{(1)}} \ldots x_n^{i_n^{(1)}} \cdot x_1^{i_1^{(2)}} x_2^{i_2^{(2)}} \ldots x_n^{i_n^{(2)}} \ldots x_1^{i_1^{(t)}} x_2^{i_2^{(t)}} \ldots x_n^{i_n^{(t)}}$$
$$\left(\sum_{l=1}^{t} i_j^{(l)} = i_j \;\text{ für } j = 1, 2, \ldots, n \;,\; 1 \leq t \leq \sum_{j=1}^{n} i_j \right) ,$$

Einsetzen der Darstellungen (4.7) für die Teilprodukte in (4.8), Ausmultiplizieren und weiteres Reduzieren des Ergebnisses (4.8a) der Multiplikation

(4.8a) $x_1^{i_1} x_2^{i_2} \dots x_n^{i_n} \equiv \sum b_{k_1 k_2 \dots k_n} x_1^{k_1} x_2^{k_2} \dots x_n^{k_n} \ (\mathfrak{a})$

durch Verwendung der Darstellungen (4.7) für die $x_1^{k_1} x_2^{k_2} \dots x_n^{k_n}$ immer zur selben Darstellung (4.7) von $x_1^{i_1} x_2^{i_2} \dots x_n^{i_n}$ kommt, unabhängig davon wie die Aufteilung (4.8) in Teilprodukte vorgenommen wurde. Dann können wir sicher gehen, daß die $u_1, u_2, \dots, u_m$ linear unabhängig sind, das heißt im Sinne von (2.2.5) eine Basis von $\mathfrak{r}$ bilden.

Ist nämlich die Unabhängigkeit der Darstellung (4.7) eines jeden PP von der Zerlegung in (4.8) gezeigt, so haben die Restklassen der Polynome

(4.9) $x_1^{l_1} x_2^{l_2} \dots x_n^{l_n} f_j = x_1^{l_1+k_1^{(j)}} x_2^{l_2+k_2^{(j)}} \dots x_n^{l_n+k_n^{(j)}} + \sum a^{(j)}_{i_1 i_2 \dots i_n} x_1^{l_1+i_1} x_2^{l_2+i_2} \dots x_n^{l_n+i_n} \in \mathfrak{a}$
$(j = 1, 2, \dots, s\ ;\ l_i = 0, 1, 2, \dots \text{ für } i = 1, 2, \dots, n)$

die wegen (4.4c) eine Darstellung

(4.9a) $x_1^{l_1} x_2^{l_2} \dots x_n^{l_n} f_j \equiv 0 \cdot u_1 + 0 \cdot u_2 + \dots + 0 \cdot u_m \equiv 0 \quad (j = 1, 2, \dots, s,\ l_i = 0, 1, 2, \dots \text{ für } i = 1, 2, \dots, n)$

(≡ ist hier das Identitätszeichen!)

besitzen, auch nur diese eine Darstellung, unabhängig davon, in welcher Reihenfolge wir die bei der Berechnung der Restklasse von $x_1^{l_1} x_2^{l_2} \dots x_n^{l_n} f_j$ nötigen Multiplikationen und Additionen ausführen. Gäbe es nun noch eine Beziehung

(4.10) $\sum_{i=1}^{m} c_i u_i = 0$ ($c_i \neq 0$ für mindestens ein i),

die die lineare Abhängigkeit von $u_1, u_2, \dots, u_m$ ausdrückte, so würde dem ein Polynom $f \in \mathfrak{a}$ entsprechen, das eine Darstellung (4.5) besitzt, die auch so geschrieben werden kann:

(4.11) $f = \sum b^{(1)}_{l_1 l_2 \dots l_n} x_1^{l_1} x_2^{l_2} \dots x_n^{l_n} f_1 + \sum b^{(2)}_{l_1 l_2 \dots l_n} x_1^{l_1} x_2^{l_2} \dots x_n^{l_n} f_2 + \dots + \sum b^{(s)}_{l_1 l_2 \dots l_n} x_1^{l_1} x_2^{l_2} \dots x_n^{l_n} f_s$

wenn

(4.12) $d_j(x_1, x_2, \dots, x_n) \overset{\text{Df}}{=} \sum b^{(j)}_{l_1 l_2 \dots l_n} x_1^{l_1} x_2^{l_2} \dots x_n^{l_n} \quad (j = 1, 2, \dots, s\ ;\ b^{(j)}_{l_1 l_2 \dots l_n} \in K)$

Die hier auftretenden Polynome $x_1^{l_1} x_2^{l_2} \dots x_n^{l_n} f_j$ $(j = 1, 2, \dots, s)$ sind gerade von der Art (4.9), von denen wir wissen, daß ihre Restklassen nur die Darstellung ≡0 haben. Es hat also auch $\bar{f}=\sum_{i=1}^{m} c_i u_i$ bezüglich der Restklassen $u_1, u_2, \ldots, u_m$ in $\mathcal{A}$ nur die Darstellung $\equiv 0$. Eine Beziehung (4.1o) kann es also nicht mehr geben.

Der folgende Algorithmus geht nun gerade so vor sich, daß er ausgehend von den schon vorhandenen Beziehungen (4.4b) die Darstellungen der einzelnen PPR auf die beschriebene Weise durch Ausmultiplizieren der Darstellungen von Teilprodukten rechnet und sie miteinander vergleicht. Aus zwei verschiedenen Darstellungen ein und derselben PPR kann dann eine der in beiden Darstellungen vorkommenden PPR (z.B. diejenige mit der höchsten Nummer) eliminiert werden. Das heißt wir können eine Darstellung dieser PPR durch andere PPR (mit niedererer Nummer) errechnen. Es muß nun immer wieder von neuem überprüft werden, ob alle verschiedenen Wege, die PPR aus den Teilprodukten zu berechnen, zum gleichen Ergebnis führen, solange bis das tatsächlich einmal für sämtliche PPR der Fall ist. Dann wissen wir auf Grund der bisherigen Überlegungen, daß die verbleibenden, nicht durch andere PPR linear kombinierbaren PPR eine linear unabhängige Basis von $\mathcal{A}$ bilden. Natürlich können wir die Überprüfung der Darstellung nicht für die unendlich vielen PPR durchführen. Wir werden deshalb im Anschluß an die Beschreibung des Algorithmus noch Kriterien angeben müssen, die es gestatten, aus dem Übereinstimmen der Darstellung bei endlich vielen PPR auf das Übereinstimmen bei allen PPR zu schließen.

Beschreibung des Algorithmus.

Zunächst noch eine Vereinbarung über die Sprechweise: die Darstellung der Restklasse eines PP $x_1^{i_1} x_2^{i_2} \dots x_n^{i_n}$ als Linearkombination anderer PPR mit niedererer Nummer, die beim gerade vorliegenden Schritt des Algorithmus selbst nicht durch andere PPR linear kombiniert werden können, heißen wir eine Σ-Darstellung der PPR (öfters auch ungenauer eine Σ-Darstellung des betreffenden PP).

Wir beschreiben jetzt den Algorithmus für das Ideal $\mathfrak{a}$ (4.2), und zwar in einer Form, aus der sich später leicht ein großes Flußdiagramm für die Rechnung mit elektronischer Rechenanlage ableiten ließe. Das wird allerdings nicht geschehen, da für die Programmierung eine andere Variante des Algorithmus verwendet wurde. Jedenfalls erleichtert die folgende Art der Darstellung sehr die Übersichtlichkeit.

(A) Wir merken die Beziehungen (4.4b) in einer Liste, die wir Liste S nennen, vor.
Wir betrachten die Restklasse von 1. Läßt sich diese schon wegen einer Beziehung in der Liste S durch die Restklasse einer anderen Konstanten ersetzen, so besäße $\mathfrak{a}$ überhaupt nur eine Restklasse, hätte also die Dimension -1. (Das gleiche wäre der Fall, wenn wir im Laufe der weiteren Rechnung zu einer Beziehung 1=o kämen.) Im allgemeinen wird das nicht der Fall sein und wir gehen zu (B).

(B) Wir nehmen das in der Anordnung (4.1) folgende PP und betrachten seine Restklasse.

(BA) Diese hat vielleicht schon wegen der Beziehungen in der Liste S eine oder mehrere Σ-Darstellungen. Wenn ja, so schreiben wir diese in die Zeile neben das betrachtete PP und gehen nach (BB). Wenn nein, gehen wir sofort nach (BB).

(BB) Wir zerlegen das betrachtete PP auf alle möglichen Weisen in zwei Teilprodukte und berechnen daraus sofern möglich in der auf S.10 beschriebenen Art Σ-Darstellungen des PP unter Verwendung der bisher bekannten Σ-Darstellungen von PP. Sowohl die so erhaltenen Σ-Darstellungen als auch die Zerlegungen des PP in zwei Teilprodukte, die zu keiner Σ-Darstellung geführt haben, schreiben wir in die Zeile neben das betrachtete PP.

(C) In der Zeile neben dem PP kann nun stehen:

(CA) Keine Σ-Darstellung des PP, sondern nur Zerlegungen in Teilprodukte. Wir vermerken, daß sich diese PPR bisher noch nicht durch andere niedererer Nummer darstellen läßt und gehen nach (B).

(CB) Eine einzige oder mehrere gleiche Σ-Darstellungen des betrachteten PP. Wir gehen sofort nach (B).

(CC) Mehrere Σ-Darstellungen des betrachteten PP, unter denen mindestens zwei verschiedene vorkommen. Wir eliminieren aus ihnen mit den Methoden der linearen Algebra so viele von den vorkommenden PPR wie möglich, und zwar bei jenen mit der höchsten Nummer beginnend. Wir erhalten also Σ-Darstellungen von PP, die bisher keine solchen besaßen. Alle diese Σ-Darstellungen schreiben wir wieder in die Liste S. Dann beginnen wir wieder die Restklasse von 1 zu betrachten und setzen bei (BA) fort (wir sagen: wir beginnen mit einem neuen Durchgang.)

Wenn man die vorbereitenden Überlegungen zusammenfaßt, gilt über das Abbrechen des Algorithmus bisher folgendes:

(4.13) Der Algorithmus kann abgebrochen werden, wenn

1. beim gerade laufenden Durchgang sämtliche PP, von denen in der Liste S Σ-Darstellungen vermerkt sind, als in (B) betrachtete PP vorgekommen sind und
2. sicher ist, daß aus den Zerlegungen in zwei Teilprodukte bei keiner PPR mehr mehrere verschiedene Σ-Darstellungen auftreten. (Dies wird auf Grund der Kriterien (4.14) und (4.19) schon behauptet werden können, wenn bei gewissen endlichen Graden keine verschiedenen Σ-Darstellungen mehr auftreten.)

Da wir gleichzeitig mit den Σ-Darstellungen der PPR auch die

Zerlegungen in zwei Teilprodukte notieren, ist es leicht, aus den Zeilen des Algorithmus auch die Multiplikationstafel der Basiselemente abzulesen. Wegen der konsequenten Vorgangsweise des Algorithmus von einem PP zum anderen streng nach Anordnung (4.1) genügt es, sämtliche Aufspaltungen eines PP in zwei Teilprodukte zu betrachten. Verschiedene Zerlegungen eines Teilproduktes in weitere Faktoren können an den resultierenden Σ-Darstellungen nichts mehr ändern, da bei den früheren Schritten des Algorithmus ja gerade die Zerlegung der Teilprodukte in weitere Faktoren durchgeführt wurde und dafür gesorgt wurde, daß für diese Teilprodukte höchstens eine einzige Σ-Darstellung vorhanden ist.

Die Vorgangsweise des Algorithmus soll jetzt an einem Beispiel verdeutlicht werden:

Beispiel 1:
Gegeben sei das nulldimensionale P-Ideal

$\mathfrak{a} = (x_1^2 - 2x_2 + x_1,\ x_1x_3 - x_3,\ x_3^2 - 2x_3 + x_2) \subset K[x_1, x_2, x_3]$.

Wir schreiben zunächst die einzelnen Zeilen des Algorithmus an und beschreiben dann jeden Schritt ausführlich.

Liste S:
$$x_1^2 \equiv 2x_2 - x_1\ (\mathfrak{a})$$
$$x_1x_3 \equiv x_3\ (\mathfrak{a})$$
$$x_3^2 \equiv 2x_3 - x_2\ (\mathfrak{a})$$
$$(x_2x_3 \rightarrow)\ u_6 = u_3$$
$$(x_1x_2 \rightarrow)\ u_4 = u_2$$
$$(x_2^2 \rightarrow)\ u_5 = u_2$$

1

$x_1 \rightarrow u_1\cdot$

$x_2 \rightarrow u_2\cdot$

$x_3 \rightarrow u_3\cdot$

$x_1^2 \rightarrow 2u_2 - u_1 = u_1^2$

$x_1x_2 \rightarrow u_1u_2 = \cancel{u_4\cdot} = u_2$

$x_1x_3 \rightarrow u_3 = u_1u_3$

$x_2^2 \rightarrow u_2^2 = \cancel{u_5\cdot} = u_2$

$x_2x_3 \rightarrow u_2u_3 = \cancel{u_6\cdot} = u_3$

$x_3^2 \to 2u_3 - u_2 = u_3^2$

$x_1^3 \to 2u_4 - \cancel{2u_2} + u_1$

$x_1^2 x_2 \to \cancel{u_1 u_4} = \cancel{2u_5} - \cancel{u_4} = u_2$

$x_1^2 x_3 \to u_3 = \cancel{2u_6} - \cancel{u_3}$

$x_1 x_2^2 \to \cancel{u_1 u_5} = \cancel{u_2 u_4} = \cancel{u_7} = u_2$

$x_1 x_2 x_3 \to u_3 = \cancel{u_5} = \cancel{u_3 u_4}$

$x_1 x_3^2 \to \cancel{2u_3} - \cancel{u_4} = 2u_3 - u_2$

$x_2^3 \longrightarrow u_2$

$x_2^2 x_3 \longrightarrow \cancel{u_3} = u_3$

$x_2 x_3^2 \longrightarrow \cancel{2u_3} - \cancel{u_2} = 2u_3 - u_2$

$x_3^3 \longrightarrow 3u_3 - 2u_2$

$x_1^4 \longrightarrow \ldots$

$\vdots$

1. Wir haben also zunächst gemäß (A) die Basispolynome von $\mathfrak{a}$ umgeschrieben in Restklassenbeziehungen und als die ersten drei Zeilen der Liste S vorgemerkt. Die Restklasse von 1 läßt sich durch diese Beziehungen nicht darstellen, wir gehen also zu (B).

2. Gemäß (B) betrachten wir die Restklasse von x_1. x_1 erhält weder bei (BA) boch bei (BB) eine Σ-Darstellung. x_1 fällt also unter (CA). Wir setzen $x_1 \to u_1^{\circ}$, was kenntlich machen soll, daß x_1 noch keine Σ-Darstellung besitzt. Wir gehen nach (B).

3. Die in 2. angegebenen Schritte müssen nun nach den Anordnungen des Algorithmus auch für x_2 und x_3 durchgeführt werden. Wir gelangen dann wieder zu (B).

4. Das nächstfolgende PP ist x_1^2. Dessen Restklasse erhält bei (BA) eine Σ-Darstellung $x_1^2 \to 2u_2 - u_1$, bei (BB) nicht, jedoch merken wir uns die Zerlegung $x_1^2 \to u_1 \cdot u_1$ vor. Wegen (CB) ge-

hen wir sofort wieder nach (B).

5. Für $x_1 x_2$ ist nur wegen (BB) eine Zerlegung $u_1 \cdot u_2$ vorzumerken. Gemäß (CA) wird $x_1 x_2$ durch $x_1 x_2 \to u_4$. als PP ohne Σ-Darstellung kenntlich gemacht.

6. $x_1 x_3$ wird wie x_1^2 verarbeitet, x_2^2 und $x_2 x_3$ wie $x_1 x_2$, x_3^2 wie x_1^2.

7. x_1^3 hat bei (BB) eine Zerlegung $x_1^3 = x_1^2 \cdot x_1$, x_1^2 eine Σ-Darstellung, die wir aus der Liste S oder aus der Zeile von x_1^2 entnehmen können. x_1^3 berechnet sich also:

$$x_1^3 = x_1^2 x_1 \Rightarrow (2u_2 - u_1)u_1 = 2u_1 u_2 - u_1^2 = 2u_4 - 2u_2 + u_1$$

Diese Σ-Darstellung schreiben wir an und gehen wegen (CB) sofort nach (B).

8. $x_1^2 x_2$ hat eine Σ-Darstellung, die wie in 7. berechnet wird, besitzt aber außerdem noch eine Zerlegung

$$x_1^2 x_2 = x_1 (x_1 x_2) \to u_1 u_4,$$

die zu keiner Σ-Darstellung führt.

9. $x_1^2 x_3$ besitzt nun zwei verschiedene Σ-Darstellungen, die sich aus

$$x_1^2 x_3 = x_1 (x_1 x_3) \quad \text{und} \quad x_1^2 x_3 = (x_1^2) \cdot x_3$$

wie in 7. berechnen. Es liegt also Fall (CC) vor. Wir eliminieren aus den beiden Darstellungen u_6 ($u_6 = \overline{x_2 x_3}$ hat eine höhere Nummer als $u_3 = \overline{x_3}$!). Die Beziehung $u_6 = u_3$ merken wir in der Liste S vor und beginnen mit dem zweiten Durchgang.

10. Wir sehen sofort, daß sich bis zur Zeile von $x_2 x_3$ im Algorithmus beim zweiten Durchgang gegenüber dem ersten nichts ändert. Bei $x_2 x_3$ können wir u_6 durch u_3 ersetzen, u_6 streichen wir durch. Bis zur Zeile von $x_1^2 x_3$ ändert sich wieder nichts, bei $x_1^2 x_3$ erhalten wir durch Einsetzen von $u_6 = u_3$ zwei gleiche Σ-Darstellungen für $x_1^2 x_3$. Wir lassen nur eine stehen, die andere streichen wir durch.

