Computeralgebra

Zusammenfassung

Inhaltsverzeichnis

1 Was ist das Hier?

Dieses Dokument ist eine Zusammenfassung von Fragen und kurzen Antworten zur Computeralgebra basierend auf Prüfungsfragen. Die Antworten verwenden zahlreiche Zusatzliteratur und sind vor allem nicht auf formale Exaktheit, sondern auf Verständnis und "Vortragbarkeit" ausgerichtet.

2 Fragensammlung

Hier sind die Fragen mit kurzen Antworten.

2.1 Grundlagen

- **Was ist ein Körper der Charakteristik** 0**?**

  Ein Körper in dem eine endliche Summe von 1-ern nie 0 ergibt.

- **Was ist eine multiplikative Einheit?**

  Multiplikative Einheit ist ein Element der multiplikativen Halbgruppe eines Ringes, das ein Inverses besitzt.

- **Was ist ein Integritätsbereich?**

  Integritätsbereich ist ein kommutativer Ring mit 1 ohne Nullteiler.

- **Was ist ein Ideal in einem kommutativen Ring?**

  Idel ist eine Teilmenge die abgeschlossen bezüglich der Multiplikation mit Ringelementen, Addition ist und die 0 enthält.

- **Was ist ein echtes Ideal in einem kommutativen Ring?**

  Ein echtes idel ist ein Ideal, das nicht gleich dem ganzen Ring ist, bzw. wenn es nicht die 1 bzw. wenn es keine multiplikativen Einheiten enthält.

- **Was ist ein Hauptideal?**

  Ein Hauptideal wird von einem Element erzeugt.

- **Was ist ein Hauptidealbereich?**

  Ein Hauptidealbereich ist ein Bereich (z.B. Ring) in dem jedes Ideal von einem Element erzeugt wird.

- **Welche Beispiele von Hauptidealbereichen kennen Sie?**

  $\mathbb{Z}$, Univariate Polynomringe, jeder Euklidische Ring ist ein Hauptidealbereich.

- **Was ist ein** GGT**?**

  Der grösste gemeinsame Teiler einer Menge von Ringelementen, falls er existiert teilt alle Elemente dieser Menge und für jedes Element, dass dies auch tut gilt, dass es kleiner ist als das GGT.

- **Kann man die** GGT**-Berechnung einer Menge auf die** GGT**-Berechnung zweier Elemente zurückführen?**

  Ja. Der GGT einer Vereinigung zweier Mengen ist das GGT der GGT's dieser Mengen.

- **Welcher Zusammenhang besteht zwischen dem** GGT **einer Menge und dem davon erzeugten Ideal in einem Haupidealbereich?**

  Das Ideal erzeugt vom GGT einer Menge ist gleich dem Ideal erzeugt von der Menge selbst.

- **Gibt es Integritätsbereiche, in denen stets ein** GGT **existiert, die aber keine Hauptidealbereiche sind?**

  Ja. Z.B. die multivariaten Polynomringe.

- **Was besagt der Teilerkettensatz?**

  Es gibt keine unendlichen strikt aufsteigenden Folge von Idealen in einem Hauptidealbereich. Es gibt auch keine unendlichen Ketten von Elementen, sodass der Nachfolger den Vorgänger teilt und jedes Kettenglied kein teiler aller seiner Nachfolger ist.

- **Wann sind zwei Elemente teilerfremd?**

  Wenn der GGT davon gleich 1 ist.

- **Wann heisst ein Element irreduzibel?**

  Wenn es keine Einheit ist und aus einer Produktzerlegung stets Folgt, dass einer der Faktoren eine Einheit ist.

- **Wann heisst ein Element prim?**

  Wenn es keine Einheit ist und wenn aus der Teilbarkeit eines Produktes stets die Teilbarkeit eines der Faktoren folgt.

- **Welcher Zusammenhang besteht zwischen Primelementen und irreduziblen Elementen?**

  Allgemein ist jedes Primelement irreduzibel. Die Umkehrung ist im Allgemeinen falsch. In einem Hauptidealbereich oder in einem faktoriellen Bereich gilt die Äquivalenz.

- **Wie berechnet man den** GGT **in** $\mathbb{Z}$**?**

  Mit dem Euklidschen Algorithmus.

