Computerpraktikum Polyvalenz Ulrich Thiel
SS 2013

Projekt 1.5: Gröbnerbasen

Anforderungen:

(a) Bearbeiten Sie alle in dem Text gestellten Aufgaben.
(b) Reichen Sie die implementierten Intrinsics ausführlich dokumentiert in einer Datei ein.
(c) Schreiben Sie einen Text, in dem Sie die Aufgabenstellung kurz in eigenen Worten zusammenfassen, und Ihre Ideen, Ansätze und Ergebnisse erläutern.
(d) Bereiten Sie einen Vortrag (15-20 Minuten) darüber vor.
(e) Sind Ergebnisse zu den Aufgaben bereits in der Literatur diskutiert (und das sind sie meistens), möchte ich keine Referenz auf diese Literatur als Lösung bekommen, sondern funktionsfähige Algorithmen (bzw. Beweise), die diese Lösungen ergeben.
(f) Sie dürfen alle in Magma bereits implementierten Intrinsics benutzen, es sei denn, es ist ausdrücklich untersagt.

Es dürfen Intrinsics zu Monomordnungen auf Polynomringen verwendet werden. Intrinsics zu Gröbner-Basen dürfen allerdings nicht verwendet werden.

1 Annahme. Es sei K immer ein Körper und $K[\boldsymbol{X}]$ der Polynomring über K in einer Familie $\boldsymbol{X} := (X_i)_{i=1}^n$ von Variablen. Für $\alpha \in \mathbb{N}^n$ sei $\boldsymbol{X}^\alpha := \prod_{i=1}^n X_i^{\alpha_i}$.

In diesem Projekt geht es um das Problem, für ein Ideal $I \trianglelefteq K[\boldsymbol{X}]$ und ein Polynom $f \in K[\boldsymbol{X}]$ zu entscheiden, ob $f \in I$ gilt oder nicht. Die Idee ist hierbei für ein Ideal $I \trianglelefteq K[\boldsymbol{X}]$ eine Methode zu finden, die für jedes $f \in K[\boldsymbol{X}]$ eine *Normalform* $\mathrm{N}_I(f) \in K[\boldsymbol{X}]$ von f modulo I produziert, sodass $f \equiv \mathrm{N}_I(f) \bmod I$ und man an $\mathrm{N}_I(f)$ leicht ablesen kann, ob $f \in I$ gilt oder nicht.

Um diese Idee zu konkretisieren, wählen wir ein endliches Erzeugendensystem $\mathscr{I} := (g_1, \dots, g_s)$ von I. Eine Kongruenz $f \equiv \mathrm{N}_I(f) \bmod I$ gilt genau dann, wenn $f = \sum_{j=1}^s q_j g_j + \mathrm{N}_I(f)$ mit $q_j \in K[\boldsymbol{X}]$ gilt. Solche Darstellungen von f sind allerdings keineswegs eindeutig, sodass wir darüber nicht $\mathrm{N}_I(f)$ charakterisieren können. Wir müssen für eine eindeutige Darstellung weitere Bedingungen an $\mathrm{N}_I(f)$ stellen und dies kann man mittels einer Monomordnung auf $K[\boldsymbol{X}]$ machen.

2 Definition. Eine *Monomordnung* auf $K[\boldsymbol{X}]$ ist eine Wohlordnung $\prec$ auf der Menge der Monome in $K[\boldsymbol{X}]$, sodass außerdem gilt: Ist $f \prec g$ für Monome f und g, dann ist

auch $fh \prec gh$ für alle Monome $h \in K[\boldsymbol{X}]$. Äquivalent ist eine Monomordnung eine Wohlordnung auf $\mathbb{N}^n$, sodass $\alpha \prec \beta$ impliziert, dass $\alpha + \gamma \prec \beta + \gamma$ für alle γ gilt.