11. $x_1x_2^2$ hat zwei Zerlegungen in Teilprodukte, die aber beide nicht zu Σ-Darstellungen führen, wegen (CA) setzen wir $x_1x_2^2 \to u_7$.

12. $x_1x_2x_3$ hat drei Zerlegungen in Teilprodukte, von denen zwei zu Σ-Darstellungen führen, die aber untereinander gleich sind. Gemäß (CB) gehen wir sofort wieder zu (B).

13. $x_1x_3^2$ wird wie $x_1^2x_3$ verarbeitet. Wir erhalten eine neue Beziehung für die Liste S: $u_4 = u_2$, beginnen mit einem neuen Durchgang, machen die entsprechenden Schritte wie in 10., wodurch $x_1x_2 \to u_2$ und $x_1^3 \to u_1$ wird, stoßen aber bei $x_1^2x_2$ durch Ausnützen aller jetzt vorhandenen Beziehungen auf zwei verschiedene Σ-Darstellungen, aus denen wir $u_5 = u_2$ eliminieren können. Wir speichern diese Beziehung wieder in der Liste S.

14. Wenn wir jetzt wieder mit einem neuen Durchgang beginnen, erhalten wir $x_2^2 \to u_2$, dann $x_1^2x_2 \to u_2$ als einzige Darstellung. Die beiden Zerlegungen von $x_1x_2^2$ liefern Σ-Darstellungen, die aber untereinander gleich sind. Die Zerlegung von $\overline{x_1x_2x_3}$ in $u_3 \cdot u_4$ liefert noch einmal u_3. $2u_3 - u_2$ wird die einzige Σ-Darstellung von $x_1x_3^2$. Die weiteren PP bis x_3^3 haben jeweils nur mehr eine einzige Σ-Darstellung.

Hier kann der Algorithmus abgebrochen werden, denn erstens sind die PP, die in der Liste S auf der linken Seite der Kongruenzen stehen, auch beim letzten Durchgang alle vorgekommen und zweitens können nie mehr Beziehungen durch verschiedene Aufspaltung eines PP in Teilprodukte auftreten, wie aus der Anwendung des noch folgenden Satzes (4.14) hervorgeht.

Als Basiselemente bleiben die PPR ohne Σ-Darstellung übrig:

$$1,\ u_1,\ u_2,\ u_3\ .$$

Ihre Multiplikationstafel kann aus den Zeilen des Algorithmus abgelesen werden:

	u_1	u_2	u_3
u_1	$2u_2-u_1$	u_2	u_3
u_2		u_2	u_3
u_3			$2u_3-u_2$

Die Multiplikationen

$$1 \cdot 1 = 1$$
$$1 \cdot u_1 = u_1$$
$$1 \cdot u_2 = u_2$$
$$1 \cdot u_3 = u_3$$

sind trivial und werden deshalb in der Multipliaktionstafel nicht eigens angeführt.

In der praktischen Rechnung wird man die Zeilen des Algorithmus und die Liste S zu einem einzigen Schema vereinigen.

Kriterien für das Abbrechen des Algorithmus.

(4.14) Satz: Seien $u_1, u_2, \ldots, u_m$ endlich viele PPR, aus denen alle andern linear kombiniert werden können. u_m habe dabei in der Anordnung (4.1) die höchste Nummer und besitze den Grad k. (Im Sinne der Bemerkung (4.13) sei weiters schon dafür gesorgt, daß die PP auf der linken Seite der Liste S, deren Grad höchstens einen endlichen Wert p haben kann, im Algorithmus beim Schritt (BA) und (BB) nur eine einzige Σ-Darstellung erhalten können, was beim Grad p überprüft ist!). Dann gilt: Wenn wir überprüft haben, daß die PP bis zum Grad $2k+1$ jeweils nur eine einzige Σ-Darstellung liefern, dann können wir sicher sein, daß auch die Zerlegungen der weiteren PP immer nur zu einer einzigen Σ-Darstellung führen.

Beweis: Bis zum Grad $2k+1$ ist geprüft, daß folgende Identitäten gelten:

(4.15) $u_j(u_i u_k) = (u_j u_i) u_k \quad (j = 1, 2, \ldots, m-1;\ k = 1, 2, \ldots, m;\ i = 1, 2, \ldots, l;\ l \leq m)$

(wobei $u_1, u_2, \ldots, u_l$ die Restklassen jener Variablen $x_{i_1}, x_{i_2}, \ldots, x_{i_l}$ seien mit der Eigenschaft: x_{i_j} hat keine Σ-Darstellung $(j = 1, 2, \ldots, l)$).

Bei den PP eines Grades $> 2k+1$ ergibt jede Aufteilung in zwei Teilprodukte eine Σ-Darstellung, denn einer der beiden Faktoren muß einen größeren Grad als k haben und besitzt deshalb sicher eine Σ-Darstellung, aus der eine Σ-Darstellung des betrachteten PP resultiert. Zwei beliebige Zerlegungen eines solchen PP $x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n}$ in zwei Faktoren können durch endlich viele Schritte der Art:

(4.16) $x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n} = (x_1^{i_1-i_1'} \ldots x_p^{i_p-i_p'} \ldots x_n^{i_n-i_n'})((x_p) x_1^{i_1'} \ldots x_p^{i_p'-1} \ldots x_n^{i_n'}) =$

(4.17) $= (x_1^{i_1-i_1'} \ldots x_p^{i_p-i_p'} \ldots x_n^{i_n-i_n'} (x_p))(x_1^{i_1'} \ldots x_p^{i_p'-1} \ldots x_n^{i_n'})$

ineinander übergeführt werden. Sobald wir also wissen, daß (4.16) und (4.17) unter der Voraussetzung des Satzes (4.14)

dieselbe Σ-Darstellung liefern, wissen wir auch, daß durch die verschiedenen Zerlegungen von $x_1^{i_1} x_2^{i_2} \dots x_n^{i_n}$ in zwei Faktoren nur eine einzige Σ-Darstellung berechnet werden kann.
Es gilt:

(4.18a) $x_1^{i_1-i_1'} \dots x_p^{i_p-i_p'} \dots x_n^{i_n-i_n'} \to \sum_{j=1}^{m} \alpha_j u_j$,

(4.18b) $x_1^{i_1'} \dots x_p^{i_p'-1} \dots x_n^{i_n'} \to \sum_{k=1}^{m} \beta_k u_k$ und

(4.18c) $x_p \to \sum_{i=1}^{L} \gamma_i u_i \qquad (\alpha_j, \beta_k, \gamma_i \in K;\ j,k = 1,2,\dots,m;\ i = 1,2,\dots,L)$

Wir berechnen (4.16) und (4.17) unter Verwendung von (4.18a), (4.18b) und (4.18c) weiter:

(4.16a) $\left(x_1^{i_1-i_1'} \dots x_p^{i_p-i_p'} \dots x_n^{i_n-i_n'}\right)\left((x_p)\, x_1^{i_1'} \dots x_p^{i_p'-1} \dots x_n^{i_n'}\right) \to$

$$\to \left(\sum_{j=1}^{m} \alpha_j u_j\right)\left(\sum_{i=1}^{L} \gamma_i u_i \sum_{k=1}^{m} \beta_k u_k\right) = \sum_{j=1}^{m}\sum_{i=1}^{L}\sum_{k=1}^{m} \alpha_j \gamma_i \beta_k\, u_j (u_i u_k)$$

(4.17a) $\left(x_1^{i_1-i_1'} \dots x_p^{i_p-i_p'} \dots x_n^{i_n-i_n'} (x_p)\right)\left(x_1^{i_1'} \dots x_p^{i_p'-1} \dots x_n^{i_n'}\right) \to$

$$\to \left(\left(\sum_{j=1}^{m} \alpha_j u_j\right) \sum_{i=1}^{L} \gamma_i u_i\right)\left(\sum_{k=1}^{m} \beta_k u_k\right) = \sum_{j=1}^{m}\sum_{i=1}^{L}\sum_{k=1}^{m} \alpha_j \gamma_i \beta_k\, (u_j u_i) u_k .$$

Die Endausdrücke von (4.16a) und (4.17a) liefern aber unter der Voraussetzung des Satzes wegen (4.15) dieselbe Σ-Darstellung.

Wegen dieses Satzes können wir im Beispiel 1 den Algorithmus bei Schritt 14. abbrechen, denn u_1, u_2, u_3 erfüllen die Voraussetzungen des Satzes (4.14), alle weiteren PPR haben also nur mehr eine einzige Σ-Darstellung. Satz (4.14) läßt sich manchmal noch verschärfen:

(4.19) Satz: Besitzen die PP eines Grades $k+1$ alle schon eine Σ-Darstellung, weil sie Vielfache von PP mit einer Σ-Darstellung sind (das Basiselement mit der höchsten Nummer hat also wieder höchstens den Grad k, auch wird wieder vorausgesetzt, daß die in der Liste S stehenden Beziehungen schon ausgenützt sind), dann gilt: wenn wir überprüft haben, daß die PP bis zum Grade $2k-1$ höchstens eine einzige Σ-Darstellung liefern, dann können wir sicher sein, daß auch die Zerlegungen der weiteren PP immer nur auf eine Σ-Darstellung führen.

Beweis: der Beweis dieses Satzes geschieht im Anschluß an die

Überlegungen des Abschnittes 5 im Abschnitt 6. Im Beispiel 1 kann dieser Satz nicht mit Vorteil angewendet werden, da beim Grad $k+1=2$ wohl alle PP eine Σ-Darstellung besitzen, jedoch nicht deshalb, weil sie Vielfaches von PP mit Σ-Darstellungen sind, sondern wegen der in der Liste S vorgemerkten Beziehungen. Nehmen wir $k+1=3$, so gilt die Voraussetzung des Satzes (4.19): alle Σ-Darstellungen der PP 3. Grades ergeben sich daraus, daß diese PP Vielfaches von PP 2. Grades mit Σ-Darstellung sind. Wegen $2k-1=3$ bringt dieser Satz jedoch gegenüber Satz (4.14) keinen Vorteil.

Die folgenden Vermutungen (4.2o) und (4.21) über das Abbrechen des Algorithmus lassen sich jedoch nicht bestätigen.

(4.2o) Vermutung: Sind im Algorithmus alle Produkte $u_i u_k$ $(i=1,2,\dots,p;\ k=i,i+1,\dots,p)$ aus allen jemals bei (CA) aufgetretenen neuen Restklassen $u_i{}^\circ$ $(i=1,2,\dots,p$; p ist der höchste bisher vorgekommene Index bei den PPR $u_i{}^\circ$, im Beispiel 1 wäre $p=7$) sowie alle in der Liste S auf der linken Seite stehenden PP nach den Vorschriften des Algorithmus behandelt, so können bei keiner PPR mehr verschiedene Σ-Darstellungen auftreten.

Es geht hier also kurz gesagt um die Frage, ob es genügt, nur die Multiplikationstafel aus den $u_i{}^\circ$ zu berechnen.

Gegenbeispiel: $\mathfrak{a} = (x_1^2 - 2x_2,\ x_2^2 - 2x_2,\ x_1 x_2 - x_2) \subset k[x_1, x_2]$

1

$x_1 \to u_1{}^\circ$

$x_2 \to u_2{}^\circ$

$x_1^2 \to 2u_2 = u_1^2$

$x_1 x_2 \to u_2 = u_1 u_2$

$x_2^2 \to 2u_2 = u_2^2$ $\longleftarrow$ hier könnten wir nach der Voraussetzung des vermuteten Satzes schon aufhören,

$x_1^3 \to 2u_2$

$x_1^2 x_2 \to u_2 = 4u_2$ $\longleftarrow$ hier treten aber noch zwei verschiedene Σ-Darstellungen bei einer PPR auf.

(4.21) Vermutung: Ist das Bestehen der Assoziativitäten

(4.21.1) $u_i(u_j u_k) = (u_i u_j) u_k$

geprüft ($i, j, k = 1, 2, \ldots, l$, wobei $u_1, u_2, \ldots, u_l$ wieder die Restklassen jener Variablen $x_{i_1}, x_{i_2}, \ldots, x_{i_l}$ seien mit der Eigenschaft: x_{i_j} hat keine Σ -Darstellung $(j = 1, 2, \ldots, l)$), was beim Grad 3 der Fall ist, und sind die in der Liste S auf der linken Seite stehenden PP schon nach den Vorschriften des Algorithmus behandelt, so können bei keiner PPR mehr verschiedene Σ-Darstellungen auftreten.

Gegenbeispiel: $\mathfrak{a} = (x_1^2 x_2 - x_1^2,\ x_1 x_2^2 - x_2) \subset k[x_1, x_2]$

1

$x_1 \to u_1 \circ$

$x_2 \to u_2 \circ$

$x_1^2 \to u_3 \circ$

$x_1 x_2 \to u_4 \circ$

$x_2^2 \to u_5 \circ$

$x_1^3 \to u_6 \circ = u_1 u_3$

$x_1^2 x_2 \to u_3 = u_2 u_3 = u_1 u_4$

$x_1 x_2^2 \to u_1 u_5 = u_2 u_4 = u_2$

$x_2^3 \to u_2 u_5 = u_7 \circ$ ← Hier könnten wir nach den Voraussetzung der Vermutung (4.21) aufhören,

$x_1^4 \to u_3^2 = u_1 u_6 = u_8 \circ$

$x_1^3 x_2 \to u_6 = u_2 u_6 = u_3 u_4$

$x_1^2 x_2^2 \to u_4 = u_3 = u_3 u_5 = u_4^2$ ← hier tritt aber noch eine neue Beziehung zwischen Restklassen auf.

Bei Durchsicht des Beweises zu Satz (4.14) läßt sich überdies erkennen, daß die Voraussetzung (4.21.1) jedenfalls nicht genügt, um die Behauptung (4.21) auf ähnliche Weise zu beweisen. Erst das Bestehen der Assoziativitäten (4.15) (die mehr fordern als (4.21.1)) ermöglicht den Beweis.

5. Das Auftreten verschiedener Σ-Darstellungen in einer Zeile des Algorithmus.

Wir möchten in diesem Abschnitt ein Gesetz herleiten, das uns sagt, in welchen Zeilen des Algorithmus die Möglichkeit besteht, daß wir zu verschiedenen Σ-Darstellungen ein und derselben PPR kommen. Dazu beweisen wir vier Hilfssätze, mit denen wir dann im Abschnitt 6 den Algorithmus in eine etwas veränderte Form bringen können.

(5.1) Hilfssatz: Wenn wir den Algorithmus auf Ideale der Form

$$\mathfrak{a} = (f_1) \subset K[x_1, x_2, \dots, x_n] \qquad \text{(Hauptideale)}$$

anwenden, wobei

$$f_1 \overset{\text{Df}}{=} x_1^{l_1} x_2^{l_2} \cdots x_n^{l_n} + \cdots$$

($x_1^{l_1} x_2^{l_2} \cdots x_n^{l_n}$ ist unter den PP von f_1 dasjenige mit der höchsten Nummer),

so können die verschiedenen Zerlegungen (4.8) eines beliebigen PP in Teilprodukte niemals auf verschiedene Σ-Darstellungen der PPR führen.

Beweis: Zunächst sei noch bemerkt, daß wir den Algorithmus auch in seiner bisherigen Form rein formal auf P-Ideale anwenden können, von denen wir nicht wissen, welche Dimension sie haben. Nur ist es dann möglich, daß immer neue PPR ohne Σ-Darstellung auftreten. Die Voraussetzungen der Sätze (4.14) oder (4.19) sind dann nie erfüllt, wir wissen also nie, wann wir den Algorithmus abbrechen dürfen. Wir dürfen also mit dem Algorithmus auch an das Ideal $\mathfrak{a} = (f_1)$ herangehen, das im Falle $n > 1$ sicher nicht nulldimensional ist ([1], S.123).

Zum Beweis von (5.1) stellen wir zunächst fest, daß aus $f \in \mathfrak{a}$, wobei

(5.2) $f \overset{\text{Df}}{=} x_1^{k_1} x_2^{k_2} \cdots x_n^{k_n} + \cdots$ ($x_1^{k_1} x_2^{k_2} \cdots x_n^{k_n}$ ist unter den PP von f dasjenige mit der höchsten Nummer),

folgt: $x_1^{k_1} x_2^{k_2} \cdots x_n^{k_n}$ ist Vielfaches von $x_1^{l_1} x_2^{l_2} \cdots x_n^{l_n}$. PP, die Vielfaches von $x_1^{l_1} x_2^{l_2} \cdots x_n^{l_n}$ sind, erhalten beim Schritt (BB) Σ-Darstellungen. PP $x_1^{b_1} x_2^{b_2} \cdots x_n^{b_n}$, die nicht Vielfaches von

$x_1^{l_1} x_2^{l_2} \ldots x_n^{l_n}$ sind, können keine Σ-Darstellung haben, denn wäre

(5.3) $x_1^{k_1} x_2^{k_2} \ldots x_n^{k_n} \equiv \sum a_{i_1 i_2 \ldots i_n} x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n} \quad (\mathfrak{a})$
($x_1^{k_1} x_2^{k_2} \ldots x_n^{k_n}$ hat eine größere Nummer als alle $x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n}$),
so wäre

(5.4) $f \overset{\text{Df}}{=} x_1^{k_1} x_2^{k_2} \ldots x_n^{k_n} - \sum a_{i_1 i_2 \ldots i_n} x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n} \in \mathfrak{a}$

im Widerspruch dazu, daß $x_1^{k_1} x_2^{k_2} \ldots x_n^{k_n}$ kein Vielfaches von $x_1^{l_1} x_2^{l_2} \ldots x_n^{l_n}$ ist. Würde nun eine PPR im Laufe des Algorithmus zwei verschiedene Σ-Darstellungenerhalten, so könnte man daraus eine Σ-Darstellung für ein PP $x_1^{k_1} x_2^{k_2} \ldots x_n^{k_n}$ berechnen, wo $x_1^{k_1} x_2^{k_2} \ldots x_n^{k_n}$ nicht Vielfaches von $x_1^{l_1} x_2^{l_2} \ldots x_n^{l_n}$ ist, denn die Restklassen der anderen PP (die Vielfachen von $x_1^{l_1} x_2^{l_2} \ldots x_n^{l_n}$) kommen in Σ-Darstellungen nicht vor, werden sie doch sofort beim Schritt (BA) oder (BB) selbst als Linearkombination von PPR dargestellt.