- **Wie bestimmt man den** GGT **als eine Linearkombination der erzeugenden Elemente in** $\mathbb{Z}$**?**

  Mit dem erweiterten Euklidischen Algorithmus, indem man zusätzlich die Kofaktoren aufsammelt.

- **Warum terminiert der Euklidische Algorithmus?**

  Die Summe aller Elemente ist eine Abstiegsfunktion.

- **Warum ist das Euklidische Algorithmus korrekt?**

  Vor, nach und bei jedem Schleifendurchlauf gelten die Invarianten, die die Idealgleicheit, Endlichkeit und Nichttrivialität der betrachteten Menge fixieren.

- **Ist der Euklidische Algorithmus in $\mathbb{Z}$ deterministisch?**

  Nein. Die Auswahl in der Schleife ist frei.

- **Ist der GGT eindeutig?**

  Im Allgemeinen Nicht. Im Sinne der Eindeutigkeit bis auf multiplikative Einheiten ja.

2.2 Univariater Fall

- **Wie berechnet man den GGT in einem Polynomenring?**

  Mit dem Euklidschen Algorithmus für Polynome aufbauend auf der Polynomreduktion (oder Polynomdivision) mit Rest.

- **Welche Voraussetzungen muss der Polynomenring erfüllen, damit man die normale Polynomdivision einsetzen kann?**

  Der Koefizientenring muss ein Körper sein.

- **Wie bestimmt man den GGT als eine Linearkombination der erzeugenden Elemente in einem Polynomring?**

  Mit dem erweiterten Euklidischen Algorithmus für Polynome, indem man zusätzlich die Kofaktoren aufsammelt.

- **Ist der Divisionsalgorithmus für univariate Polynome eindeutig?**

  Ja. Es gibt genau eine Darstellung $f = DIV * p + REST$.

- **Warum terminiert der Euklidische Algorithmus für Polynome?**

  Die Summe aller (Grade + 1) ist eine Abstiegsfunktion.

- **Warum ist das Euklidische Algorithmus korrekt?**

  Vor, nach und bei jedem Schleifendurchlauf gelten die Invarianten, die die Idealgleicheit, Endlichkeit und Nichttrivialität der betrachteten Menge fixieren.

- **Besitzt der GGT die gleichen Nullstellen, wie das Ausgangssysem?**

  Ja. Denn $Id(F) = Id(GGT(F))$ und $V_L(F) = V_L(Id(F))$ für ein endliches Polynomensystem F.

- **Was ist der quadratfreie Anteil?**

  Das ist das Produkt aller verschiedenen Primfaktoren in eiener Primfaktorzerlegung.

- **Wie berechnet man den quadratfreien Anteil?**

  Den GGT von f und f' berechnen. Der Quotient von f und $GGT(f, f')$ ergibt den quadratfreien Anteil.

- **Was hat der quadratfreie Anteil mit der Primfaktorzerlegung zu tun?**

  Ist $u \prod_{i=0}^{n} p_i^{e_i}$ dann ist der quadratfreie Anteil in einem algebraisch abgeschlossenen Körper $\prod_{i=0}^{n} p_i$. Somit ist der quadratfreie Anteil gerade das Produkt der (verschiedenen) Primfaktoren (ohne Potenzen).

- **Was ist eine quadratfreie Zerlegung?**

  Fasst man in einer Primfaktorzerlegung Faktoren mit gleichen Exponenten zusammen, so ist das Produkt der entsprechenden Potenzen dieser eine quadratfreie Zerlegung.

- **Was kann man über die Faktoren der quadratfreien Zerlegung aussagen?**

  Sie sind teilerfremd und quadratfrei.

- **Sind die Faktoren einer quadratfreien Zerlegung eindeutig?**

  Nur bis auf multiplikative Einheiten. Die Eindeutigkeit kann man erlangen, indem man zusätzlich die Normiertheit verlangt.

- **Wie berechnet man eine quadratfreie Zerlegung?**

  Definiert man rekursiv eine Folge von Polynomen, sodass jedes nächste aus dem GGT des vorherigen und seiner Ableitung berechnet wird, so ist die Folge der Quotienten von je zwei benachbarten Polynomen gerade die Folge der Faktoren in der quadratfreien Zerlegung (nicht potenziert).