3 Beispiel. Eine Monomordnung auf $K[\boldsymbol{X}]$ ist zum Beispiel die *lexikographische Ordnung*

$$\boldsymbol{X}^\alpha \prec_{\text{lex}} \boldsymbol{X}^\beta :\Longleftrightarrow \alpha \prec_{\text{lex}} \beta$$

mit $\alpha \prec_{\text{lex}} \beta$ genau dann, wenn die erste (von links gesehen) nicht-verschwindende Komponente von $\alpha - \beta$ negativ ist. Zum Beispiel gilt

$$(0,4,0) \prec_{\text{lex}} (1,1,2) \prec_{\text{lex}} (1,2,1) \prec_{\text{lex}} (3,0,0)\ .$$

4 Annahme. Von nun an bezeichne $\prec$ immer eine Monomordnung auf $K[\boldsymbol{X}]$.

5 Definition. Für ein Polynom $\sum_{\alpha \in \mathbb{N}^n} c_\alpha \boldsymbol{X}^\alpha \in K[\boldsymbol{X}] \setminus \{0\}$ führen wir folgende Begriffe ein:

(a) Ein *Monom* in f ist ein Monom $\boldsymbol{X}^\alpha$ mit $c_\alpha \neq 0$.
(b) Der *Träger* $\operatorname{Supp}(f)$ von f ist die Menge $\{\boldsymbol{X}^\alpha \mid c_\alpha \neq 0\}$.
(c) Ein *Term* in f ist ein Term $c_\alpha \boldsymbol{X}^\alpha$ mit $c_\alpha \neq 0$.
(d) Der *Multigrad* von f ist $\operatorname{mdeg}_\prec(f) := \max_\prec\{\alpha \in \mathbb{N}^n \mid c_\alpha \neq 0\}$.
(e) Der *Leitterm* von f ist $\operatorname{LT}_\prec(f) := c_{\operatorname{mdeg}_\prec(f)} \boldsymbol{X}^{\operatorname{mdeg}_\prec(f)}$.

Für eine Teilmenge $\mathscr{I} \subseteq K[\boldsymbol{X}] \setminus \{0\}$ setzen wir $\operatorname{LT}_\prec(\mathscr{I}) := \{\operatorname{LT}_\prec(g) \mid g \in I, g \neq 0\}$.

6 Bemerkung. In Magma sind bereits Monomordnungen und zugehörige Intrinsics wie `LeadingTerm` implementiert. Sie dürfen dies verwenden.

Mittels einer festen Monomordnung können wir nun eine eindeutige Darstellung eines Polynoms und daher eine Normalform charakterisieren.

7 Theorem. Für ein Polynom $f = \sum_{\alpha \in \mathbb{N}^n} c_\alpha \boldsymbol{X}^\alpha \in K[\boldsymbol{X}] \setminus \{0\}$ und eine Folge $\mathscr{I} := (g_1, \ldots, g_s) \subseteq K[\boldsymbol{X}] \setminus \{0\}$ existieren eindeutige Elemente $q_1, \ldots, q_s, \operatorname{N}^\prec_{\mathscr{I}}(f) \in K[\boldsymbol{X}]$ mit folgenden Eigenschaften:

(a) $f = \sum_{j=1}^n q_j g_j + \operatorname{N}^\prec_{\mathscr{I}}(f)$, und daher insbesondere $f \equiv \operatorname{N}^\prec_{\mathscr{I}}(f) \bmod I$.
(b) Kein Term in $\operatorname{N}^\prec_{\mathscr{I}}(f)$ ist enthalten in $\langle \operatorname{LT}_\prec(g_1), \ldots, \operatorname{LT}_\prec(g_s)\rangle$.
(c) Für jedes j und jeden Term t in q_j gilt

$$t \cdot \operatorname{LT}_\prec(g_j) \notin \langle \operatorname{LT}_\prec(g_1), \ldots, \operatorname{LT}_\prec(g_{j-1})\rangle\ .$$

Man nennt $\operatorname{N}^\prec_{\mathscr{I}}(f)$ die *Normalform* von f bezüglich $\mathscr{I}$ und $\prec$.