Wegen späterer Anwendungen soll (5.1) noch auf eine zweite Art umständlicher bewiesen werden: wir schauen nacheinander PP mit kleinerer Nummer als $x_1^{l_1} x_2^{l_2} \ldots x_n^{l_n}$ an, dann $x_1^{l_1} x_2^{l_2} \ldots x_n^{l_n}$ selber, und schließlich PP mit größerer Nummer als $x_1^{l_1} x_2^{l_2} \ldots x_n^{l_n}$ und zeigen, daß die PP einer jeden Gruppe durch die Methoden des Algorithmus höchstens eine einzige Σ-Darstellung erhalten.

Beginnen wir bei der ersten Gruppe, bei den PP mit kleinerer Nummer als $x_1^{l_1} x_2^{l_2} \ldots x_n^{l_n}$. Für diese kann überhaupt keine Σ-Darstellung abgeleitet werden, da sie keine Vielfachen von $x_1^{l_1} x_2^{l_2} \ldots x_n^{l_n}$ sind.

$x_1^{l_1} x_2^{l_2} \ldots x_n^{l_n}$ hat eine einzige Σ-Darstellung wegen $f_1 \equiv 0(\mathfrak{a})$. Zerlegungen von $x_1^{l_1} x_2^{l_2} \ldots x_n^{l_n}$ in Teilprodukte können nicht auf Σ-Darstellungen führen, weil die Teilprodukte als PP der ersten Gruppe keine Σ-Darstellungen besitzen.

Innerhalb der dritten Gruppe, die die PP mit größerer Nummer als $x_1^{l_1} x_2^{l_2} \ldots x_n^{l_n}$ umfaßt, gibt es zwei verschiedene Typen von PP: wir bezeichnen sie mit 3A und 3B.

Die Gruppe 3A umfasse die PP $x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n}$, die nicht Vielfaches von $x_1^{l_1} x_2^{l_2} \ldots x_n^{l_n}$ sind. Das erste solche ist das unmittelbar auf $x_1^{l_1}x_2^{l_2}\dots x_n^{l_n}$ folgende. Dieses hat als Teilprodukte nur PP der ersten Gruppe und hat deswegen keine Σ-Darstellung. Wir machen die Induktionsannahme: bis zum PP $x_1^{k_1}x_2^{k_2}\dots x_n^{k_n}$ hat kein PP der Gruppe 3A eine Σ-Darstellung. $x_1^{k_1}x_2^{k_2}\dots x_n^{k_n}$ selbst kann dann auch keine Σ-Darstellung haben. Bei einer Zerlegung von $x_1^{k_1}x_2^{k_2}\dots x_n^{k_n}$ in Teilprodukte ist nämlich kein Faktor Vielfaches von $x_1^{l_1}x_2^{l_2}\dots x_n^{l_n}$. Die Teilprodukte sind also PP der ersten Gruppe oder der Gruppe 3A mit kleinerer Nummer als $x_1^{k_1}x_2^{k_2}\dots x_n^{k_n}$. In beiden Fällen haben sie also keine Σ-Darstellung, damit besitzt auch $x_1^{k_1}x_2^{k_2}\dots x_n^{k_n}$ keine.

Die Gruppe 3B umfasse die PP $x_1^{i_1}x_2^{i_2}\dots x_n^{i_n}$, die Vielfaches von $x_1^{l_1}x_2^{l_2}\dots x_n^{l_n}$ sind. Wieder beweisen wir mit Induktion. Für $x_1^{l_1}x_2^{l_2}\dots x_n^{l_n}$ selbst ist schon gezeigt, daß es nur eine Σ-Darstellung besitzt. Die Induktionsannahme sei: alle PP der Gruppe 3B bis zum PP $x_1^{k_1}x_2^{k_2}\dots x_n^{k_n}$ ausschließlich habennur eine einzige Σ-Darstellung. $x_1^{k_1}x_2^{k_2}\dots x_n^{k_n}$ habe nun mindestens zwei Zerlegungen, die zu einer Σ-Darstellung führen (sonst brauchen wir nichts zu zeigen), das sind solche Zerlegungen, wo mindestens einer der beiden Faktoren Vielfaches von $x_1^{l_1}x_2^{l_2}\dots x_n^{l_n}$ ist:

(5.5) $x_1^{k_1}x_2^{k_2}\dots x_n^{k_n} = x_1^{j_1}x_2^{j_2}\dots x_n^{j_n}\cdot x_1^{k_1-j_1}x_2^{k_2-j_2}\dots x_n^{k_n-j_n} = U$

(5.6) $x_1^{k_1}x_2^{k_2}\dots x_n^{k_n} = x_1^{j_1'}x_2^{j_2'}\dots x_n^{j_n'}\cdot x_1^{k_1-j_1'}x_2^{k_2-j_2'}\dots x_n^{k_n-j_n'} = V$

O.B.d.A. seien $x_1^{k_1-j_1}x_2^{k_2-j_2}\dots x_n^{k_n-j_n}$ und $x_1^{k_1-j_1'}x_2^{k_2-j_2'}\dots x_n^{k_n-j_n'}$ die Vielfachen von $x_1^{l_1}x_2^{l_2}\dots x_n^{l_n}$. Die beiden Darstellungen lassen sich nun so schreiben:

(5.5a) $U = (x_1^{j_1}x_2^{j_2}\dots x_n^{j_n})((x_1^{k_1-j_1-l_1}x_2^{k_2-j_2-l_2}\dots x_n^{k_n-j_n-l_n})(x_1^{l_1}x_2^{l_2}\dots x_n^{l_n})) \equiv$

$\equiv (x_1^{j_1}x_2^{j_2}\dots x_n^{j_n})\left(x_1^{k_1-j_1-l_1}x_2^{k_2-j_2-l_2}\dots x_n^{k_n-j_n-l_n}\left(\sum_{j=1}^{p}\alpha_j u_j\right)\right) \equiv$

(5.5b) $\equiv \sum_{j=1}^{p}\alpha_j\,(x_1^{j_1}x_2^{j_2}\dots x_n^{j_n})(x_1^{k_1-j_1-l_1}x_2^{k_2-j_2-l_2}\dots x_n^{k_n-j_n-l_n}(u_j))\ (\mathfrak{a})$,

wenn $\sum_{j=1}^{p}\alpha_j u_j$ die Σ-Darstellung von $x_1^{l_1}x_2^{l_2}\dots x_n^{l_n}$ ist,

(5.6b) $V = \sum_{j=1}^{p}\alpha_j\,(x_1^{j_1'}x_2^{j_2'}\dots x_n^{j_n'})(x_1^{k_1-j_1'-l_1}x_2^{k_2-j_2'-l_2}\dots x_n^{k_n-j_n'-l_n}(u_j))\ (\mathfrak{a})$

Die PPR

$$(5.7)\quad \overline{x_1^{j_1} x_2^{j_2} \dots x_n^{j_n} \cdot x_1^{k_1-j_1-l_1} x_2^{k_2-j_2-l_2} \dots x_n^{k_n-j_n-l_n} u_j} =$$
$$= \overline{x_1^{j_1'} x_2^{j_2'} \dots x_n^{j_n'} \cdot x_1^{k_1-j_1'-l_1} x_2^{k_2-j_2'-l_2} \dots x_n^{k_n-j_n'-l_n} u_j} = \overline{x_1^{k_1-l_1} x_2^{k_2-l_2} \dots x_n^{k_n-l_n} u_j}$$

treten im Algorithmus schon vor der Restklasse von $x_1^{k_1} x_2^{k_2} \dots x_n^{k_n}$ auf und haben deshalb wegen der bisherigen Überlegungen und der Induktionsannahme nur eine einzige Σ-Darstellung, womit auch $x_1^{k_1} x_2^{k_2} \dots x_n^{k_n}$ nur eine einzige besitzt.

(5.8) Hilfssatz: Wenn wir den Algorithmus auf ein Ideal der Form $\mathfrak{a} = (f_1, f_2) \subset K[x_1, x_2, \dots, x_n]$

anwenden. ($f_1 \overset{\text{Df}}{=} x_1^{l_1} x_2^{l_2} \dots x_n^{l_n} + \dots$, $f_2 \overset{\text{Df}}{=} x_1^{K_1} x_2^{K_2} \dots x_n^{K_n} + \dots$;

$x_1^{l_1} x_2^{l_2} \dots x_n^{l_n}$ ($x_1^{K_1} x_2^{K_2} \dots x_n^{K_n}$) ist unter den in f_1 (f_2) vorkommenden PP dasjenige mit der höchsten Nummer),
so gilt:

1. Die Restklasse von $x_1^{G_1} x_2^{G_2} \dots x_n^{G_n}$ ($G_j = \mathrm{Max}(l_j, K_j)$, $j = 1, 2, \dots, n$), also des KGV von $x_1^{l_1} x_2^{l_2} \dots x_n^{l_n}$ und $x_1^{K_1} x_2^{K_2} \dots x_n^{K_n}$ ist die erste PPR, wo im Algorithmus verschiedene Σ-Darstellungen auftreten können.
2. Treten bei $x_1^{G_1} x_2^{G_2} \dots x_n^{G_n}$ keine verschiedenen Σ-Darstellungen auf, so liefert der Algorithmus bei keiner PPR mehr verschiedene Σ-Darstellungen.

Beweis: Ein PP, das vor $x_1^{G_1} x_2^{G_2} \dots x_n^{G_n}$ kommt, kann durch die Methoden des Algorithmus nicht zwei verschiedene Σ-Darstellungen erhalten. Ein PP $x_1^{i_1} x_2^{i_2} \dots x_n^{i_n}$ hat zunächst überhaupt nur dann Σ-Darstellungen, wenn es Vielfaches von $x_1^{l_1} x_2^{l_2} \dots x_n^{l_n}$ oder $x_1^{K_1} x_2^{K_2} \dots x_n^{K_n}$ ist. Es kann nicht Vielfaches von $x_1^{l_1} x_2^{l_2} \dots x_n^{l_n}$ und $x_1^{K_1} x_2^{K_2} \dots x_n^{K_n}$ zugleich sein, wenn es vor $x_1^{G_1} x_2^{G_2} \dots x_n^{G_n}$ kommt, denn sonst enthielte es ja auch $x_1^{G_1} x_2^{G_2} \dots x_n^{G_n}$. Durch die gleichen Überlegungen wie beim Beweis von (5.1), Gruppe 3B wird klar, daß diese PP nur eine einzige Σ-Darstellung haben können.

Anders liegen die Verhältnisse bei $x_1^{G_1} x_2^{G_2} \dots x_n^{G_n}$. Dafür gilt nämlich

$$(5.9)\quad x_1^{G_1} x_2^{G_2} \dots x_n^{G_n} = x_1^{G_1-l_1} x_2^{G_2-l_2} \dots x_n^{G_n-l_n} \cdot x_1^{l_1} x_2^{l_2} \dots x_n^{l_n} \equiv x_1^{G_1-l_1} x_2^{G_2-l_2} \dots x_n^{G_n-l_n} \Big(\sum_{j=1}^{p} \alpha_j u_j\Big) \;(\mathfrak{a})$$

und

(5.1o) $x_1^{G_1}x_2^{G_2}\dots x_n^{G_n} = x_1^{G_1-k_1}x_2^{G_2-k_2}\dots x_n^{G_n-k_n}x_1^{k_1}x_2^{k_2}\dots x_n^{k_n} \equiv x_1^{G_1-l_1}x_2^{G_2-l_2}\dots x_n^{G_n-l_n}\left(\sum_{j=1}^{p}\alpha_j u_j\right)\ (\alpha)$

wobei $\sum_{j=1}^{p}\alpha_j u_j$ und $\sum_{j=1}^{p}\beta_j u_j$ die Σ-Darstellungen von $x_1^{l_1}x_2^{l_2}\dots x_n^{l_n}$ und $x_1^{k_1}x_2^{k_2}\dots x_n^{k_n}$ sind. Nichts läßt aber darauf schließen, daß (5.9) und (5.1o) gleich sind, wenn man sie weiter ausrechnet.

Wir beweisen nun den zweiten Teil von (5.8) mit Induktion. Bei $x_1^{G_1}x_2^{G_2}\dots x_n^{G_n}$ sei also nur eine einzige Σ-Darstellung aufgetreten. Sicherlich tritt dann auch bei dem auf $x_1^{G_1}x_2^{G_2}\dots x_n^{G_n}$ unmittelbar folgenden PP nur eine einzige Σ-Darstellung auf, denn dieses kann nicht $x_1^{l_1}x_2^{l_2}\dots x_n^{l_n}$ und $x_1^{k_1}x_2^{k_2}\dots x_n^{k_n}$ enthalten. (Wenn es beide enthielte, würde es auch das KGV $x_1^{G_1}x_2^{G_2}\dots x_n^{G_n}$ enthalten. Das kann es aber nur, wenn es größeren Grad als $x_1^{G_1}x_2^{G_2}\dots x_n^{G_n}$ hat oder mit ihm identisch ist. Wenn es größeren Grad hat, so war $x_1^{G_1}x_2^{G_2}\dots x_n^{G_n}$ von der Form x_n^{L}, das nachfolgende PP ist aber dann x_1^{L+1}, welches x_n^{L} sicher nicht enthält.)

Die Induktionsannahme lautet: alle auf $x_1^{G_1}x_2^{G_2}\dots x_n^{G_n}$ folgenden PP bis zum PP $x_1^{k_1}x_2^{k_2}\dots x_n^{k_n}$ ausschließlich haben nur eine einzige Σ-Darstellung. $x_1^{k_1}x_2^{k_2}\dots x_n^{k_n}$ selbst kann nun aus seinen Zerlegungen Σ-Darstellungen gewinnen, wenn:

1. Ein Teilprodukt $x_1^{l_1}x_2^{l_2}\dots x_n^{l_n}$ enthält oder
2. ein Teilprodukt $x_1^{k_1}x_2^{k_2}\dots x_n^{k_n}$ enthält.

Die Σ-Darstellungen aus einer Zerlegung der ersten Art sind untereinander gleich, ebenso diejenigen aus den Zerlegungen der 2. Art, und zwar auf Grund ganz gleicher Überlegungen wie beim Beweis von (5.1), Gruppe 3B. Wenn Zerlegungen der 1. und 2. Art vorkommen, so auch eine Zerlegung, wo ein Teilprodukt $x_1^{G_1}x_2^{G_2}\dots x_n^{G_n}$ enthält. Diese Zerlegung gehört nun sowohl zu 1. als auch zu 2. Die daraus berechenbare Σ-Darstellung ist identisch mit den bei 1. und 2. resultierenden Σ-Darstellungen, also sind auch diese untereinander gleich.

(5.11) Hilfssatz: Sind die in (5.8) auftretenden PP $x_1^{l_1}x_2^{l_2}\dots x_n^{l_n}$ und $x_1^{k_1}x_2^{k_2}\dots x_n^{k_n}$ so beschaffen, daß $G_j = l_j + k_j$ $(j=1,2,\dots,n)$

(daß also das KGV $x_1^{G_1}x_2^{G_2}\dots x_n^{G_n}$ von $x_1^{l_1}x_2^{l_2}\dots x_n^{l_n}$ und $x_1^{k_1}x_2^{k_2}\dots x_n^{k_n}$ gleich dem Produkt der beiden ist), so hat $x_1^{G_1}x_2^{G_2}\dots x_n^{G_n}$ sicher nur eine einzige Σ-Darstellung.

Beweis: $x_1^{G_1} x_2^{G_2} \ldots x_n^{G_n}$ kann Zerlegungen haben, wo

1. ein Teilprodukt $x_1^{l_1} x_2^{l_2} \ldots x_n^{l_n}$ enthält oder
2. ein Teilprodukt $x_1^{k_1} x_2^{k_2} \ldots x_n^{k_n}$ enthält.

Auf Grund entsprechender Überlegungen wie beim Beweis von (5.1), Gruppe 3B sind die Σ-Darstellungen, die Zerlegungen der 1. Art entspringen, untereinander gleich. Dasselbe gilt für die Σ-Darstellungen aus Zerlegungen der 2. Art. Die Zerlegung

(5.12) $$x_1^{G_1} x_2^{G_2} \ldots x_n^{G_n} = x_1^{l_1} x_2^{l_2} \ldots x_n^{l_n} \cdot x_1^{K_1} x_2^{K_2} \ldots x_n^{K_n}$$

ist gleichzeitig eine der 1. als auch der 2. Art. Daraus folgt wieder, daß alle Σ-Darstellungen untereinander gleich sind.

(5.13) Hilfssatz: Gegeben sei das P-Ideal

> (5.13.1) $\mathfrak{a} = (f_1, f_2, \ldots, f_s)$, wobei $x_1^{l_1^{(l)}} x_2^{l_2^{(l)}} \ldots x_n^{l_n^{(l)}}$ das PP von f_l mit der höchsten Nummer sei $(l = 1, 2, \ldots, s)$.
> Wenn nun die PP
>
> (5.13.2) $x_1^{G_1^{(k,l)}} x_2^{G_2^{(k,l)}} \ldots x_n^{G_n^{(k,l)}}$, $G_j^{(k,l)} = \mathrm{Max}(l_j^{(k)}, l_j^{(l)})$, $(j = 1, 2, \ldots, n;$ $k, l = 1, 2, \ldots, s)$
>
> (die KGV von $x_1^{l_1^{(k)}} x_2^{l_2^{(k)}} \ldots x_n^{l_n^{(k)}}$ und $x_1^{l_1^{(l)}} x_2^{l_2^{(l)}} \ldots x_n^{l_n^{(l)}}$) durch die Methoden des Algorithmus nur eine Σ-Darstellung erhalten, so haben alle PPR nur eine einzige Σ-Darstellung.