- **Wenn Sie die Zahl der komplexen Nullstellen eines Gleichungssystems in $\mathbb{Q}[X]$ bestimmen wollen, wie gehen sie vor?**

  GGT aller Polynome berechnen. Dann beschreibt das GGT die gemeinsamen Nullstellen aller Polynome. Dann quadratfreien Anteil des GGT's berechnen. Dann ist der Grad des quadratfreien Anteils die Anzahl der Nullstellen in einem geeignet gewählten algebraisch vollständigen Erweiterungskörper (z.B. $\mathbb{C}$ für $\mathbb{Q}$).

- **Wie erkennt man am quadratfreien Anteil die Anzahl der komplexen Nullstellen?**

  Das ist der Grad des quadratfreien Anteils.

- **Wie bestimmt man die Anzahl komplexer Nullstellen für ein polynomielles Gleichungssystem mit Nebenbedingungen aus polynomiellen Ungleichungen?**

  Man berechnet das Produkt aller Nebenbedingungen g, den quadratfreien Anteil des GGT aller Polynome im Gleichungssystem f^* und bestimmt dann die Anzahl der Nullstellen (in dem Fall Grad) des Qutienten

  $$h = \frac{f^*}{GGT(f^*, g)}$$

  Die Idee ist, die Nullstellen aller Nebenbedingungen aus der Nullstellenmenge des Gleichungssystems zu entfernen. h ist quadratfrei also ist der Grad gleich der Anzahl der komplexen Nullstellen.

- **Was ist eine Resultante?**

  Die resultante zweier Polynome ist die Determinante der Sylvester-Matrix dieser Polynome.

- **Was kann man mit hilfe der Resultante bestimmen?**

  Zwei Polynome haben genau dann eine gemeinsame Nullstelle in einem Erweiterungskörper, wenn ihre Resultante 0 ist.

- **Was ist eine Determinante?**

  Die Determinante eines Polynoms ist die Resultante des Polynoms mit seiner Ableitung.

- **Was kann man mit Hilfe der Determinanten bestimmen?**

  Ein Polynom ist genau dann quadratfrei, wenn seine Determinante ungleich 0 ist.

- **Wie sieht die Sturm-Sylvester Kette aus?**

  Für ein quadratfreies Polynom und f und g mit $GGT(f,g) = 1$ eine rekursiv definierte Folge $f_0 = f$, $f_1 = f'g$, $f_{i+1} = -REST(f_{i-1}, f_i)$. Das Ende der Folge ist durch das 0-Polynom definiert.

- **Was kann man über den Grad des letzten Polynoms in der Sturm-Sylvester-Kette sagen, das nicht 0 ist?**

  Das ist konstant.

- **Wie geht der Satz von Sturm-Sylvester?**

  Für quadratfreies f und ein teilerfremdes g ($GGT(f,g) = 1$) und $a < b$ mit $f(a)f(b) \neq 0$.

  $$N(f,g,1,(a,b)) - N(f,g,-1,(a,b)) = ZW(S(f,g)(a)) - ZW(S(f,g)(b))$$

- **Wie berechnen sie da die Zahl der reellen Nullstellen, eines endlichen Polynomensystems, wenn sie keine Ungleichungen haben?**

  Quadratfreien Anteil des GGT's aller Polynome berechnen, Cauchy-Schwanken $a < b$ bestimmen, Sturmsche Kette Bilden und $N(f,1,1,(a,b))$ berechnen.

- **Wie berechnet man mit dem Satz von Sturm-Sylvester die Anzahl der Nullstellen, wenn g nicht konstant 1?**

  Direkt mit dem Satz von Sturm-Sylvester.

- **Was sind isolierende Intervalle?**

  Ein isolierendes Interval für eine Nullstelle ist entweder ein Punkt für eine rationale Nullstelle oder ein Interval mit genau einer reellen Nullstelle ($N(f,1,1,(a,b)) = 1$).

- **Wie berechnet man isolierende Intervalle?**

  Ausgehend von Cauchy-Schranken durch iteriertes Halbieren der Intervalle. Findet man dabei eine rationale Nullstelle α, so teilt man durch $(X - \alpha)$.