Beweis. Wir zeigen hier nur die Eindeutigkeit, die Existenz wird aus dem Algorithmus unten folgen. Seien also $f = \sum_{j=1}^n q_j g_j + r = \sum_{j=1}^n q'_j g_j + r'$ zwei Darstellungen, die obige Eigenschaften erfüllen. Es gilt dann

$$0 = (q_1 - q'_1)g_1 + \ldots + (q_s - q'_s)g_s + (r - r')\ . \tag{1}$$

Angenommen, es ist nicht schon $r = r'$. Es ist $\operatorname{Supp}(r - r') \subseteq \operatorname{Supp}(r) \cup \operatorname{Supp}(r')$.

Ist also m ein Monom in $r - r'$, so ist m oBdA auch ein Monom in r und daher gilt nach (b) auch, dass $m \notin \langle \mathrm{LT}_\prec(g_1), \ldots, \mathrm{LT}_\prec(g_s)\rangle$. Dann gilt auch für jeden Term t in $r - r'$, dass $t \notin \langle \mathrm{LT}_\prec(g_1), \ldots, \mathrm{LT}_\prec(g_s)\rangle$ und daher schließlich

$$\mathrm{LT}_\prec(r - r') \notin \langle \mathrm{LT}_\prec(g_1), \ldots, \mathrm{LT}_\prec(g_s)\rangle \ .$$

Angenommen, es ist nicht schon $q_j = q'_j$ für ein j. Es ist $\mathrm{Supp}(q_j - q'_j) \subseteq \mathrm{Supp}(q_j) \cup \mathrm{Supp}(q'_j)$. Ist also m ein Monom in $q_j - q'_j$, so ist m oBdA auch ein Monom in q_j und daher gilt nach (c) auch, dass $\mathrm{LT}_\prec(mg_j) \notin \langle \mathrm{LT}_\prec(g_1), \ldots, \mathrm{LT}_\prec(g_{j-1})\rangle$. Dann gilt auch für jeden Term t in $q_j - q'_j$, dass $\mathrm{LT}_\prec(tg_j) \notin \langle \mathrm{LT}_\prec(g_1), \ldots, \mathrm{LT}_\prec(g_{j-1})\rangle$. Es ist $\mathrm{LT}_\prec((q_j - q'_j)g_j) = \mathrm{LT}_\prec(tg_j)$ für einen Term t in $q_j - q'_j$ und daher gilt

$$\mathrm{LT}_\prec((q_j - q'_j)g_j) \notin \langle \mathrm{LT}_\prec(g_1), \ldots, \mathrm{LT}_\prec(g_{j-1})\rangle \ .$$

Ist $r \neq r'$, so folgt sofort, dass $\mathrm{LT}_\prec(r - r') \neq \mathrm{LT}_\prec((q_j - q'_j)g_j)$ für alle j mit $q_j \neq q'_j$ gilt. Seien andererseits $q_j \neq q'_j$ und $q_k \neq q'_k$ mit $j < k$. Wäre $\mathrm{LT}_\prec((q_j - q'_j)g_j) = \mathrm{LT}_\prec((q_k - q'_k)g_k)$, so wäre

$$\mathrm{LT}_\prec((q_j - q'_j)g_j) = \mathrm{LT}_\prec((q_k - q'_k)g_k) \notin \langle \mathrm{LT}_\prec(g_1), \ldots, \mathrm{LT}_\prec(g_{k-1})\rangle \ ,$$

was aber ein Widerspruch wegen $j < k$ ist. Also gilt auch $\mathrm{LT}_\prec((q_j - q'_j)g_j) \neq \mathrm{LT}_\prec((q_k - q'_k)g_k)$.

Insgesamt haben daher alle nicht-verschwindenden Summanden in (1) paarweise verschiedene Leitterme. Das wäre aber unmöglich, und daher müssen alle Summanden bereits verschwinden, d.h. $q_j = q'_j$ für alle j und $r = r'$. ■

Die Elemente $q_1, \ldots, q_s, \mathrm{N}^\prec_{\mathscr{J}}(f)$ können in der Tat über folgenden Algorithmus leicht berechnet werden, womit auch deren Existenz bewiesen ist.