Beweis: (5.13) gilt sicher für die Restklasse von 1. Wir machen die Induktionsannahme: (5.13) gilt bis $x_1^{k_1} x_2^{k_2} \ldots x_n^{k_n}$ ausschließlich. $x_1^{k_1} x_2^{k_2} \ldots x_n^{k_n}$ kann nun alle möglichen $x_1^{l_1^{(l)}} x_2^{l_2^{(l)}} \ldots x_n^{l_n^{(l)}}$ enthalten. Mit $x_1^{l_1^{(l_1)}} x_2^{l_2^{(l_1)}} \ldots x_n^{l_n^{(l_1)}}$ und $x_1^{l_1^{(l_2)}} x_2^{l_2^{(l_2)}} \ldots x_n^{l_n^{(l_2)}}$ enthält es aber auch das KGV der beiden. Auf Grund ganz entsprechender Überlegungen wie beim Beweis von (5.1), Gruppe 3B. sind die Σ-Darstellungen, die sich aus Zerlegungen ergeben, wo ein Teilprodukt $x_1^{l_1^{(l_1)}} x_2^{l_2^{(l_1)}} \ldots x_n^{l_n^{(l_1)}}$ enthält, untereinander gleich, ebenso die Σ-Darstellungen aus Zerlegungen, wo ein Teilprodukt $x_1^{l_1^{(l_2)}} x_2^{l_2^{(l_2)}} \ldots x_n^{l_n^{(l_2)}}$ enthält. Beide Z-Darstellungen sind gleich der Σ-Darstellung aus einer Zerlegung, wo ein Teilprodukt $x_1^{G_1^{(l_1,l_2)}} x_2^{G_2^{(l_1,l_2)}} \ldots x_n^{G_n^{(l_1,l_2)}}$ enthält. Also sind sie auch untereinander gleich. In derselben Weise kann auch die Gleichheit aller möglichen Σ-Darstellungen von $x_1^{k_1} x_2^{k_2} \ldots x_n^{k_n}$ gezeigt werden.

6. Anwendung der Hilfssätze (5.1), (5.8), (5.11) und (5.13) zur Vereinfachung des Algorithmus.

Es liege wieder das Ideal $\mathfrak{a}$ in der Form (5.13.1) vor mit der Zusatzdefinition (5.13.2). $x_1^{G_1^{(p,q)}} x_2^{G_2^{(p,q)}} \dots x_n^{G_n^{(p,q)}}$ sei unter allen $x_1^{G_1^{(k,l)}} x_2^{G_2^{(k,l)}} \dots x_n^{G_n^{(k,l)}}$ dasjenige mit der niedrigsten Nummer ($1 \leq p \leq s$, $1 \leq q \leq s$).

Wenn wir gemäß den Vorschriften des Algorithmus vorgehen, ist $x_1^{G_1^{(p,q)}} x_2^{G_2^{(p,q)}} \dots x_n^{G_n^{(p,q)}}$ das erste PP, das zwei verschiedene Σ-Darstellungen erhalten kann. Deshalb überspringen wir jetzt alle Schritte des Algorithmus bis dahin und berechnen gleich zwei Σ-Darstellungen von $x_1^{G_1^{(p,q)}} x_2^{G_2^{(p,q)}} \dots x_n^{G_n^{(p,q)}}$ auf zwei wesentlich verschiedene Arten, nämlich indem wir $x_1^{G_1^{(p,q)}} x_2^{G_2^{(p,q)}} \dots x_n^{G_n^{(p,q)}}$ einmal so zerlegen, daß ein Teilprodukt Vielfaches von $x_1^{l_1^{(p)}} x_2^{l_2^{(p)}} \dots x_n^{l_n^{(p)}}$ ist, und einmal so, daß ein Teilprodukt Vielfaches von $x_1^{l_1^{(q)}} x_2^{l_2^{(q)}} \dots x_n^{l_n^{(q)}}$ ist. Erhalten wir auf diese Weise tatsächlich zwei verschiedne Σ-Darstellungen, so eliminieren wir daraus die PPR mit der höchsten Nummer, erhalten also die Σ-Darstellung einer PPR, die bisher keine solche besaß. Dieser Darstellung entspricht ein Polynom $f_{t+1} \in \mathfrak{a}$, das wir in die Basis von $\mathfrak{a}$ aufnehmen. Haben wir aber nicht zwei verschiedne Σ-Darstellungen erhalten, so gehen wir zum KGV mit der nächst höheren Nummer über, von dem wir wieder Σ-Darstellungen auf zwei wesentlich verschiedene Arten berechnen.

Jedesmal wenn wir auf diese Weise eine neue Σ-Darstellung gefunden haben, fügen wir das entsprechende Polynom der Basis bei (dem entspricht im alten Algorithmus das Vormerken einer Σ-Darstellung in der Liste S) und gehen zum KGV mit der nächst höheren Nummer über (dem entspricht im alten Algorithmus, daß wir mit einem nächsten Durchgang beginnen, jetzt wissen wir aber genau, wo beim neuen Durchgang das erstemal wieder zwei verschiedene Σ-Darstellungen für eine PPR auftreten können und setzen deshalb mit der Rechnung gleich dort ein).

Wenn bei einem KGV $x_1^{G_1^{(k,l)}} x_2^{G_2^{(k,l)}} \dots x_n^{G_n^{(k,l)}}$ gilt: $G_j^{(k,l)} = l_j^{(k)}$

(oder: $G_j^{(k,l)} = l_j^{(l)}$) für $j = 1, 2, \ldots, n$ (d.h. wenn das KGV gleich einem der beiden PP ist), so berechnen wir die beiden Σ-Darstellungen, fügen ein sich etwa ergebendes neues Polynom der Basis bei, können aber f_k (bzw. f_l) aus der Basis streichen, weil die Beziehung, die wegen $f_k \equiv 0\ (\mathfrak{a})$ ($f_l \equiv 0\ (\mathfrak{a})$) zwischen den Restklassen besteht, jetzt ohnedies schon wegen $f_l \equiv 0 (\mathfrak{a})$ ($f_k \equiv 0 (\mathfrak{a})$) vorliegt.

Sobald die Voraussetzung des Hilfssatzes (5.13) erfüllt ist in bezug auf die gerade vorliegende Basis $\mathfrak{a} = (f_1', f_2', \ldots, f_{s'}')$ des Ideals, können wir den Algorithmus abbrechen. Diejenigen PPR, die weder wegen $f_j' \equiv 0 (\mathfrak{a})$, $(j = 1, 2, \ldots, s')$, noch wegen $x_1^{l_1} x_2^{l_2} \ldots x_n^{l_n} f_j' \equiv 0\ (\mathfrak{a})$ $(l_i = 0, 1, 2, \ldots;\ i = 1, 2, \ldots, n)$, eine Σ-Darstellung haben, sind die Basiselemente des Ideals $\mathfrak{a}$, deren Multiplikationstafel jetzt noch unter Ausnützung aller vorliegenden Σ-Darstellungen $f_j' \equiv 0\ (\mathfrak{a})$ $(j = 1, 2, \ldots, s')$ berechnet werden muß.

Die Berechnung von zwei verschiedenen Σ-Darstellungen eines KGV ist die Hauptarbeit in der praktischen Rechnung. Viele Σ-Darstellungen von PP niedererer Nummer müssen dazu vorbereitet werden. Selbstverständlich wird man diese einmal berechneten Σ-Darstellungen nicht unmittelbar interessanter PP in einem ähnlichen Schema wie beim früheren Algorithmus vormerken, um sie nur einmal berechnen zu müssen. Auf diese Weise werden auch viele Glieder der Multiplikationstafel ständig mitgerechnet.

Bei der Programmierung wurde der Algorithmus in der jetzt besprochenen Form verwendet. Ein "Vormerken" der Σ-Darstellungen nicht unmittelbar wesentlicher PP war wegen des geringen Speicherraumes der verwendeten Maschine nicht möglich und würde bei etwas umfangreicheren Beispielen sofort auch die Kapazität größerer Anlagen überschreiten. Man muß deshalb eine längere Rechenzeit zugunsten einer gewaltigen Speicherraumeinsparung in Kauf nehmen.

Für die Rechnung mit elektronischer Rechenanlage werden wir noch eine Überlegung brauchen: Es ist gleichgültig, in welcher Reihenfolge wir die KGV $x_1^{G_1^{(k,l)}} x_2^{G_2^{(k,l)}} \dots x_n^{G_n^{(k,l)}}$ nehmen, um für sie auf zwei wesentlich verschiedene Arten Σ-Darstellungen zu berechnen. Hat nämlich ein KGV nur eine einzige Σ-Darstellung, wenn die Basis des Ideals in diesem Stadium des Algorithmus gerade $\mathfrak{a}=(f_1', f_2', \dots, f_s')$ ist, so kann dieses KGV auch in einem späteren Stadium, wo alle Beziehungen $f_j' \equiv 0 (\mathfrak{a})$ $(j=1,2,\dots,s')$ und vielleicht noch weitere gelten, nicht zwei verschiedene Σ-Darstellungen erhalten.

Würden wir also die KGV in einer anderen Reihenfolge als in der vorhin beschriebenen nehmen, die wir die normale Reihenfolge nennen wollen, und bekämen wir damit eine Basisdarstellung $\mathfrak{a}=(f_1^*, f_2^*, \dots, f_{s^*}^*)$, so könnten wir darauf wieder den Algorithmus anwenden, diesmal unter Benutzung der normalen Reihenfolge der KGV. Alle diese KGV wurden aber auch schon bei der Rechnung in der anderen Reihenfolge auf zwei wesentlich verschiedene Arten berechnet und ergaben nur mehr eine einzige Σ-Darstellung. Also können sie auch jetzt nicht zwei verschiedene erhalten, wo sicher nicht weniger Beziehungen vorliegen als damals. Die Basis $\mathfrak{a}=(f_1^*, f_2^*, \dots, f_{s^*}^*)$ muß deshalb schon jene sein, die wir auch bei der Rechnung bezüglich der normalen Reihenfolge erhalten hätten.

Wir berechnen im folgenden noch einmal das Beispiel 1, diesmal mit dem Algorithmus in der neuen Form.

Beispiel 1:

$$\mathfrak{a}=(x_1^2-2x_2+x_1,\ x_1x_3-x_3,\ x_3^2-2x_3+x_2).$$

Wir schreiben die Basispolynome in die entsprechenden Beziehungen (1), (2), (3) in $\mathfrak{o}$ um:

(1) $x_1^2 \equiv 2x_2-x_1\ (\mathfrak{a})$	(4) $x_2x_3 \equiv x_3\ (\mathfrak{a})$
(2) $x_1x_3 \equiv x_3\ (\mathfrak{a})$	(5) $x_1x_2 \equiv x_2\ (\mathfrak{a})$
(3) $x_3^2 \equiv 2x_3-x_2\ (\mathfrak{a})$	(6) $x_2^2 \equiv x_2$.

Weiters fertigen wir eine Liste der $x_1^{G_1^{(k,l)}} x_2^{G_2^{(k,l)}} \dots x_n^{G_n^{(k,l)}}$ an, um ihre Reihenfolge feststellen zu können, wobei wir (k,l) und das zugehörige PP $x_1^{G_1^{(k,l)}} x_2^{G_2^{(k,l)}} \dots x_n^{G_n^{(k,l)}}$ angeben, im Ausgangsstadium also (2,1), (3,1) und (3,2):

(2,1) $x_1^2 x_3$	~~(3,1)~~ $\cancel{x_1^2 x_3^2}$	~~(4,1)~~ $\cancel{x_1^2 x_2 x_3}$	(5,1) $x_1^2 x_2$	~~(6,1)~~ $\cancel{x_1^2 x_2^2}$
	(3,2) $x_1 x_3^2$	(4,2) $x_1 x_2 x_3$	(5,2) $x_1 x_2 x_3$	~~(6,2)~~ $\cancel{x_1 x_2^2 x_3}$
		(4,3) $x_2 x_3^2$	~~(5,3)~~ $\cancel{x_1 x_2 x_3^2}$	~~(6,3)~~ $\cancel{x_2^2 x_3^2}$
			(5,4) $x_1 x_2 x_3$	(6,4) $x_2^2 x_3$
				(6,5) $x_1 x_2^2$

$x_1^{a_1^{(k,l)}} x_2^{a_2^{(k,l)}} \cdots x_n^{a_n^{(k,l)}}$, von denen wir wegen (5.11) keine Σ-Darstellungen berechnen müssen, streichen wir sofort durch. Schließlich bereiten wir noch ein Schema vor, um die Hilfsbeziehungen vorzumerken. Hier können wir zu Beginn schon (1), (2) und (3) eintragen.

1

x_1

x_2

x_3

$x_1^2 \equiv 2x_2 - x_1 \ (\alpha)$

$x_1 x_2 \equiv x_2 \ (\alpha)$

$x_1 x_3 \equiv x_3 \ (\alpha)$

$x_2^2 \equiv x_2 \ (\alpha)$

$x_2 x_3 \equiv x_3 \ (\alpha)$

$x_3^2 \equiv 2x_3 - x_2 \ (\alpha)$

x_1^3

$x_1^2 x_2 \equiv x_2 \ (\alpha)$

$x_1^2 x_3 \equiv x_3 \ (\alpha)$

$x_1 x_2^2$

$x_1 x_2 x_3$

$x_1 x_3^2 \equiv 2x_3 - x_2 \ (\alpha)$

x_2^3

$x_2^2 x_3$

$x_2 x_3^2$

x_3^3

Wir beginnen nun, $x_1^2 x_3$ als das KGV mit der niedrigsten Nummer auf zwei Arten zu berechnen.

(6.1a) $x_1^2 x_3 \equiv (x_1^2)\, x_3 \equiv (2x_2 - x_1)\, x_3 \equiv 2x_2 x_3 - \cancel{x_1 x_3} - x_3 \ (\alpha)$

(6.1b) $x_1^2 x_3 \equiv x_1 (x_1 x_3) \equiv x_1 x_3 \equiv x_3 \ (\alpha)$

(Die Reduktion einer Darstellung eines PP als Linearkombination aus anderen PP (mod $\mathfrak{a}$!) auf eine Σ-Darstellung läßt sich mit möglichst geringem Aufwand ausführen, wenn wir weiter darstellbare PP der Darstellung durchstreichen und deren Darstellung an das Ende des Ausdrucks anfügen.)

Aus (6.1a) und (6.1b) läßt sich $x_2x_3 \equiv x_3 (\mathfrak{a})$ gewinnen. Das schreiben wir als (4) unter (3) (wir nehmen $x_2x_3 - x_3$ in die Basis auf!). Ebenso ergänzen wir damit die Liste der Hilfsbeziehungen. Wir erhalten dadurch auch neue KGV, nämlich (4,1), (4,2) und (4,3), die wir im Anschluß an (3,2) hinschreiben. Auch die bei (6.1) berechnete Darstellung $x_1^2x_3 \equiv x_3 (\mathfrak{a})$ merken wir in der Liste der Hilfsbeziehungen vor. Zum Zeichen, daß (2,1) schon verwendet wurde, versehen wir es mit einem Haken.

Jetzt gehen wir an die Berechnung von Σ-Darstellungen für das nächste KGV, nämlich (4,2). Es ergibt sich keine Beziehung, also nehmen wir sofort (3,2):

(6.2a) $x_1x_3^2 \equiv (x_1x_3)x_3 \equiv x_3 \cdot x_3 \equiv \cancel{x_3^2} + 2x_3 - x_2 (\mathfrak{a})$

(6.2b) $x_1x_3^2 \equiv x_1(x_3^2) \equiv x_1(2x_3 - x_2) \equiv 2\cancel{x_1x_3} - x_1x_2 + 2x_3 (\mathfrak{a})$.

Es ergibt sich (5). Wie früher wird auch die Liste der Hilfsbeziehungen und der KGV ergänzt.

Jetzt kommt (5.1) an die Reihe:

(6.3a) $x_1^2x_2 \equiv (x_1^2)x_2 \equiv (2x_2 - x_1)x_2 \equiv 2x_2^2 - \cancel{x_1x_2} - x_2 (\mathfrak{a})$

(6.3b) $x_1^2x_2 \equiv (x_1x_2)x_1 \equiv x_2x_1 \equiv x_2 (\mathfrak{a})$.

Es ergibt sich (6). Wieder machen wir die nötigen Eintragungen in die Vormerklisten.

Auf diese Weise gehen wir weiter. Die weiteren KGV haben jeweils nur mehr eine einzige Σ-Darstellung, wie leicht überprüft werden kann.

Die Arbeitsersparnis, die sich durch die Vereinfachung des Algorithmus ergibt, wird an diesem Beispiel nicht deutlich, sie ist aber bei komplizierteren Idealen beträchtlich. Auch wird man wieder die verschiedenen Listen zu einem einzigen Schema vereinigen.