- **Wie sehen die Cauchy-Schranken aus?**

  $$M = \max(1, \frac{|a_0|}{|a_n|} + ... + \frac{|a_{n-1}|}{|a_n|})$$

  $$N = 1 + \max(\frac{|a_0|}{|a_n|}, ..., \frac{|a_{n-1}|}{|a_n|})$$

- **Wie berechnet man die Anzahl der reellen Nullstellen eines polynomiellen Gleichungssystems mit nebenbedingungen aus polynomiellen Ungleichungen?**

  Man führt die Ungleichnungen auf eine Nebenbedingung, mit der man nach Sturm-Sylerster die Nullstellen bestimmt.

- **Wie bestimmt man die rationalen Nullstellen eines Polynoms?**

  Durch Probieren aller solcher Brüche, sodass der Zähler ein Teiler vom konstanten Anteil und der Nenner ein Teiler vom höchstem Koefizienten ist.

- **Kann man die Anzahl der rationalen Nullstellen eines univariaten Polynoms bestimmen?**

  Nein. Nach Hilbert-Matijasevich ist das definitiv algorithmisch unmöglich.

- **Wenn man die isolierenden Intervalle hat, dann wollen sie vielleicht wissen, ob eine rationale Nullstelle in denen enthalten ist, geht das irgendwie?**

  Man sucht einfach die rationalen Nullstellen durch Probieren im gegebenen Interval.

- **Wie faktorisiert man univariante Polynome?**

  Mit hilfe des modifizierten Kronecker-Algoritmus.

- **Was ist die Idee des Kronecker-Algorithmus?**

  Man Probiert alle teiler von Funktionswerten an gegebenen Stützstekllen, die gerade keine Nullstellen sind. Durch Lagrange-Interpolation sucht man dann nach einem Polynom, das das gegebene Teilt.

- **Warum ist der modifizierte Kronecker-Algorithmus korrekt?**

  Es gilt $b_i = f(a_i) = g(a_i)h(a_i)$ für eine Produktzerlegung von $f = gh$. Somit ist $g(a_i)$ ein Teiler von b_i. Wegen der Eindeutigkeit der Lagrange-Interpolation ist das durch die Stützstzellen interpolierte Polynom gerade ein Faktor in der gesuchten Zerlegung.

- **Warum terminiert der Kronecker-Algorithmus?**

  Die Anzahl der durchzuprobierenden Fälle ist endlich.

- **Wie ist die Effizienz vom Kronecker-Algorithmus zu bewerten?**

  Zu viele Kombinationen der Teiler fürhen zu viel zu vielen Interpolationsschritten.

2.3 Multivariater Fall

- **Wieso kann man im multivariaten nicht genauso vorgehen wie im univariaten?**

  Der multivariate Polynomenring ist kein Hauptidealbereich, sondern ein Noetherscher Bereich. Allerdings besitzt jedes Ideal eine endliche Basis.

- **Beweisen Sie, dass der multivariate Polynomenring kein Hauptidealbereich ist?**

  Das Ideal $Id(x,y)$ besitzt keine einelementige Basis.

- **Besitzt der multivariate Polynomenring die Eigenschaft der eindeutigen Primfaktorzerlegun?**

  Bis auf multivariate multiplikative Einheiten.

- **Was ist eine Termordnung?**

  Für eine Termordnung gilt, dass das 1-Polynom das kleinste Element ist und für alle Terme die monotonie der Multiplikation gilt.

- **Welche Ordnungen kennen Sie?**

  Lexikographische, Invers-Lexikographische, Totalgrad mit invers bzw. lexikographischen Ordnung.

- **Gibt es im multivariaten einen GGT?**

  Ja. Der GGT ist das Produkt aller gemeinsamen Primfaktorpotenzen in einer Primfaktorzerlegung. Allerdings besitzt das GGT nicht die Eigenschaft die Linearkombination aller Komponenten zu sein.

- **Wie lässt sich die Lösung von Systemen mit Nebenbedingungen aus Ungleichungen auf ein System von Gleichungen reduzieren?**

  Der Rabinowitsch-Trick besagt, dass man das Produkt aller Ungleichungsfaktoren g mit einer neuen Unbestimmten Y in das Gleichungssystem in der Form $h = gY - 1$ aufnemmen kann.

- **Welche grundlegenden Probleme über Varietäten gibt es?**

  Ist eine Varietät endlich und wenn ja, was ist ihre Kardinalität? Eingrenzung der Punkte der Varietät durch Intervale mit rationalen Endpunkten.