8 Algorithmus.
EINGABE: $f \in K[\boldsymbol{X}]$ und $\mathscr{J} := (g_1, \ldots, g_s) \subseteq K[\boldsymbol{X}] \setminus \{0\}$.
AUSGABE: $(q_1, \ldots, q_s)$ und $\mathrm{N}^\prec_{\mathscr{J}}(f)$ wie in 7.

$r := 0$;
$p := f$;
for $j = 1, \ldots, s$ **do**
  $q_j := 0$;
end for;
while $p \neq 0$ **do**
  if $\mathrm{LT}_\prec(g_j)$ divides $\mathrm{LT}_\prec(p)$ **then**
    choose j minimal with this property;
    $q_j := q_j + \frac{\mathrm{LT}_\prec(p)}{\mathrm{LT}_\prec(g_j)}$;
    $p := p - \frac{\mathrm{LT}_\prec(p)}{\mathrm{LT}_\prec(g_j)} g_j$;
  else
    $r := r + \mathrm{LT}_\prec(p)$;
    $p := p - \mathrm{LT}_\prec(p)$;

end if;
end while;
return $q_1, \ldots, q_s, r$;

9 Aufgabe. Implementieren Sie eine Intrinsic

```
MyNormalForm(f::RngMPolElt, I::SeqEnum) -> RngMPolElt, SeqEnum ,
```

die den Algorithmus in 8 ausführt und sowohl $\mathrm{N}^{\prec}_{\mathscr{J}}(f)$ als auch $(q_1, \ldots, q_s)$ zurückgibt. Dabei soll die bereits definierte Monomordnung auf dem Polynomring verwendet werden.

10. Zwar haben wir jetzt eindeutige Normalformen definiert und können diese auch berechnen, dennoch haben wir immer noch nicht unser eigentliches Problem gelöst. Sicherlich ist $f \in I$ genau dann, wenn $\mathrm{N}^{\prec}_{\mathscr{J}}(f) \in I$, aber das hilft uns noch nicht. Es gilt aber $f \in I$, falls $\mathrm{N}^{\prec}_{\mathscr{J}}(f) = 0$, und das ist bereits gut. Leider gilt die Umkehrung jedoch nicht! Betrachtet man nämlich $f = xy^2 - x \in K[x, y]$, $\mathscr{J} := (xy + 1, y^2 - 1)$ und $I := \langle \mathscr{J} \rangle$ bezüglich $\prec_{\mathrm{lex}}$, so gilt $\mathrm{N}^{\prec}_{\mathscr{J}}(f) = -x - y \neq 0$, es ist aber $f = x(y^2 - 1) \in I$. Die Äquivalenz $f \in I \iff \mathrm{N}^{\prec}_{\mathscr{J}}(f) = 0$ gilt jedoch, wenn $\mathscr{J}$ ein spezielles Erzeugendensystem, nämlich eine *Gröbner-Basis*, besitzt.

11 Theorem. Sei $I \trianglelefteq K[\boldsymbol{X}]$ ein Ideal. Ist $\mathscr{G} := (g_1, \ldots, g_s) \subseteq \mathscr{J} \setminus \{0\}$ mit $\langle \mathrm{LT}_{\prec}(\mathscr{G}) \rangle = \langle \mathrm{LT}_{\prec}(I) \rangle$, so ist gilt für ein $f \in K[\boldsymbol{X}]$ genau dann $f \in I$ genau dann, wenn $\mathrm{N}^{\prec}_{\mathscr{G}}(f) = 0$.