Der Beweis des Satzes (4.19) kann jetzt leicht geliefert werden. Nehmen wir an, es sei bei der Rechnung mit dem Algorithmus in der früheren Form der in der Voraussetzung von (4.19) beschriebene Zustand eingetreten, in der Liste S mögen dabei $f_1', f_2', \ldots, f_{s'}'$ stehen ($f_j' \overset{\mathrm{DF}}{=} x_1^{l_1^{(j)}} x_2^{l_2^{(j)}} \ldots x_n^{l_n^{(j)}} + \ldots$, $(j = 1, 2, \ldots, s')$, $x_1^{l_1^{(j)}} x_2^{l_2^{(j)}} \ldots x_n^{l_n^{(j)}}$ sei unter den PP von f_j' dasjenige mit der höchsten Nummer). Diejenigen von den PP $x_1^{l_1^{(j)}} x_2^{l_2^{(j)}} \ldots x_n^{l_n^{(j)}}$ mit einem Grad $\geq k+1$ sind laut Voraussetzung selbst Vielfache von irgendeinem anderen $x_1^{l_1^{(p)}} x_2^{l_2^{(p)}} \ldots x_n^{l_n^{(p)}}$, also

$$x_1^{c_1^{(p,j)}} x_2^{c_2^{(p,j)}} \ldots x_n^{c_n^{(p,j)}} = x_1^{l_1^{(j)}} x_2^{l_2^{(j)}} \ldots x_n^{l_n^{(j)}}, \qquad (1 \leq p \leq s', \; p \neq j).$$

Wir müssen für sie auf **zwei** wesentlich verschiedene Arten Σ-Darstellungen berechnen, dann können wir sie aus der Basis entlassen. (Gerade das wird in (4.19) als geschehen vorausgesetzt.) Es bleiben also noch die KGV $x_1^{c_1^{(j_1,j_2)}} x_2^{c_2^{(j_1,j_2)}} \ldots x_n^{c_n^{(j_1,j_2)}}$ zu berechnen übrig zwischen jeweils zwei PP $x_1^{l_1^{(j_1)}} x_2^{l_2^{(j_1)}} \ldots x_n^{l_n^{(j_1)}}$ und $x_1^{l_1^{(j_2)}} x_2^{l_2^{(j_2)}} \ldots x_n^{l_n^{(j_2)}}$ mit Graden $\leq k$. Die $x_1^{c_1^{(j_1,j_2)}} x_2^{c_2^{(j_1,j_2)}} \ldots x_n^{c_n^{(j_1,j_2)}}$ treten aber spätestens beim Grad $2k-1$ auf (mit Zuhilfenahme von (5.11)!).

In der neuen Form kann der Algorithmus für jedes beliebige Ideal angewendet werden, auch wenn wir von vorneherein nichts über seine Dimension wissen. Es kann nämlich jetzt in jedem Stadium entschieden werden, ob noch weiter gerechnet werden muß oder ob schon alle wichtigen Beziehungen gefunden wurden. Durch Anwendung des Algorithmus auf ein beliebiges Ideal $\mathfrak{a} = (f_1, f_2, \ldots, f_s)$ erhalten wir eine Basisdarstellung des Ideals GB

(6.4) $\mathfrak{a} = (f_1', f_2', \ldots, f_{s'}')$ mit

(6.5) $f_j' \overset{\mathrm{DF}}{=} x_1^{l_1^{(j)}} x_2^{l_2^{(j)}} \ldots x_n^{l_n^{(j)}} + \ldots$

(wobei $x_1^{l_1^{(j)}} x_2^{l_2^{(j)}} \ldots x_n^{l_n^{(j)}}$ unter den PP von f_j' dasjenige mit der höchsten Nummer sei),

die die Eigenschaft hat, daß das höchstnummrige PP eines beliebigen Polynoms $f \in \mathfrak{a}$ Vielfaches von mindestens einem der PP $x_1^{l_1^{(j)}} x_2^{l_2^{(j)}} \cdots x_n^{l_n^{(j)}}$ ist. (Gäbe es ein Polynom $f \in \mathfrak{a}$, das diese Eigenschaft nicht hat, so hätte eine PPR u_{i_0}, die durch den Algorithmus als Basiselement festgestellt wurde (siehe S. 12), eine Σ-Darstellung.)

Es sei noch bemerkt, daß in Bezug auf die Anordnung (4.1) der PP nur eine einzige Basis des Ideals mit dieser Eigenschaft gefunden werden kann. Gäbe es nämlich zwei verschiedene solche Basen

(6.6a) $\mathfrak{a} = (f_1', f_2', \ldots, f_{s'}')$ und

(6.6b) $\mathfrak{a} = (f_1'', f_2'', \ldots, f_{s''}'')$

(wobei $x_1^{l_1^{(j)}} x_2^{l_2^{(j)}} \cdots x_n^{l_n^{(j)}}$ $\left(x_1^{k_1^{(i)}} x_2^{k_2^{(i)}} \cdots x_n^{k_n^{(i)}}\right)$ unter den PP von f_j' (f_i''), $j = 1, 2, \ldots, s'$ $(i = 1, 2, \ldots, s'')$ dasjenige mit der höchsten Nummer sei),

so hätte nämlich entweder ein PP in bezug auf die eine Basisdarstellung des Ideals eine Σ-Darstellung, in bezug auf die andere aber keine (wenn unter den $x_1^{l_1^{(j)}} x_2^{l_2^{(j)}} \cdots x_n^{l_n^{(j)}}$ ein PP vorkommt, das unter den $x_1^{k_1^{(i)}} x_2^{k_2^{(i)}} \cdots x_n^{k_n^{(i)}}$ nicht vorkommt oder umgekehrt) oder die Σ-Darstellung von mindestens einem PP wäre in bezug auf die beiden Basisdarstellungen verschieden. Beides steht im Widerspruch zu dem Ergebnis, das die Anwendung des Algorithmus auf ein Ideal hat.

Wenn unter den $x_1^{l_1^{(j)}} x_2^{l_2^{(j)}} \cdots x_n^{l_n^{(j)}}$ $(j = 1, 2, \ldots, s')$ nun PP der Form $x_i^{l_i}$ $(i = 1, 2, \ldots, n)$ vorkommen, so haben alle PP ab einem Grad $\sum_{i=1}^{n} l_i$ sicher eine Σ-Darstellung, dies auf Grund der gleichen Überlegungen wie beim Beweis von (3.1). Es gibt also nur endlich viele linear unabhängige PPR in $\mathfrak{r}$. $\mathfrak{a}$ ist also nulldimensional wegen Satz (3.6). Kommen aber unter den $x_1^{l_1^{(j)}} x_2^{l_2^{(j)}} \cdots x_n^{l_n^{(j)}}$ nicht für alle i PP der Form $x_i^{l_i}$ vor, (z.B. habe kein $x_1^{l_1^{(j)}} x_2^{l_2^{(j)}} \cdots x_n^{l_n^{(j)}}$ die Form $x_k^{l_k}$), dann hat kein PP der Form x_k^{p} $(p = 0, 1, 2, \ldots)$ eine Σ-Darstellung, $\mathfrak{r}$ hat also unendlich viele linear unabhängige Elemente, ist ein hyperkomplexes System mit unendlich vielen Basiselementen im Sinne von (3.5), $\mathfrak{a}$ hat also eine höhere Dimension.

Muß im Laufe des Algorithmus einmal $f \equiv 1$ in die Basis aufgenommen werden, so ist $\mathfrak{a}$ der ganze P-Ring, $\mathfrak{a}$ hat also die Dimension -1. Wir können also mit Hilfe des Algorithmus auch gewisse Aussagen über die Dimension eines beliebigen Ideals machen.

Wenn wir den Algorithmus in seiner zweiten Form auf Ideale $\mathfrak{a} = (f_1(x), f_2(x), \ldots, f_s(x)) \subset k[x]$ anwenden, liefert er uns den größten gemeinsamen Teiler der Basispolynome $f_j(x)$ $(j = 1, 2, \ldots, s)$, ersetzt also den Euklidischen Algorithmus. Dazu ein Beispiel:

Beispiel 2: $\mathfrak{a} = (x^3 - 7x^2 + 11x - 5,\ x^5 - 28x^3 + 16x^2 - 3x - 10,\ x^4 - 2x^3 - 19x^2 + 15x + 25)$

~~(1) $x^3 \equiv 7x^2 - 11x + 5\ (\mathfrak{a})$~~

~~(2) $x^5 \equiv 28x^3 - 16x^2 + 3x + 10\ (\mathfrak{a})$~~

~~(3) $x^4 \equiv 2x^3 + 19x^2 - 15x - 25\ (\mathfrak{a})$~~

~~(4) $x^2 \equiv 7x - 10\ (\mathfrak{a})$~~

(5) $x \equiv 5\ (\mathfrak{a})$.

Wir berechnen zunächst zwei Σ-Darstellungen von x^4. Eine steht schon da: (3). Sie braucht nur mehr durch Verwendung von (1) vereinfacht werden zu:

$$x^4 \equiv \cancel{2x^3} + \cancel{19x^2} - \cancel{15x} - \cancel{25} + \cancel{14x^2} - \cancel{22x} + \cancel{10} + 33x^2 - 37x - 15\ (\mathfrak{a}).$$

Die andere berechnen wir aus (1):

$$x^4 \equiv 7x^3 - \cancel{11x^2} + \cancel{5x} + \cancel{49x^2} - \cancel{77x} + \cancel{35} + 38x^2 - 72x + 35\ (\mathfrak{a}).$$

Es ergibt sich als neue Beziehung (4): $x^2 \equiv 7x - 10\ (\mathfrak{a})$.
(3) kann aus der Basis gestrichen werden. Wir betrachten x^3:

Aus (1): $x^3 \equiv \cancel{7x^2} - \cancel{11x} + \cancel{5} + \cancel{49x} - \cancel{70} + 38x - 65\ (\mathfrak{a})$

Aus (4): $x^3 \equiv \cancel{7x^2} - \cancel{10x} + \cancel{49x} - 70 + 39x\ (\mathfrak{a})$

Es ergibt sich (5): $x \equiv 5\ (\mathfrak{a})$.
(1) kann aus der Basis gestrichen werden. Wir betrachten x^2:

Aus (4): $x^2 \equiv 25\ (\mathfrak{a})$

Aus (5): $x^2 \equiv 5x \equiv 25\ (\mathfrak{a})$.

Es ergibt sich keine neue Beziehung, doch kann (4) aus der Basis gestrichen werden. Auch die Berechnung von x^5 aus (2) und aus (5) liefert dieselbe Σ-Darstellung, (2) kann aus der Basis gestrichen werden. (5) bleibt als einziges Basispolynom übrig und ist der größte gemeinsame Teiler der ursprünglichen drei Basispolynome ([1], S.39).

7. Die Berechnung der Hilbertfunktion eines Ideals aus einer Basis der Art (6.4).

In diesem Abschnitt werden die Symbole und Definitionen von [1], S.154 ff. verwendet. Wenn wir mit den Methoden des Algorithmus für ein Ideal $\mathfrak{a}$ eine Basis der Art (6.4) gefunden haben, so gelten in bezug auf diese zwei Hilfssätze:

(7.1) Hilfssatz: Die Zahl der linear unabhängigen Polynome $\in \mathfrak{a}$ eines Grades $\leq t$ ist gleich der Zahl jener PP eines Grades $\leq t$, die Vielfaches von mindestens einem $x_1^{l_1^{(\iota)}} x_2^{l_2^{(\iota)}} \cdots x_n^{l_n^{(\iota)}}$ sind, wenn

$\mathfrak{a} = (f_1', f_2', \ldots, f_{s'}')$ eine Basis (6.4) von $\mathfrak{a}$ ist,

und $f_\iota' \overset{DF}{=} x_1^{l_1^{(\iota)}} x_2^{l_2^{(\iota)}} \cdots x_n^{l_n^{(\iota)}} + \cdots$

($x_1^{l_1^{(\iota)}} x_2^{l_2^{(\iota)}} \cdots x_n^{l_n^{(\iota)}}$ ist unter den PP von f_ι dasjenige mit der höchsten Nummer), $\iota = 1, 2, \ldots, s'$.

(7.2) Hilfssatz: Die Anzahl der in (7.1) erwähnten PP ist

$$N(t; (f_1', f_2', \ldots, f_{s'}') =$$
$$= H(t-t_1; n-1) + H(t-t_2; n-1) + \cdots + H(t-t_{s'}; n-1) -$$
$$- H(t-t_{1,2}; n-1) - H(t-t_{1,3}; n-1) - \cdots - H(t-t_{s'-1,s'}; n-1) +$$
$$+ \cdots$$
$$\vdots$$
$$+ (-1)^{s'-1} H(t-t_{1,2,\ldots,s'}; n-1),$$

wenn t_ι der Grad von f_ι' ist und $t_{i_1, i_2, \ldots, i_k}$ der Grad von $x_1^{G_1(i_1,i_2,\ldots,i_k)} x_2^{G_2(i_1,i_2,\ldots,i_k)} \cdots x_n^{G_n(i_1,i_2,\ldots,i_k)}$ wobei $G_i^{(i_1,i_2,\ldots,i_k)} = \mathrm{Max}(l_i^{(i_1)}, l_i^{(i_2)}, \ldots, l_i^{(i_k)})$ für $i = 1, 2, \ldots, n$ und $1 \leq i_1 < i_2 < \cdots < i_k \leq s'$, $2 \leq s'$.

Aus diesen beiden Hilfssätzen folgt unmittelbar die folgende Formel zur Berechnung der Hilbertfunktion von $\mathfrak{a}$:

(7.3) $H(t; (f_1, f_2, \ldots, f_s)) = H(t; n-1) - N(t; (f_1', f_2', \ldots, f_{s'}'))$

Für $t<0$ wird dabei $H(t; n)$ durch $H(t; n) = 0$ definiert.

Beweis von (7.1): Zunächst wissen wir, daß es mindestens so viele linear unabhängige Polynome $f \in \mathfrak{a}$ eines Grades $\leq t$

wie PP eines Grades $\leq t$ gibt, die Vielfaches von mindestens einem $x_1^{l_1^{(l)}} x_2^{l_2^{(l)}} \ldots x_n^{l_n^{(l)}}$ $(l=1,2,\ldots,s')$ sind. Denn die Σ-Darstelungen der Restklassen dieser PP sind die Restklassen von Polynomen

(7.4) $f_{i_1 i_2 \ldots i_n} \overset{DF}{=} x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n} + \ldots \in \mathfrak{a}$,

wobei jedes $f_{i_1 i_2 \ldots i_n}$ das PP $x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n}$ als PP mit der höchsten Nummer enthält. Diese PP sind aber linear unabhängig, also kann es eine Beziehung

(7.5) $\sum a_{i_1 i_2 \ldots i_n} f_{i_1 i_2 \ldots i_n} = 0 \quad (a_{i_1 i_2 \ldots i_n} \in K)$

nur für $a_{i_1 i_2 \ldots i_n} = 0$ geben.

Würde nun noch ein Polynom $f^* \in \mathfrak{a}$ mit einem Grad $\leq t$ existieren, das nicht Linearkombination der $f_{i_1 i_2 \ldots i_n}$ wäre, so könnten wir ein Polynom

(7.6) $g = f^* - \sum a_{i_1 i_2 \ldots i_n} f_{i_1 i_2 \ldots i_n} \in \mathfrak{a} \quad (a_{i_1 i_2 \ldots i_n} \in K)$

bilden und dabei die Koeffizienten $a_{i_1 i_2 \ldots i_n}$ so wählen, daß g keines der PP $x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n}$ enthält. Unter den in g verbleibenden PP mit Koeffizienten $\neq 0$ suchen wir nun dasjenige mit der höchsten Nummer, wir nennen es $x_1^{l_1} x_2^{l_2} \ldots x_n^{l_n}$. Seine Restklasse wurde durch den Algorithmus als ein Basiselement festgestellt. (7.6) wird aber in $\mathfrak{a}$ zu

(7.7) $g \equiv 0 \ (\mathfrak{a})$,

wodurch $x_1^{l_1} x_2^{l_2} \ldots x_n^{l_n}$ eine Σ-Darstellung erhält im Widerspruch zu seiner Eigenschaft als Basiselement.

Den Beweis von (7.2) liefern wir mit Induktion nach s'. Im Falle $s'=1$ liefert die Formel $N(t,(f_1)) = H(t-t_1, n-1)$ in Übereinstimmung damit, daß wir $x_1^{l_1^{(1)}} x_2^{l_2^{(1)}} \ldots x_n^{l_n^{(1)}}$ mit sämtlichen PP des Grades $t-t_1$ multiplizieren müssen, um die PP des Grades t zu erhalten, die Vielfaches von $x_1^{l_1^{(1)}} x_2^{l_2^{(1)}} \ldots x_n^{l_n^{(1)}}$ sind. Nehmen wir nun an, die Formel gelte für s' Basispolynome. Die Anzahl der PP, die Vielfaches von mindestens einem der PP

(7.8) $x_1^{l_1^{(l)}} x_2^{l_2^{(l)}} \ldots x_n^{l_n^{(l)}} \quad (l=1,2,\ldots,s'+1)$

sind, können wir nun so zusammenstellen: Wir nehmen sämtliche PP, die Vielfache von den ersten s' PP von (7.8) sind (ihre Anzahl läßt sich auf Grund der Induktionsvoraussetzung berechnen) und fügen dazu sämtliche PP, die Vielfache von $x_1^{l_1^{(s'+1)}} x_2^{l_2^{(s'+1)}} \cdots x_n^{l_n^{(s'+1)}}$ sind, deren Anzahl sich auch schon berechnen läßt. Damit haben wir allerdings einige PP doppelt gezählt, nämlich diejenigen, die Vielfaches von einem $x_1^{G_1^{(j,s'+1)}} x_2^{G_2^{(j,s'+1)}} \cdots x_n^{G_n^{(j,s'+1)}}$ sind ($j = 1, 2, \ldots, s'$; $G_i^{(j,s'+1)} = \operatorname{Max}(l_i^{(j)}, l_i^{(s'+1)})$ für $i = 1, 2, \ldots, n$) und damit schon bei der ersten Gruppe mitgezählt wurden. Auch diese Anzahl läßt sich schon auf Grund der Induktionsvoraussetzung berechnen. Diese PP müssen wir also von der früheren Zahl abziehen. Es ergibt sich:

$$N(t; (f_1, f_2, \ldots, f_{s'+1})) =$$

$$H(t-t_1; n-1) + \cdots + H(t-t_{s'}; n-1) - H(t-t_{1,2}; n-1) - \cdots - H(t-t_{s'-1,s'}; n-1) + \cdots + (-1)^{s'-1} H(t-t_{1,\ldots,s'}; n-1) +$$

$$+ H(t-t_{s'+1}; n-1) -$$

$$-\Big[H(t-t_{1,s'+1}; n-1) + \cdots + H(t-t_{s',s'+1}; n-1) - H(t-t_{1,2,s'+1}; n-1) - \cdots - H(t-t_{s'-1,s',s'+1}; n-1) + \cdots +$$

$$+ (-1)^{s'-1} H(t-t_{1,2,\ldots,s';s'+1}; n-1)\Big] =$$

$$= H(t-t_1; n-1) + H(t-t_2; n-1) + \cdots + H(t-t_{s'+1}; n-1) -$$

$$- H(t-t_{1,2}; n-1) - H(t-t_{1,3}; n-1) - \cdots - H(t-t_{s',s'+1}; n-1) +$$

$$+ \cdots$$

$$\vdots$$

$$+ (-1)^{s'} H(t-t_{1,2,\ldots,s'+1}; n-1) .$$

Dabei wurde noch verwendet, daß das KGV von

$$x_1^{G_1^{(i_1,s'+1)}} \cdots x_n^{G_n^{(i_1,s'+1)}}, \; x_1^{G_1^{(i_2,s'+1)}} \cdots x_n^{G_n^{(i_2,s'+1)}}, \; \ldots, \; x_1^{G_1^{(i_k,s'+1)}} \cdots x_n^{G_n^{(i_k,s'+1)}}$$

gleich dem KGV von

$$x_1^{l_1^{(i_1)}} \cdots x_n^{l_n^{(i_1)}}, \; x_1^{l_1^{(i_2)}} \cdots x_n^{l_n^{(i_2)}}, \; \ldots, \; x_1^{l_1^{(i_k)}} \cdots x_n^{l_n^{(i_k)}}, \; x_1^{l_1^{(s'+1)}} \cdots x_n^{l_n^{(s'+1)}}$$

ist, wobei $1 \leq i_1 < i_2 < \ldots < i_k \leq s'$; $1 \leq k \leq s'$.