- **Was ist ein Noetherscher Bereich?**

  Ein Bereich in dem jedes Ideal endlicherzeugt ist.

- **Was besagt der Hilbertsche Basissatz?**

  Der multivariate Polynomenring über einem Körper ist ein Noetherscher Bereich.

- **Was ist eine Halbordnung?**

  Reflexive, transitive, antisymmetrische Relation.

- **Was ist eine Basis einer Ordnung?**

  Eine Menge, sodass für jedes Element ein Element der Basis existiert, das kleiner ist.

- **Was ist die Dickson-Eigenschaft?**

  Jede nichtleere Teilmenge besitzt eine endliche Basis.

- **Was ist eine fundierte Halbordnung?**

  Wenn jede nichtleere Teilmenge mindestens ein minimales Element besitzt.

- **Was ist eine Wohlordnung?**

  Wenn jede nichtleere Teilmenge ein kleinstes Element besitzt.

- **Welche Beziehungen gelten zwischen Ordnungen?**

  Wohlordnungen haben die Dickson-Eigenschaft. Dickson-Eigenschaft impliziert eine Fundierte ordnung. Die Umkehrungen gelten nicht. $((\mathbb{N}, |)$ hat keine endlichen Basis). Jede linear geordnete endliche Menge ist eine Wohlordnung. Komponentenweise Halbordnung auf $\{0,1\} \times \{0,1\}$ ist keine Wohlordnung aber erfüllt die Dickson-Eigenschaft.

- **Was besagt das Dicksonsche Lemma?**

  $(\mathbb{N}_0^n, \leq)$ besitzt die Dickson-Eigenschaft.

- **Warum erfüllt die Menge der multivariaten Terme mit der Teilbarkeit die Dickson-Eigenschaft?**

  Der Ordnungsisomorphismus, der die Potenzentupel auf die Menge $\mathbb{N}_0^n$ abbildet führt die Aussage auf das Dicksonsche Lemma.

- **Wie kann man eine Ordnung auf Polynomen definieren?**

  Eine strikte Quasiordnung auf den Polynomen kann man so definieren, dass

  $$f < g \iff T(f) \Delta T(g) \neq \emptyset \text{ und } \max(T(f) \Delta T(g)) \in T(g)$$

- **Was ist ein Radikalideal?**

  Ein Radikalideal ist ein Ideal in dem gilt

  $$a^n \in I \Longrightarrow a \in I$$

- **Was besagt der Hilbertsche Nullstellensatz?**

  In einem Polynomenring über einem Körper gilt für das endliche multivariate Polynomensystem

  $$V_L(F) \subseteq V_L(g) \iff g \in rad(F)$$

- **Was nimmt man statt GGT bei multivariate Polynomringen?**

  Die Gröbnerbasen.

- **Welche direkten Anwendungen haben Gröbnerbasen?**

  Idealmitgliedschaftsproblem, Kanonischer Simplifizierer modulo I, Rechnen in Restklassenkörpern modulo I.

- **Was kann man mit Hilfe von Gröbnerbasen über die Lösunsmenge eines multivariaten Polynomensystems aussagen?**

  Mit Hilfe des Hilbertschen Nullstellensatzes lässt sich die Aussage über Lösbarkeit eines Systems von Gleichungen und Ungleichungen auf ein Idealmitgliedschaftsproblem zurückführen. Es gilt $V_{\mathbb{C}}(F) \cap U_{\mathbb{C}}(G) = \emptyset$ wenn

  $$1 \in Id(H) \text{ in } \mathbb{Q}[X_1, ..., X_n]$$

  für ein geeignet gewähltes H.

- **Definieren sie eine Gröbnerbasis?**

  In einem mit einer Termordnung versehenen Polynomenring über einem Körper ist eine nichtleere Teilmenge G eine Gröbnerbasis für ein Ideal I wenn

  $$Mult(HT(G)) = HT(I)$$

  oder für jdeses $0 \neq f \in I$ ein $g \in G$ existiert mit

  $$HT(g) \mid HT(f)$$

- **Existiert für jedes Ideal eine Gröbnerbasis?**

  Ja. Sogar für jede Termordnung. Dies liegt daran, dass man eine Endliche Dickson-Basis von $HT(I)$ auswählen kann und somit eine endliche Polynomenmenge mit zugehörigen höchsten Termen hat.