Damit haben wir die Möglichkeit, die Hilbertfunktion eines beliebigen Ideals zu berechnen, nachdem seine Basis zuerst mit Hilfe des Algorithmus auf die hier geforderte Form (6.4) gebracht wurde.

8. Bestimmung einer Schranke für das Abbrechen des Algorithmus aus den Basispolynomen des Ideals.

Auf Grund der Überlegungen im Abschnitt 6 kann jetzt versucht werden, schon aus den Basispolynomen $f_1, f_2, \dots, f_s$ eines P-Ideals $\mathfrak{a} = (f_1, f_2, \dots, f_s)$ eine Schranke zu berechnen, bis zu wie hohen Graden höchstens gerechnet werden müssen wird, damit alle Schritte des Algorithmus durchgeführt sind (d.h. die Voraussetzung des Satzes (5.13) erfüllt ist).

Hier sei eine Schranke abgeleitet für den Fall, daß

(8.1) $\qquad \mathfrak{a} = (f_1, f_2, \dots, f_s) \subset K[x_1, x_2]$,

$\qquad\qquad f_j \stackrel{\text{Df}}{=} x_1^{l_1^{(j)}} x_2^{l_2^{(j)}} + \dots$

($j = 1, 2, \dots, s$; $x_1^{l_1^{(j)}} x_2^{l_2^{(j)}}$ ist dasjenige PP unter den PP von f_j, das die höchste Nummer hat).

Wir werden noch folgende Größen brauchen:

(8.2a) $\quad l_j^{(l,k)} = \operatorname{Max}(l_j^{(l)}, l_j^{(k)})$, $\quad j = 1, 2$, $\quad l = 1, 2, \dots, s-1$; $\quad k = l+1, \dots, s$;

(8.2b) $\quad K^{(l,k)} = l_1^{(l,k)} + l_2^{(l,k)}$

(8.2c) $\quad K = \operatorname{Max}(K^{(l,k)})$, $\quad l = 1, 2, \dots, s-1$; $\quad k = l+1, \dots, s$;

(8.2d) $\quad l_1 = \operatorname{Min}(l_1^{(l)}) = l_1^{(l_1)}$, $\quad l = 1, 2, \dots, s$; $\quad 1 \leq l_1 \leq s$

(8.2e) $\quad l_2 = \operatorname{Min}(l_2^{(l)}) = l_2^{(l_2)}$, $\quad l = 1, 2, \dots, s$; $\quad 1 \leq l_2 \leq s$

(8.2f) $\quad l = l_1 + l_2$

Zunächst gilt, daß es höchstens I PP des Grades K ohne Σ-Darstellung gibt, nämlich $x_1^K, x_1^{K-1}x_2, \dots, x_1^{K-l_2+1}x_2^{l_2-1}$ und $x_1^{l_1-1}x_2^{K-l_1+1}, x_1^{l_1-2}x_2^{K-l_1+2}, \dots, x_2^K$. $x_1^{K-l_2}x_2^{l_2}$ bis $x_1^{l_1^{(l_2)}}x_2^{K-l_1^{(l_2)}}$ sind Vielfache von $x_1^{l_1^{(l_2)}}x_2^{l_2^{(l_2)}}$, $x_1^{l_1^{(l_2)}-1}x_2^{K-l_1^{(l_2)}+1}$ bis $x_1^{l_1}x_2^{K-l_1}$ sind Vielfache von $x_1^{l_1^{(l_1)}}x_2^{l_2^{(l_1)}}$. Dazu ist nur zu zeigen, daß

(8.3a) $\quad K - l_1^{(l_2)} + 1 \geq l_2^{(l_1)}$ oder

(8.3b) $\quad K + 1 \geq l_1^{(l_2)} + l_2^{(l_1)}$.

Das stimmt, denn

$$(8.3c)\quad K = \mathrm{Max}(K^{(l,k)} = \mathrm{Max}(\mathrm{Max}(l_1^{(l)}, l_1^{(k)}) + \mathrm{Max}(l_2^{(l)}, l_2^{(k)})) \geq$$
$$\geq \mathrm{Max}(l_1^{(l_2)}, l_1^{(l_1)}) + \mathrm{Max}(l_2^{(l_2)}, l_2^{(l_1)}) = l_1^{(l_2)} + l_2^{(l_1)}$$

Aus denselben Überlegungen heraus gibt es auch höchstens I PP eines Grades $t > K$ ohne Σ-Darstellung. Hat ein PP eines Grades $\leq$ zwei verschiedene Σ-Darstellungen, aus denen die Σ-Darstellung eines bisher nicht darstellbaren PP $x_1^{l_1^{(s+1)}} x_2^{l_2^{(s+1)}}$ gewonnen werden kann, so kann $x_1^{l_1^{(s+1)}} x_2^{l_2^{(s+1)}}$ höchstens wieder den Grad K haben. Ist nun $l_1^{(s+1)} \geq l_1$ und $l_2^{(s+1)} \geq l_2$, so gilt:

$$(8.4)\quad K \geq l_1^{(s+1,k)} + l_2^{(s+1,k)}, \quad k = 1,2,\dots,s; \quad l_j^{(s+1,k)} = \mathrm{Max}(l_j^{(s+1)}, l_j^{(k)}), \ j = 1,2.$$

Das heißt also, daß die neuen KGV alle einen Grad $\leq K$ haben. Das beweisen wir so: Da $x_1^{l_1^{(s+1)}} x_2^{l_2^{(s+1)}}$ bisher noch keine Σ-Darstellung besaß, muß $l_2^{(s+1)} < l_2^{(l_1)}$ und $l_1^{(s+1)} < l_1^{(l_2)}$ sein. Dann gilt auch:

$$(8.5)\quad l_1^{(s+1,k)} + l_2^{(s+1,k)} \leq l_1^{(s+1,l_2)} + l_2^{(s+1,l_1)} = l_1^{(l_2)} + l_2^{(l_1)} \leq K, \quad (k = 1,2,\dots,s),$$

wenn man berücksichtigt, daß bis zum Grad K schon alle Polynome aus der Basis ausgeschieden wurden, deren PP mit der höchsten Nummer Vielfaches von einem anderen $x_1^{l_1^{(l)}} x_2^{l_2^{(l)}}$ ist, und deshalb gilt:

$$(8.6)\quad l_1^{(k)} \geq l_1, \ l_2^{(k)} < l_2^{(l_1)}, \ l_2^{(k)} \geq l_2, \ l_1^{(k)} < l_1^{(l_2)} \qquad (k = 1,2,\dots,s; \ k \neq l_1, \ k \neq l_2)$$
$$l_2^{(k)} = l_2^{(l_1)} \text{ für } k = l_1, \quad l_1^{(k)} = l_1^{(l_2)} \text{ für } k = l_2.$$

Wenn also $x_1^{l_1^{(s+1)}} x_2^{l_2^{(s+1)}}$ und eines der $x_1^{l_1^{(l)}} x_2^{l_2^{(l)}}$ ein KGV hat mit einem Grad $> K$, so muß entweder $l_1^{(s+1)} < l_1$ oder $l_2^{(s+1)} < l_2$ sein. Wenn wir nun l_1 und l_2 neu definieren

$$(8.7a)\quad l_1 = \mathrm{Min}(l_1^{(l)}), \quad l = 1,2,\dots,s+1 \quad \text{und}$$

$$(8.7b)\quad l_2 = \mathrm{Min}(l_2^{(l)}), \quad l = 1,2,\dots,s+1,$$

so können wir sagen, es muß sich l_1 oder l_2 gegenüber früher verringert haben. Das heißt aber auch, daß es jetzt bei den Graden $t \geq K$ weniger PPR ohne Σ-Darstellungen gibt als früher. Die neuen KGV von $x_1^{l_1^{(s+1)}} x_2^{l_2^{(s+1)}}$ und $x_1^{l_1^{(l)}} x_2^{l_2^{(l)}}$ $(l = 1,2,\dots,s)$ müssen beim Grad 2K alle aufgetreten sein. Beim Grad 2K kann man dieselben Schlüsse wieder anwenden: entweder es verringert sich durch eine neu auftretende Beziehung l_1 oder

l_2 oder alle neuen KGV treten schon vor dem Grad 2K auf. Im ersten Fall treten die neuen KGV vor dem Grad $K+2K=3K$ auf. Auf diese Weise können wir weitergehen. Im ganzen kann sich $l=l_1+l_2$ nur l-mal verringern und damit die Schranke erhöhen.

Wenn also $l=1$ ist, so treten alle jemals zu berechnenden KGV vor dem Grad $K^{(1)}=2K$ auf,
ist $l=2$, so vor dem Grad $K^{(2)}=K+K^{(1)}=3K$
ist $l=3$, so vor dem Grad $K^{(3)}=K^{(1)}+K^{(2)}=5K$.
So gehen wir rekursiv weiter: wenn $l=L$, so treten die KGV vor dem Grad $K^{(L)}=K^{(L-2)}+K^{(L-1)}$ auf.

Um zu einer direkten Formel zu gelangen, müssen wir die Abschätzung etwas vergröbern und sagen:

Für $l=1$ treten die KGV vor $K^{(1)}=2K$ auf,
für $l=2$ treten die KGV vor $K^{(2)}=2K^{(1)}=2^2 K$ auf,
.
.
.
für $l=L$ treten die KGV vor

(8.8) $K^{(L)}=2^L\cdot K$ auf,

wie ein leichter Induktionsschluß liefert.

Freilich wird der Algorithmus in den meisten Fällen schon bei sehr viel kleineren Graden abbrechen. (8.8) hat deshalb nur theoretischen Wert und sagt aus, daß der Algorithmus bei einem beliebigen P-Ideal $\subset K[x_1,x_2]$ bei gewissen, v o r h e r bestimmbaren Graden sicher schon abgebrochen werden kann.

9. Die Programmierung des Algorithmus.

Um den Algorithmus mit elektronischer Rechenanlage zu bearbeiten, müssen wir uns zuerst überlegen, wie in solchen Anlagen mit Polynomen gerechnet werden kann. Dann werden wir grobe Flußdiagramme für den Algorithmus sowie für das wichtigste Unterprogramm (Gewinnung einer Σ-Darstellung für eine PPR) angeben, die auf den Ablauf so weit eingehen, wie das ohne Berücksichtigung der speziellen Eigenschaften einer bestimmten Rechenanlage möglich ist. Im Anschluß daran beschreiben wir die für die ZUSE Z 23 V vorhandenen zwei Programme, indem wir zunächst kurz Eigenheiten dieser beiden Programme angeben und dann beschreiben, wie die Daten eingegeben werden müssen und in welcher Form die Ergebnisse erscheinen. In den Flußdiagrammen wird ein neues Symbol verwendet: $a \Leftarrow b$. Das soll bedeuten: der neue Wert von a ergibt sich aus dem bisherigen Wert von b, mit der häufigen Anwendung: $a \Leftarrow a+1$, und ähnlichen, was in Worten heißt: der neue Wert von a ergibt sich aus dem bisherigen Wert von a durch Addition von 1.

Das Rechnen mit Polynomen in Rechenanlagen.

Hier geht es erstens darum, PP darzustellen, und zweitens, diese zu Polynomen zu vereinigen. Um PP darzustellen, wurden zwei verschiedene Wege verfolgt. Der eine ordnet jedem PP die ihm in der Anordnung (4.1) zukommende Nummer zu und rechnet mit diesen Nummern. Auf diese Weise brauchen wir zur Darstellung eines PP nur eine einzige Zelle, können innerhalb gewisser Grenzen mit beliebig vielen Variablen beliebig hoher Grade rechnen, brauchen aber für die einzelnen Operationen mit PP (wie Multiplikation, Bildung des KGV und ähnliche) zeitraubende Unterprogramme. Der andere Weg stellt die Exponenten eines PP $x_1^{i_1} x_2^{i_2} \dots x_n^{i_n}$ als eine einzige Zahl dar. Wie das geschieht, kann am schnellsten an einem Beispiel gezeigt werden. Nehmen wir $n=3$ und $i_1=2$, $i_2=1$, $i_3=4$, dann würde die dem entsprechende Zahl 20104 lauten. Auf diese Weise lassen sich Exponenten ≤ 99 verarbeiten, wir belegen mit einem PP auch nur eine Zelle, die Unterprogramme für die Operationen mit PP werden wesentlich vereinfacht (vor allem die Multiplikation von PP: diese geschieht jetzt einfach durch Addition der beiden entsprechenden Zahlen). Freilich können wir nur mehr mit einer beschränkten Anzahl von Variablen (in unserem Falle mit 5) rechnen, weil in einer Zelle nur Zahlen mit beschränkter Stellenzahl darstellbar sind. Für den ersten Weg sei hier noch eine grundlegende Formel angegeben, nämlich diejenige, die es gestattet, aus der Anzahl der Variablen n, den Expononenten $i_1, i_2, \ldots, i_n$ und dem Grad $t = \sum_{j=1}^{n} i_j$ die dem PP $x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n}$ in der Anordnung (4.1) zukommende Nummer $N(i_1, i_2, \ldots, i_n)$ auszurechnen. Sie lautet:

$$(9.1) \quad N(i_1, i_2, \ldots, i_n) = \sum_{\tau=0}^{t-1} H(\tau; n-1) + H(t; n-1) - \sum_{j=1}^{n-1} \sum_{\tau = t+2-\sum_{l=1}^{j} i_l}^{t+1-\sum_{l=1}^{j-1} i_l} H(\tau-1; n-1-j)$$

mit der Definition:

$$(9.1a) \quad \sum_{\tau=k}^{l} m_\tau = 0 \qquad \text{für } l < k .$$

Der Teilausdruck

$$(9.1b) \quad \sum_{\tau=0}^{t-1} H(\tau; n-1)$$

von (9.1) gibt die Anzahl der PP des Grades $< t$ aus n Variablen, der Rest ergibt also die Nummer des PP innerhalb des betrachteten Grades t. Wir beweisen induktiv nach t und n. Zunächst gilt die Formel für $t = 0$ und alle n. Für diesen Fall errechnet die Formel:

$$(9.2) \quad N(0, 0, \ldots, 0) = \sum_{\tau=0}^{0} H(\tau; n-1) - \sum_{j=1}^{n-1} \sum_{0+2-0}^{0+1-0} H(\tau-1; n-1-j) = H(0; n-1) = 1$$

in Übereinstimmung damit, daß es für alle n vom Grade o nur ein PP gibt und dieses die Nummer 1 bekommt. Formel (9.1) gilt auch für $n = 1$ und alle t. Sie ergibt in diesem Fall:

$$(9.3) \quad N(i_1) = \sum_{\tau=0}^{t} H(\tau; 0) - 0 = \sum_{\tau=0}^{t} 1 = t+1$$

in Übereinstimmung damit, daß für $n = 1$ bei jedem Grad nur ein einziges PP auftritt und dieses deshalb die Nummer $t+1$ erhält.

Wir nehmen nun an, (9.1) gelte für n und alle τ sowie für $n+1$ und alle Grade τ bis zum Grad t. Wir zeigen, daß die Formel dann auch für $n+1$ Variable und den Grad $t+1$ gilt. Gegeben seien also $i_1, i_2, \dots, i_{n+1}$ mit $\sum_{j=1}^{n+1} i_j = t+1$. Die PP eines Grades $t+1$ setzen sich zusammen aus denen mit $i_1 \neq 0$, welche einfach die mit x_1 multiplizierten PP von $n+1$ Variablen des Grades t sind, und denen mit $i_1 = 0$, deren Anordnung durch die Anordnung der PP des Grades $t+1$ aus den n Variablen $x_2, x_3, \dots, x_{n+1}$ bestimmt ist. In beiden Fällen läßt sich die Formel wegen der Induktionsvoraussetzung anwenden. Im Falle $i_1 = 0$ gilt:

(9.4) $\qquad N(0; i_2, \dots, i_{n+1}) = N_1 + N_2 + N_3$,

wobei $N_1 = \sum_{\tau=0}^{t} H(\tau, n)$ die Anzahl der PP eines Grades $\tau \leq t$ aus $n+1$ Variablen,

$N_2 = H(t, n)$ die Anzahl der PP des Grades $t+1$ aus den $n+1$ Varialben $x_1, x_2, \dots, x_{n+1}$ mit $i_1 \neq 0$,

und $N_3 = H(t+1, n-1) - \sum_{j=1}^{n-1} \sum_{r=(t+1)+2-\sum_{l=2}^{j+1} i_l}^{(t+1)+1-\sum_{l=2}^{j} i_l} H(r-1; n-1-j)$ die Nummer des PP innerhalb der PP des Grades $t+1$ aus den $n+1$ Variablen $x_1, x_2, \dots, x_{n+1}$ mit $i_1 = 0$ ist (mit (9.1) errechnet).

N wird durch die Indexsubstitution $k-1=j$ und nachheriges Wiederersetzen von k durch j zu:

$$N_3 = H(t+1, n-1) - \sum_{j=2}^{n} \sum_{r=(t+1)+2-\sum_{l=2}^{j} i_l}^{(t+1)+1-\sum_{l=2}^{j-1} i_l} H(r-1; n-j)$$

Es ist also:

$$N(0; i_2, i_3, \dots, i_{n+1}) = \sum_{\tau=0}^{t+1} H(\tau, n) - \sum_{j=1}^{n} \sum_{r=(t+1)+2-\sum_{l=1}^{j} i_l}^{(t+1)+1-\sum_{l=1}^{j-1} i_l} H(r-1; n-j),$$

weil $\sum_{l=2}^{k} i_l = \sum_{l=1}^{k} i_l$ wegen $i_1 = 0$

und $\sum_{r=(t+1)+2-\sum_{l=1}^{1} i_l}^{(t+1)+1-\sum_{l=1}^{0} i_l} H(r-1; n-1) = 0$ wegen (9.1a).

Im Falle $i_1 \neq 0$ gilt:

(9.5) $\qquad N(i_1, i_2, \dots, i_{n+1}) = M_1 + M_2$, wobei

(9.5a) $\quad M_1 = \sum_{\tau=0}^{t} H(\tau; n)$ die Anzahl der PP eines Grades $\tau \leq t$ aus $n+1$ Variablen ist,

und die Nummer des PP $x_1^{i_1} x_2^{i_2} \dots x_{n+1}^{i_{n+1}}$ innerhalb des Grades

$t+1$ so berechnet wird (mit $i_1' = i_1 - 1$, $i_j' = i_j$ $(j = 2,3,\dots,n+1)$):

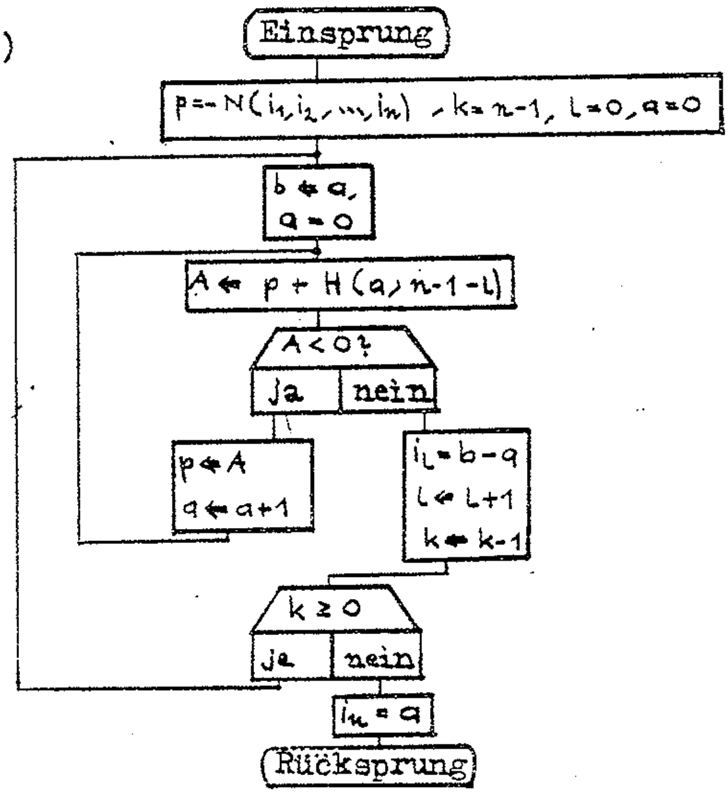
(9.5b) $$M_2 = N(i_1', i_2', \dots, i_{n+1}') - \sum_{\tau=0}^{t-1} H(\tau, n) =$$

$$= H(t,n) - \sum_{j=2}^{n} \sum_{r=t+2-\sum_{l=1}^{j-1} i_l'}^{t+1-\sum_{l=1}^{j-1} i_l'} H(r-1, n-j) - \sum_{r=t+2-i_1'}^{t+1-0} H(r-1, n-1) =$$

$$= H(t+1,n) - \cancel{H(t+1, n-1)} - \sum_{j=1}^{n} \sum_{r=(t+1)+2-\sum_{l=1}^{j-1} i_l}^{(t+1)+1-\sum_{l=1}^{j-1} i_l} H(r-1, n-j) + \cancel{H((t+1)+1-1, n-1)}.$$

(9.5a) und (9.5b) zusammengesetzt ergibt also die Richtigkeit von (9.1) auch für den Fall $i_1 \neq 0$. Die Rückverwandlung der Nummern in die $i_1, i_2, \dots, i_n$ bei gegebenem n geschieht algorithmisch nach folgendem Ablaufschema (dabei wird $-t$ als i_0 mitberechnet):

(9.6)



H(

$H(t,n) = \binom{t+n}{n}$

$\binom{(t+1)+n}{n} = \binom{k}{n} - \binom{k}{n-1}$

Dieses Flußdiagramm gilt für $n=1$. Nehmen wir an, es gilt für n Variable und betrachten wir $p = -N(i_1, i_2, \dots, i_{n+1})$. Im Falle von n Variablen wird $i_1, i_2, \dots, i_n$ ab 1 berechnet, nachdem die verwendeten Größen durch die bei der Berechnung von i_0 durchlaufenen Teile des Flußdiagramms auf folgende Werte gesetzt sind: p ist die Nummer von $x_1^{i_1} x_2^{i_2} \dots x_n^{i_n}$ unter den PP

des Grades t, negativ genommen, $l=1$, $k=n-2$, $b=t$, $a=0$.
Im Falle von $n+1$ Variablen wird t und i_1 richtig berechnet, wie ein schrittweises genaues Durchführen der Anweisungen des Flußdiagramms bestätigt. Danach stehen bei der Marke (1) die verwendeten Größen auf folgenden Werten: p ist die Nummer von $x_2^{i_2} x_3^{i_3} \dots x_{n+1}^{i_{n+1}}$ unter den PP aus den n Variablen $x_2, x_3, \dots, x_{n+1}$ des Grades $t-i_1$, negativ genommen, $l=2$, $k=n-2$ $b=$ Grad des PP $x_2^{i_2} x_3^{i_3} \dots x_{n+1}^{i_{n+1}}$, $a=0$. Nach Induktionsvoraussetzung berechnet das Ablaufschema genau $i_2, i_3, \dots, i_{n+1}$, wenn wir mit diesen Werten bei (1) eingehen. $l=2$ hat nur die Wirkung, daß die noch zu errechnenden Exponenten die Indizes $2, 3, \dots, n+1$ erhalten und das zweite Argument $(n+1)-1-l$ von $H(a, (n+1)-1-l)$ die richtigen Werte für den Fall der n Variablen $x_2, x_3, \dots, x_{n+1}$ annimmt. Das ist aber gerade die hier erforderliche Wirkung.

Polynomrestklassen

$$f \overset{\mathrm{Df}}{=} x_1^{i_1} x_2^{i_2} \dots x_n^{i_n} + \sum a_{i_1 i_2 \dots i_n} x_1^{i_1} x_2^{i_2} \dots x_n^{i_n} \equiv 0 \ (\mathfrak{a})$$

($x_1^{i_1} x_2^{i_2} \dots x_n^{i_n}$ sei unter den PP von f. dasjenige mit der höchsten Nummer; $a_{i_1 i_2 \dots i_n} \in K$)
wurden in der Maschine in der Form

$$x_1^{i_1} x_2^{i_2} \dots x_n^{i_n} \equiv -\sum a_{i_1 i_2 \dots i_n} x_1^{i_1} x_2^{i_2} \dots x_n^{i_n} \ (\mathfrak{a})$$

so dargestellt, daß in die erste von mehreren aufeinanderfolgenden Zellen die Anzahl der PP $x_1^{i_1} x_2^{i_2} \dots x_n^{i_n}$ mit Koeffizienten $\neq 0$ gespeichert wurde, in die nächste $x_1^{i_1} x_2^{i_2} \dots x_n^{i_n}$ (als Nummer oder Zahl), in die nächste der erste Koeffizient $\neq 0$, in die darauffolgende das zugehörige PP (als Nummer oder Zahl) und so fort bis zum letzten Koeffizienten $\neq 0$ und dem zugehörigen PP. Auf eine bestimmte Anordnung der PP $x_1^{i_1} x_2^{i_2} \dots x_n^{i_n}$ innerhalb des Polynoms wurde nicht wertgelegt, jedoch bei jeder Operation mit Polynomrestklassen dafür gesorgt, daß die Ergebnisrestklasse wieder nur PP mit Koeffizienten $\neq 0$ gespeichert hat, also "dicht aufgeschlossen" ist. K wurde als Körper der rationalen Zahlen angenommen. Zähler und Nenner eines Koeffizienten wurden in zwei getrennten Zellen gespeichert, sodaß also eigentlich jeder Koeffizient zwei Zellen beansprucht. Eigene Unterprogramme müssen die Rechenoperationen zwischen den auf diese Weise dargestellten rationalen Zahlen bewerkstelligen. Die einzelnen Polynome wurden in

Zeilen regelbarer Länge angeordnet. Beim Überschreiten dieser Länge (sowie beim Überschreiten je er anderen Grenze, die für die Rechnung gesteckt werden muß, zum Beispiel für die höchstens zu bewältigende Anzahl von Polynomen, für den höchst zulässigen Zahlbereich, für die maximale Anzahl speicherbarer Basiselemente und ähnliches) müssen Anzeigen eingebaut sein, die dieses Überschreiten melden, um falsche Resultate zu vermeiden, die beim Weiterrechnen entstehen. (Diese Anzeigen werden im Flußdiagramm nicht eingezeichnet, um die Übersichtlichkeit nicht zu verschlechtern.)

Flußdiagramm für den Algorithmus.

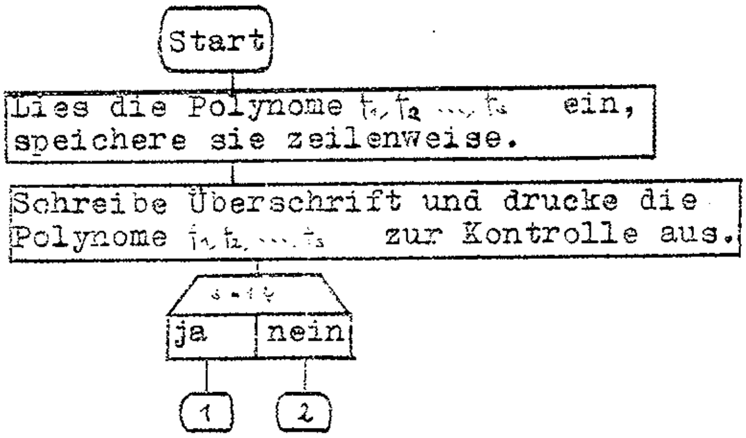
Gegeben sei das Ideal $\mathfrak{a} = (f_1, f_2, \dots, f_s) \subset K[x_1, x_2, \dots, x_n]$,

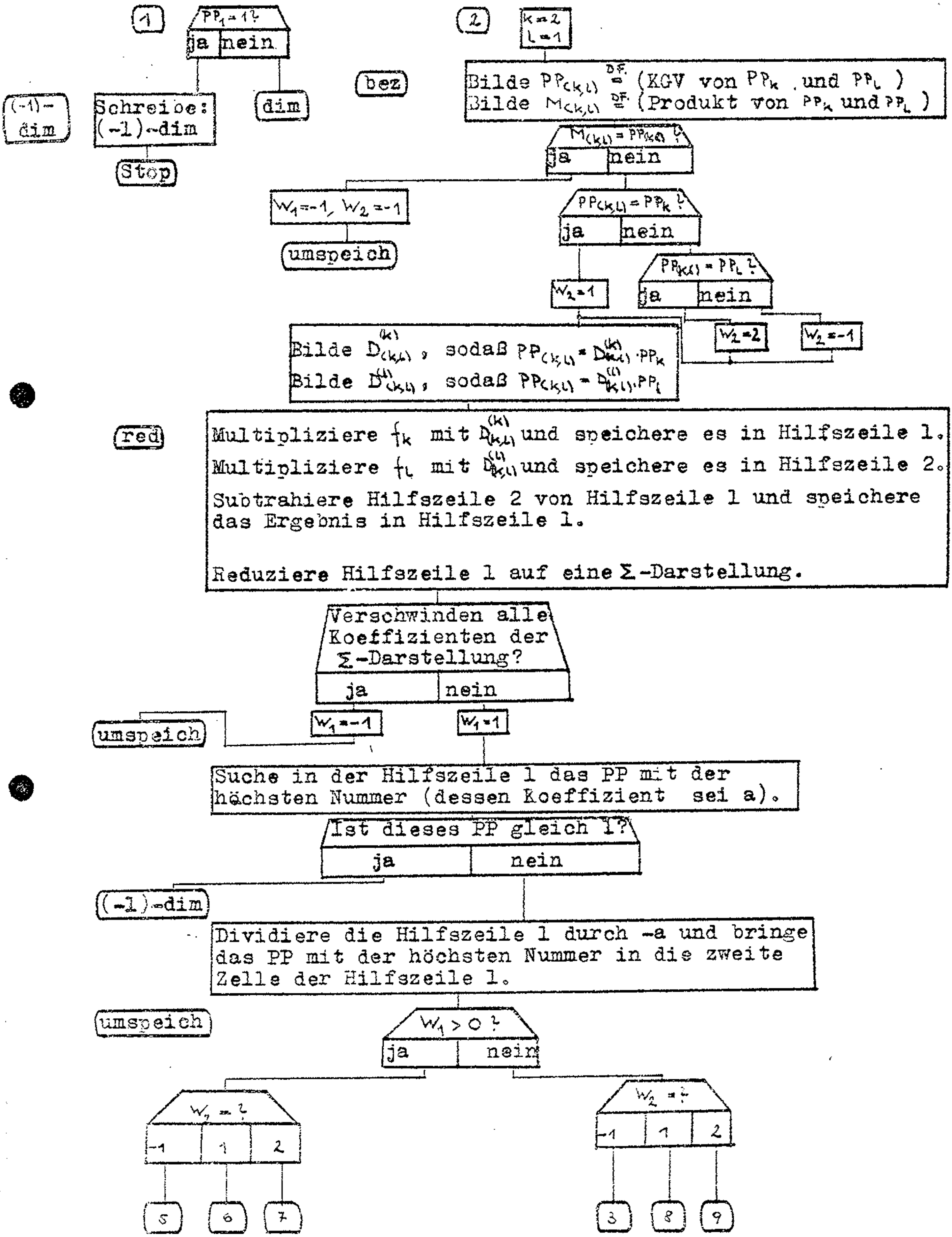
$$f_j = x_1^{i_1^{(j)}} x_2^{i_2^{(j)}} \cdots x_n^{i_n^{(j)}} + \sum a^{(j)}_{i_1 i_2 \dots i_n} x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n} =$$

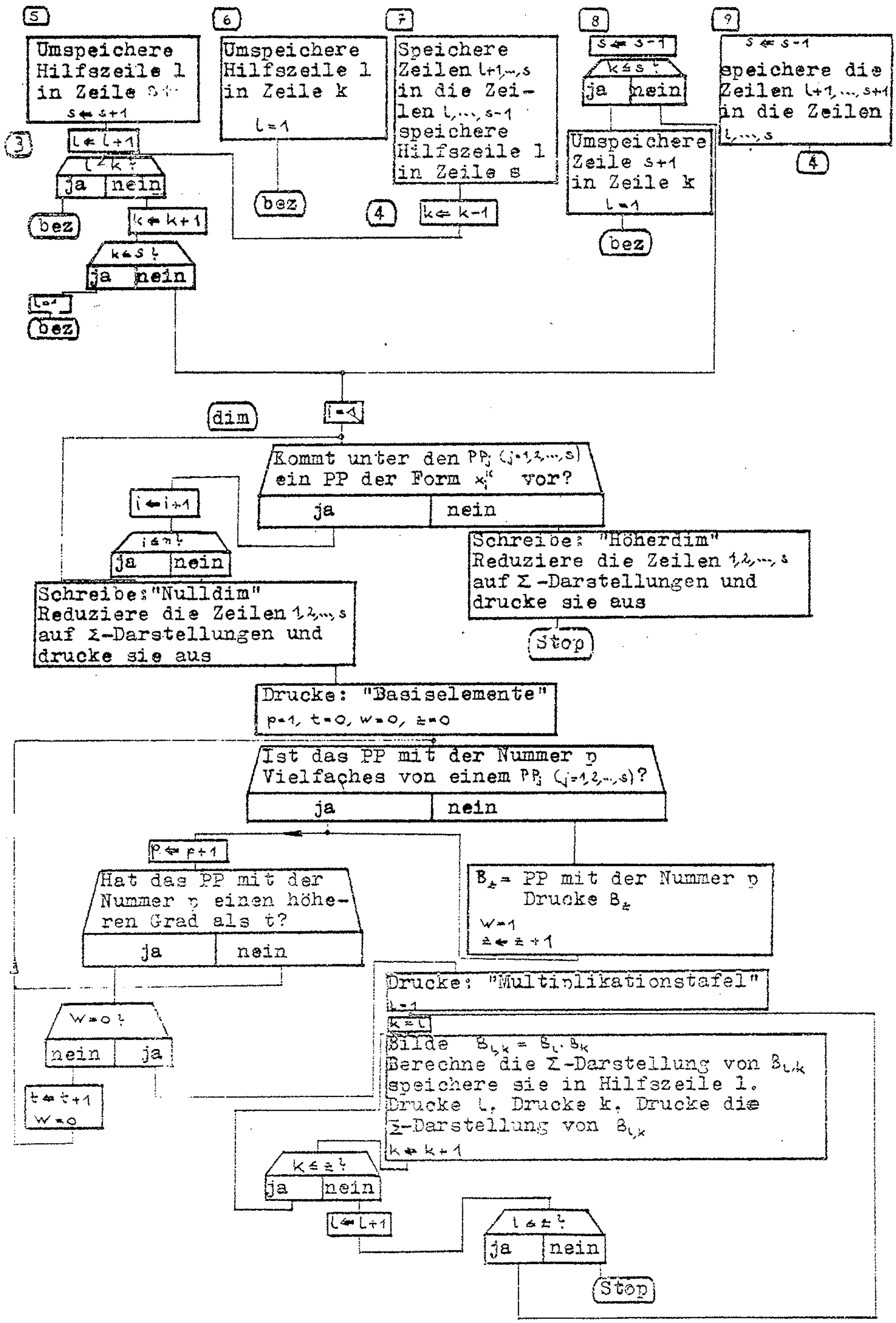
$$= PP_j + \sum_{i=1}^{t_j} a_i^{(j)} PP_i^{(j)}$$

($x_1^{i_1^{(j)}} x_2^{i_2^{(j)}} \cdots x_n^{i_n^{(j)}} = PP_j$ ist unter den PP von f_j dasjenige mit der höchsten Nummer; $a^{(j)}_{i_1 i_2 \dots i_n} \in K$; $PP_i^{(j)}$ seien die $x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}$, die bei Koeffizienten $a^{(j)}_{i_1 i_2 \dots i_n} \neq 0$ stehen, in irgendeiner Anordnung geschrieben).