- **Liefert der existenzielle Beweis für Gröbnerbasen einen konstruktiven Algorithmus?**

  Nein, da das Problem auf die Suche der Dickson-Basis zurückgeführt wird.

- **Was ist die Buchberger-Reduktion?**

  Ein Polynom p lässt sich mit einem Polynom g reduzieren, falls es ein $h \in T(g)$ und ein $t \in T(p)$ mit $h \mid t$. Dann gibt ist das Ergebnis f

  $$f = p - ug$$

  wobei u der Quotient des Koefizienten von h mit dem von t ist.

- **Was ist eine Normalform bzg. der Reduktion?**

  Ein Polynom in Normalform lässt sich nicht weiter reduzieren.

- **Wann heisst eine Reduktion Noethersch?**

  Falls keine unendlichen Ketten von Reduktionen möglich sind.

- **Was bedeutet konfluent?**

  Eine Reduktionsrelation heisst konfluent, falls die mehrfache Reduktion eines Polynoms zu zwei weiteren Polynomen impliziert, das diese einen gemeinsamen Nachfolger in der Reduktionskette haben.

- **Was bedeutet lokal konfluent?**

  Eine Reduktionsrelation heisst lokal konfluent, falls die einfache Reduktion eines Polynoms zu zwei weiteren Polynomen impliziert, das diese einen gemeinsamen Nachfolger in der Reduktionskette haben.

- **Was ist die Church-Rosser-Eigenschaft?**

  Eine Reduktionsrelation erfüllt die Church-Rosser-Eigenschaft, falls die gegenseitige mehrfache Reduktion zweier Polynome impliziert, das diese einen gemeinsamen Nachfolger in der Reduktionskette haben.

- **Was bedeutet "die Reduktion hat eine Eindeutige Normalformen?**

  Eine Reduktionsrelation besitzt eindeutige Normalformen, falls die Reduktion eines Polynoms in zwei Normalformen impliziert, dass die Normalformen gleich sind.

- **Was besagt das Newmansches Lemma?**

  Für eine Reduktionsrelation sind die Eigenschaften lokal konfluent, konfluent, hat eindeutige Normalform und hat die Church-Rosser-Eigenscaft äquivalent.

- **Welche Voraussetzungen sind notwendig für eine Reduktionsrelation, damit das Newmansches Lemma erfüllt ist?**

  Die Reduktionsrelation muss noethersch sein.

- **Was besagt das Verschiebungslemma?**

- **Welche Charakterisierungen kann man für eine Gröbnerbasis angeben?**

  Für eine Reduktionsrelation modulo G sind die Eigenschaften

  - lokal konfluent,
  - konfluent,
  - hat eindeutige Normalform,
  - hat die Church-Rosser-Eigenscaft,
  - jedes Polynom aus $Id(G)$ lässt sich zu 0 reduzieren,
  - jedes Polynom aus $Id(G)$ ist reduzibel modulo G,

  - jedes Polynom ist topreduzibel modulo G und
  - Für jedes $s \in HT(Id(G))$ existiert ein $t \in HT(G)$ mit $t \mid s$

  äquivalent zu G ist eine Gröbnerbasis. Analoge Charakterisierungen existieren für ein Ideal.

- **Es gibt ja viele äquivalente Beschreibungen einer GB. Aber die meisten haben so einen nicht-algorithmisch anwendbaren charakter. Gibt es da auch einen endlichen Test?**

  Der Test besteht darin, für alle Paare von Polynomen das S-Polynom zu berechnen und zu prüfen, ob es sich zu 0 reduzieren lässt.

- **Was ist ein S-Polynom?**

$$Spoly(f,g) = KGV(HM(f), HM(g))(\frac{f}{HM(g)} - \frac{g}{HM(p)})$$

- **Wie lassen sich die Gröbnerbasen mit Hilfe von S-Polynomen beschreiben?**

  G ist genau dann eine Gröbnerbasis, wenn für jedes Paar von Polynomen aus G das zugehörige S-Polynom sich zu 0 reduzieren lässt.

- **Welche speziellen Fälle von Gröbnerbasen kennen Sie?**

  Einelementige Mengen und endliche Mengen von Monomen sind bezüglich jeder Termordnung eine Gröbnerbasis.

- **Mit Hilfe von S-Polynomen kann man ja einen Konstruktionsalgorithmus für Gröbnerbasen machen, skizzieren Sie den mal ganz grob?**

  Man geht alle Paare von Polynomen aus der gegebenen Menge durch. Falls das S-Polynom sich nicht zu 0 reduzieren lässt fügt man das reduzierte S-Polynom zur Menge hinzu und testet die Menge erneuert.

- **Ist die Normalform während der Abarbeitung des Buchberger-Algorithmus eindeutig?**

  Nein. Dazu müsste die Menge bereits eine Gröbnerbasis sind. Das ist eine äquivalente Charakterisierung davon.

- **Warum ist der Buchberger Algorithmus korrekt?**

  Jedes S-Polynom lässt sich nach der Termination zu 0 reduzieren. Dass ist eine äquivalente Charakterisierung der Gröbnerbasis. Die Basis ist auch endlich, da nur endlich viele neue Polynome hinzugefügt worden sind.

- **Was verwenden Sie für den Beweis der Termination des Buchberger Algorithmus?**

  Das Dicksonsches Lemma.

- **Warum terminiert der Buchberger Algoritmus?**

  Falls der Algorithmus nicht terminiert so, fügt man unendlich viele neue Polynome hinzu mit höchsten Termen reduziert bezüglich der jeweiligen Menge. Wählt man zu einem festen Zeitpunkt eine Dickson-Basis der höchsten Terme, so lassen sich in der nachfolgenden Menge Terme auffinden, die durch die Elemente der Basis teilbar sind. Das ist ein Widerpruch.

- **Was besagt das Buchberger-Kriterium?**

  Für polynome mit disjunkten höchsten Termen ist das S-Polynom bezüglich der Polynomenmenge reduzibel zu 0.

- **Wie löst man mit Hilfe der Gröbnerbasen das Idealmitgliedschaftsproblem?**

  Man wählt eine Termordnung. Berechnet eine Gröbnerbasis bezügliuch dieser Ordnung und reduziert das gegebene Polynom mittels der Gröbnerbasis auf die eindeutige Normalform. Dann ist die Mitgliedschaft dazu äquivalent, dass die Normalform 0 ist. Für ein $h = 1$ muss die Gröbnerbasis ein konstantes Polynom enthalten.

- **Wie erkennt man, ob eine Varietät endlich oder unendlich ist?**

  Die Endlichkeit der Warietät ist zur Endlichdimensionalität des erzeugten Quotientenvektorraumes äquivalent?

- **Wie findet man eine Basis des Quotientenvektorraumes?**

  Die Basis ist die Menge der Äquivalenzklassen solcher Terme, die nicht durch die höchsten Terme der Gröbnerbasis teilbar sind.

- **Wie erkennt man die Endlichdimensionalität des Quotientenvektorraumes?**

  Für alle $1 \leq i \leq n$ existiert ein Polynom in der Gröbnerbasis mit dem höchsten Koefizienten der Form $X_i^{k_i}$. Dann gilt zusätzlich

$$dim_K(R/I) \leq \prod_i = 1^n k_i$$

3 Satzsammlung

Hier sind noch die Wichtigsten Sätze kurz zusammengefasst.

3.1 Grundlagen

- In einem Hauptidealbereich gilt

$$d = GGT(A) \Longleftrightarrow Id(A) = Id(d)$$

- In einem Hauptideal- bzw. Faktoriellen Bereich besitzt jede nichtleere Teilmenge einen GGT.
- **(Teilerkettensatz)** Es gibt keine strikt aufsteigenden Ketten von Idealen.
- Jedes Primelement ist irreduzibel. Die Umkehrung ist i.A. falsch.
- In einem Hauptideal- bzw. Faktoriellen Bereich gilt, dass ein Element genau dann irreduzibel ist, wenn es prim ist.
- **(Primfaktorzerlegung)** In einem Hauptideal- bzw. Faktoriellenbereich existiert für jedes Element eine bis auf multiplikativen Inversen eindeutige Primfaktorzerlegung.
- In einem Faktoriellen bereich gibt es für je zwei Elemente einen GGT (als Produkt der Primfaktoren).
- Der Quotient von f und $GGT(f, f')$ ist der quadratfreie Anteil von f.
- Die Quadratfreie Zerlegung ist algorithmisch ohne Primfaktorisierung möglich.