Ein grobes Flußdiagramm für den Algorithmus in der im Abschnitt 6 beschriebenen Form schaut dann so aus (Hilfsbeziehungen werden nicht gespeichert, die KGV werden in folgender Reihenfolge verwertet: Das KGV von PP_k und PP_l kommt vor dem KGV von PP_p und PP_q, wenn $k<p$ oder $k=p$ und $l<q$!):




1
PP1 = 1?
ja
nein
(-1)-dim
Schreibe:
(-1)-dim
Stop
dim
bez
2
k = 2
l = 1
Bilde PP(k,l) =DF (KGV von PPk und PPl)
Bilde M(k,l) =DF (Produkt von PPk und PPl)
M(k,l) = PP(k,l) ?
ja
nein
W1 = -1, W2 = -1
umspeich
PP(k,l) = PPk ?
ja
nein
W2 = 1
PP(k,l) = PPl ?
ja
nein
W2 = 2
W2 = -1
Bilde D(k)(k,l), sodaß PP(k,l) = D(k)(k,l)·PPk
Bilde D(l)(k,l), sodaß PP(k,l) = D(l)(k,l)·PPl
red
Multipliziere fk mit D(k)(k,l) und speichere es in Hilfszeile 1.
Multipliziere fl mit D(l)(k,l) und speichere es in Hilfszeile 2.
Subtrahiere Hilfszeile 2 von Hilfszeile 1 und speichere das Ergebnis in Hilfszeile 1.
Reduziere Hilfszeile 1 auf eine Σ-Darstellung.
Verschwinden alle Koeffizienten der Σ-Darstellung?
ja
nein
umspeich
W1 = -1
W1 = 1
Suche in der Hilfszeile 1 das PP mit der höchsten Nummer (dessen Koeffizient sei a).
Ist dieses PP gleich 1?
ja
nein
(-1)-dim
Dividiere die Hilfszeile 1 durch -a und bringe das PP mit der höchsten Nummer in die zweite Zelle der Hilfszeile 1.
umspeich
W1 > 0 ?
ja
nein
W2 = ?
-1
1
2
5
6
7
W2 = ?
-1
1
2
3
8
9

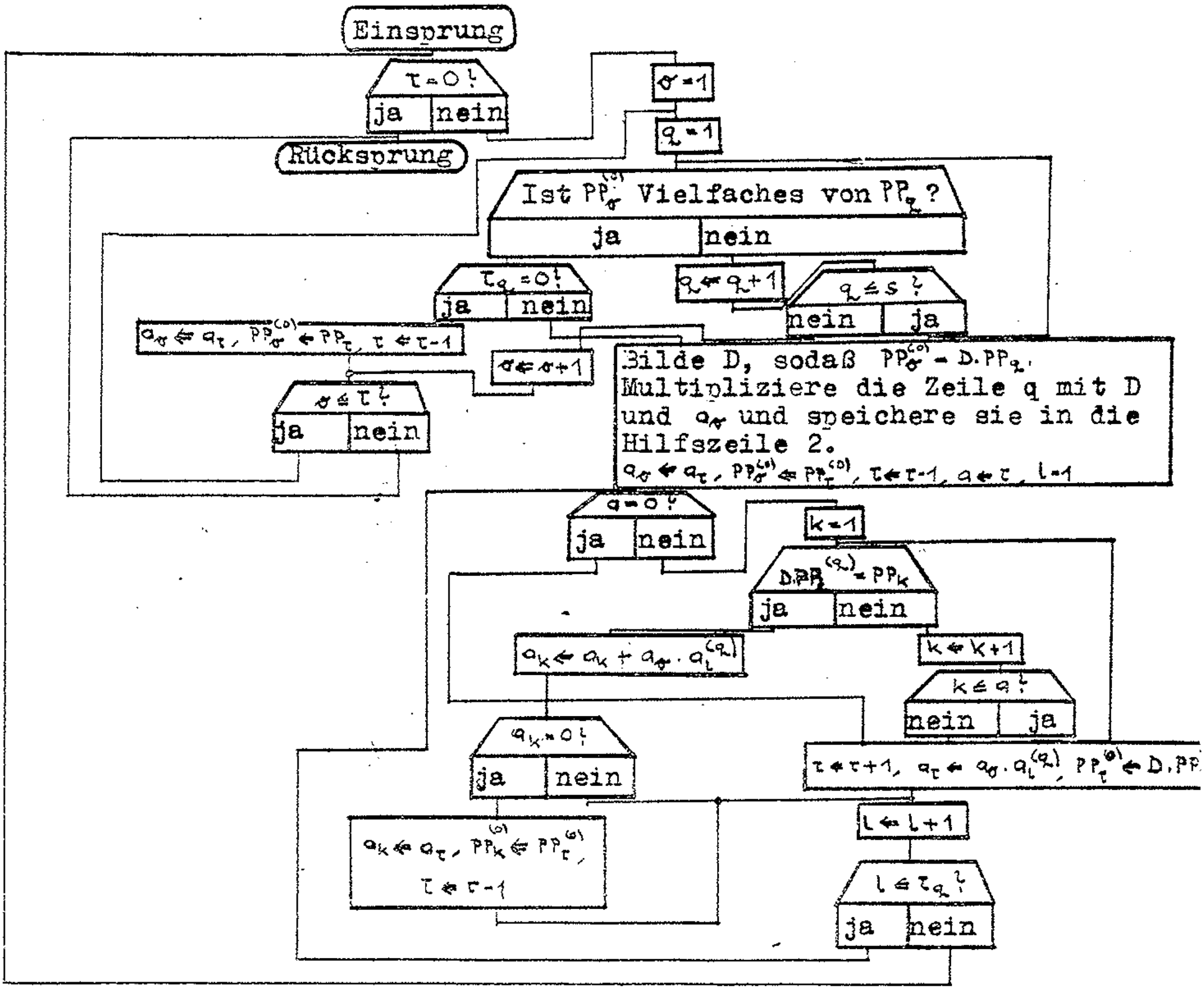


5
Umspeichere Hilfszeile 1 in Zeile s+1
s ⇐ s+1
3
l ⇐ l+1
l ≤ k ?
ja
nein
bez
k ⇐ k+1
k ≤ s ?
ja
nein
l=1
bez
6
Umspeichere Hilfszeile 1 in Zeile k
l=1
bez
7
Speichere Zeilen l+1,...,s in die Zeilen l,...,s-1
speichere Hilfszeile 1 in Zeile s
4
k ⇐ k-1
8
s ⇐ s-1
k ≤ s ?
ja
nein
Umspeichere Zeile s+1 in Zeile k
l=1
bez
9
s ⇐ s-1
speichere die Zeilen l+1,...,s+1 in die Zeilen l,...,s
4
dim
i=1
Kommt unter den PP_j (j=1,2,...,s) ein PP der Form x_i^k vor?
ja
nein
i ⇐ i+1
i ≤ n ?
ja
nein
Schreibe: "Nulldim"
Reduziere die Zeilen 1,2,...,s auf Σ-Darstellungen und drucke sie aus
Schreibe: "Höherdim"
Reduziere die Zeilen 1,2,...,s auf Σ-Darstellungen und drucke sie aus
Stop
Drucke: "Basiselemente"
p=1, t=0, w=0, z=0
Ist das PP mit der Nummer p Vielfaches von einem PP_j (j=1,2,...,s)?
ja
nein
p ⇐ p+1
Hat das PP mit der Nummer p einen höheren Grad als t?
ja
nein
B_z = PP mit der Nummer p
Drucke B_z
w=1
z ⇐ z+1
w=0 ?
nein
ja
t ⇐ t+1
w=0
Drucke: "Multiplikationstafel"
l=1
k=l
Bilde B_{l,k} = B_l · B_k
Berechne die Σ-Darstellung von B_{l,k}
speichere sie in Hilfszeile 1.
Drucke l, Drucke k, Drucke die Σ-Darstellung von B_{l,k}
k ⇐ k+1
k ≤ z ?
ja
nein
l ⇐ l+1
l ≤ z ?
ja
nein
Stop

Flußdiagramm für die Reduktion der Darstellung einer PPR durch andere PPR niedererer Nummer auf eine Σ-Darstellung.

In der Hilfszeile 1 sei die Beziehung $PP_0 = \sum_{i=1}^{\tau} a_i PP_i^{(0)}$ (α) (PP_0 und $PP_i^{(0)}$ sind Potenzprodukte, $a_i \neq 0, a_i \in K, (i=1,2,\dots,\tau)$ in folgender Form gespeichert: $\tau, PP_0, a_1, PP_1^{(0)}, \dots, a_\tau, PP_\tau^{(0)}$,

in den Zeilen $1,2,\dots,s$ die Basisbeziehungen $PP_j = \sum_{i=1}^{\tau_j} a_i^{(j)} PP_i^{(j)}$ (α) ($j=1,2,\dots,s$ PP_j und $PP_i^{(j)}$ sind Potenzprodukte, PP_j hat eine höhere Nummer als $PP_i^{(j)}$ $(i=1,2,\dots,\tau_j)$, $a_i^{(j)} \neq 0$, $a_i^{(j)} \in K$, $(i=1,2,\dots,\tau_j)$) in entsprechender Form. Die Umwandlung von $\sum_{i=1}^{\tau} a_i PP_i^{(0)}$ in eine Σ-Darstellung liefert dann folgender Ablauf:



Beschreibung des ersten Programms
(Protokoll siehe Anhang 1a)

Das erste Programm für die ZUSE Z 23 V ist in seinen groben Teilen im Formelübersetzer geschrieben, einer algorithmischen Programmiersprache, die ungefähr dem Algol entspricht. Die oft sich wiederholenden Teile (Bruchzahlrechnen und Operationen mit PP) sind jedoch in dem an den Interncode der Maschine angepaßten Freiburger Code programmiert. Die Darstellung der PP geschieht in diesem Programm auf dem Wege der Zuordnung von Nummern zu den einzelnen PP unter Verwendung der Formel (9.1) und des Algorithmus (9.6). Die Verwendung des Formelcodes und dieser Darstellung der PP hat sich im Rahmen der Rechengeschwindigkeiten dieser Maschine als zu zeitraubend erwiesen. Damit ist das Programm praktisch wertlos. Trotzdem sei es hier angeführt, weil es den allgemeinen Fall von n Variablen behandelt und ein Programm für schnellere Maschinen, die jedoch einer Programmierung im Interncode nicht zugänglich sind, wohl in einer ähnlichen Form erstellt werden müßte.

Das vorhin gegebene Ablaufdiagramm ist bei diesem Programm in zwei Punkten wesentlich geändert:

1. Bei jedem neuen Durchlaufen des Teiles bez werden die Darstellungen der PP_j $(j = 1, 2, \ldots, s)$ neuerlich zu Σ-Darstellungen reduziert.
2. Im Teil red werden die Hilfszeilen 1 und 2 getrennt auf Σ-Darstellungen reduziert und erst dann voneinander abgezogen.

Die zweite Änderung ist zeitlich von Nachteil, die erste kann besonders bei komplizierten Beispielen einen zeitlichen Vorteil bringen. Um den Gebrauch des Programms zu beschreiben, sei gezeigt, wie der Datenstreifen und das Ergebnisblatt für das Ideal

$$(9.9) \qquad \mathfrak{a} = (x_3^2 - \tfrac{1}{2}x_1^2 - \tfrac{1}{2}x_2^2,\ x_1x_3 - 2x_3 + x_1x_2,\ x_1^2 - x_2)$$

ausschauen: siehe Anhang 2.

<u>Beschreibung des zweiten Programms</u>
(Protokoll siehe Anhang 1b)

Das zweite Programm wurde zur Gänze im Freiburger Code programmiert unter Verwendung eines Hilfsprogramms, das symbolische Adressierung ermöglicht (was im Gegensatz zur Verwendung des Formelübersetzers auf die Rechenzeit keinen negativen Einfluß hat). Es wurde im besonderen darauf Wert gelegt, daß Wartezeiten auf dem langsamen Trommelspeicher vermieden wurden. (Auf diese Weise kann die Rechenzeit im allgemeinen bis auf das sechzehnfache verkürzt werden.) Außerdem wurden die PP auf die zweite Art, nämlich als Zahlen dargestellt. Durch diese drei Umstände sowie noch kleinere Verbesserungen konnte die Rechenzeit auf das 2o- bis 25-fache verkürzt werden (und zugleich der verwendbare Speicherraum vergrößert werden), sodaß sich die Rechnung mit elektronischer Rechenanlage wohl rentiert. Wieder geben wir Datenstreifen und Ergebnisblatt für das Ideal (9.9): siehe Anhang 3. Die Darstellung der PP als Zahlen wird hier insofern noch ein wenig abgeändert, daß als erster Teil einer solchen Zahl auch noch der Grad des PP angegeben wird: 2o2oooo ist also das PP x_1^2.

Bei beiden Programmen besteht die Möglichkeit, durch Einstellen einer Bedingungstaste auf dem Bedienpult auf den Wert 17, die Polynome, die neu in die Basis aufgenommen werden müssen, ausdrucken zu lassen mit Angabe der beiden Potenzprodukte PP_k und PP_l , aus denen $PP_{(k,l)}$ gebildet wurde, das die zwei verschiedenen Σ-Darstellungen liefert. Das ergibt im Falle des Ideals (9.9) folgendes Bild: Anhang 4.

Bei dem zweiten Programm können auch sehr leicht Änderungen eingebaut werden, um theoretische Vermutungen und Überlegungen über die Gesetzmäßigkeiten des Algorithmus in der praktischen Rechnung zu beobachten. Weiters besteht die Möglichkeit, den Speicher anders zu organisieren, das heißt, entweder viele kurze oder wenig lange Polynome zu speichern. Beim Ideal (9.9) braucht das Programm 2 min 46 sek um die Basis (6.4) zu finden und weitere 59 sek, um die Multiplikationstafel zu berechnen. Dazu kommen noch 3 min 13 sek, um die Ergebnisse auszugeben.

Zum Abschluß sei noch ein Beispiel eines Ideals in $K[x_1, x_2, x_3, x_4, x_5]$ gegeben, das als höherdimensional festgestellt wird: siehe Anhang 5.

10. Zusammenfassung.

Nachdem im Abschnitt 3 die Struktur des Restklassenringes eines nulldimensionalen P-Ideals als die eines hyperkomplexen Systems aufgezeigt wurde, wird im Abschnitt 4 schrittweise ein Algorithmus eingeführt, sodaß von ihm in seiner endgültigen Form behauptet werden kann, daß er tatsächlich die Aussonderung einer Basis des hyperkomplexen Systems leistet. Für das Abbrechen des Algorithmus in dieser Form werden die Kriterien (4.14) und (4.19) abgeleitet. Mit 4 Hilfssätzen des Abschnittes 5, die Angaben über das Auftreten von neuen Beziehungen zwischen Restklassen beim Algorithmus machen, kann im Abschnitt 6 der Algorithmus noch weiter vereinfacht und auf eine etwas veränderte Form gebracht werden (sodaß er spezialisiert auf den Fall einer einzigen Variablen x den Euklidischen Algorithmus zur Bestimmung des größten gemeinsamen Teilers mehrerer Polynome ersetzt). Im Abschnitt 7 werden Ergebnisse des Abschnittes 5 auf die Berechnung der Hilbertfunktion eines beliebigen P-Ideals, im Abschnitt 8 auf die Bestimmung einer Schranke für das Abbrechen des Algorithmus aus den Basispolynomen $f_1, f_2, \ldots, f_s$ eines beliebigen P-Ideals $\subset K[x_1, x_2]$ angewendet. Schließlich werden im Abschnitt 9 Vorbereitungen für die Programmierung des Algorithmus durchgeführt, die wichtigsten Flußdiagramme angegeben und schließlich Beispiele mit den tatsächlich vorhandenen Programmen für die ZUSE Z 23 berechnet.

Verwendete Literatur:

[1] Gröbner, W.: Moderne algebraische Geometrie, Wien und Innsbruck, Springer-Verlag 1949.

[2] Waerden, B.L. van der: Moderne Algebra I, 2., verbesserte Auflage, Springer-Verlag 1937.