3.2 Univariater Fall

- $V_L(F) = V_L(Id(F))$
- $V_L(F) = V_L(GGT(F))$
- $V_L(fg) = V_L(f) \cup V_L(g)$
- Für den quadratfreien Anteil f^* von f gilt

$$V_L(f) = V_L(f^*)$$

- Für eine Primfaktorzerlegung $f = \prod p_i^{k_i}$ gilt

$$V_L(f) = \bigcup_{i=1}^{n} V_L(p_i)$$

- Ein quadratfreies f hat in einem algebraisch abgeschlossenen Körper genau $Grad(f)$ verschiedene Nullstellen.

- Die Nullstellenmenge eines Polynomensystems ist genau dann leer, wenn der $GGT(F) = 1$.
- Für ein quadratfreies f und ein beliebiges g gilt

$$V_K(f) \cap U_K(g) = V_K(f) \setminus V_K(g) = V_K(f/GGT(f,g))$$

- Für die Polynomensysteme F und G gilt

$$V_K(F) \cap U_K(G) = V_K(\frac{f^*}{GGT(f^*, \prod G)})$$

- Für die Polynomensysteme F und G gilt

$$|V_{\mathbb{C}}(F) \cap U_{\mathbb{C}}(G)| = Grad(\frac{f^*}{GGT(f^*, \prod G)})$$

- In einem Polynomenring über einem Körper haben die Polynome f,g genau dann keine Nullstelle in einem Erweiterungskörper, wenn die Resultante von f und g 0 ist.
- Ein Polynom in einem Polynomenring über einem Körper ist genau dann quadratfrei, wenn seine Diskriminante nicht 0 ist.
- **(Satz von Sturm-Sylvester)** Für f,$g \in \mathbb{R}[X]$ mit f quadratfrei und $GGT(f,g) = 1$ gilt füt $a < b$ mit $f(a)f(b) \neq 0$

$$N(f,g,1,(a,b)) - N(f,g,-1,(a,b)) = ZW(S(f,g)(a)) - ZW(S(f,g)(b))$$

- Sämtliche rationalen Nullstellen eines rationalen Polynoms sind Brüche, wobei der Zähler ein Teiler vom konstanten Glied und Nenner ein Teiler vom höchsten Koeffizienten ist.
- Für multivariante Polynome ist die Frage nach der Anzahl bzw. Lage von rationalen bzw. Ganzzahligen Nullstellen algorithmisch unlösbar.
- **(Gaussches Lemma)** Produkt primitiver Polynome ist wieder primitiv.

3.3 Multivariater Fall

- **(Hilbertscher Basissatz)** Für jeden Körper ist der multivariante Polynomenring ein Noetherscher Bereich.
- **(Dicksonnsches Lemma)** $(\mathbb{N}_0^n, \leq)$ mit der komponentenweisen Halbordnung erfüllt die Dicksonn-Eigenschaft.
- Die Menge aller Terme erfüllt die Dickson-Eigenschaft.
- In einer Termordnung gibt es keine unendlichen absteigenden Ketten von Termen.

- Es gibt keine unendlich absteigenden Ketten von Polynomen mit der definierten strickten Quasiordnung.
- **(Hilbertscher Nullstellensatz)**

$$V_L(F) \subseteq V_L(g) \Longleftrightarrow g \in rad(F)$$

- Varietät von F ist leer genau dann, wenn $1 \in Id(F)$.
- G ist eine Gröbnerbasis $rarr I = Id(G)$.
- Zu jeder Termordnung und jedem Ideal gibt es eine Gröbnerbasis.
- Die buchberger Reduktion ist noethersch.
- Lokal konfluent, konfluent, CR-Eigenschaft und eindeutige Normalform sind äquivalent.
- G ist eine Gröbnerbasis genau dann, wenn sich das S-Polynom von je zwei Polynomen in G zu 0 reduzieren lässt.
- Der Quotientenkörper ist genau dann endlich dimensional, wenn für jedes $1 \leq i \leq n$ ein Element der Gröbnerbasis existiert, dass $HT(g) = X_i^{k_i}$.