Beweis. Falls $\mathrm{N}^{\prec}_{\mathscr{G}}(f) = 0$, so ist natürlich $f \in I$. Sei andererseits $f \in I$ mit $f \neq 0$. Sei $f = \sum_{j=1}^{s} q_j g_j + \mathrm{N}^{\prec}_{\mathscr{G}}(f)$ wie in 7. Da $\sum_{j=1}^{s} q_j g_j \in I$, ist $\mathrm{N}^{\prec}_{\mathscr{G}}(f) \in I$. Wäre $\mathrm{N}^{\prec}_{\mathscr{G}}(f) \neq 0$, so wäre

$$\mathrm{LT}_{\prec}(\mathrm{N}^{\prec}_{\mathscr{G}}(f)) \in \langle \mathrm{LT}_{\prec}(I) \rangle = \langle \mathrm{LT}_{\prec}(\mathscr{G}) \rangle = \langle \mathrm{LT}_{\prec}(g_1), \ldots, \mathrm{LT}_{\prec}(g_s) \rangle \; .$$

Das wäre aber ein Widerspruch zu 7(b). Also muss $\mathrm{N}^{\prec}_{\mathscr{G}}(f) = 0$ sein. ∎

12 Definition. Eine *Gröbner-Basis* eines Ideals $I \trianglelefteq K[\boldsymbol{X}]$ bezüglich $\prec$ ist eine endliche Teilmenge $\mathscr{G} \subseteq I \setminus \{0\}$, für die $\langle \mathrm{LT}_{\prec}(\mathscr{G}) \rangle = \langle \mathrm{LT}_{\prec}(I) \rangle$ gilt.

13 Fakt. Sei $0 \neq I \trianglelefteq K[\boldsymbol{X}]$. Folgendes gilt:

(a) Eine Gröbner-Basis von I bezüglich $\prec$ existiert.
(b) Ist $\mathscr{G}$ eine Gröbner-Basis von I bezüglich $\prec$, so gilt auch $\langle \mathscr{G} \rangle = I$.
(c) Ist $\mathscr{G}$ eine Gröbner-Basis von I bezüglich $\prec$, so ist für jedes $f \in K[\boldsymbol{X}]$ die Normalform $\mathrm{N}^{\prec}_{\mathscr{G}}(f)$ unabhängig von der Anordnung der Elemente in $\mathscr{G}$. ∎

14. Es existiert ein relativ einfacher Algorithmus zur Berechnung einer Gröbner-Basis eines Ideals – der sogenannte *Buchberger-Algorithmus*. Alles, was wir dafür noch benötigen, ist der Begriff des S-Polynoms.

15 Definition. Seien $f, g \in K[\boldsymbol{X}] \setminus \{0\}$. Das *S-Polynom* von f und g bezüglich $\prec$ ist definiert als

$$\mathrm{S}_{\prec}(f, g) := \frac{\boldsymbol{X}^{\gamma}}{\mathrm{LT}_{\prec}(f)} f - \frac{\boldsymbol{X}^{\gamma}}{\mathrm{LT}_{\prec}(g)} g \in K[\boldsymbol{X}] \; ,$$

wobei $\alpha := \mathrm{mdeg}(f)$, $\beta := \mathrm{mdeg}(g)$ und

$$\gamma := (\max\{\alpha_1, \beta_1\}, \ldots, \max\{\alpha_n, \beta_n\}) .$$

16 Fakt. Eine Teilmenge $\mathscr{G} := \{g_1, \ldots, g_s\} \subseteq K[\boldsymbol{X}] \setminus \{0\}$ ist genau dann eine Gröbner-Basis des Ideals $\langle \mathscr{G} \rangle$ bezüglich $\prec$, wenn

$$\mathrm{N}^{\prec}_{(g_1,\ldots,g_s)}(\mathrm{S}_{\prec}(g_j, g_k)) = 0$$

für alle $1 \leq j < k \leq s$. ■

17 Algorithmus.

EINGABE: $f_1, \ldots, f_s \in K[\boldsymbol{X}] \setminus \{0\}$.

AUSGABE: Gröbner-Basis $\mathscr{G}$ des Ideals $\langle f_1, \ldots, f_s \rangle$ bezüglich $\prec$ mit $f_1, \ldots, f_s \in \mathscr{G}$.

$\mathscr{G} := \{f_1, \ldots, f_s\}$
loop
  $\mathscr{J} := \mathscr{G}$
  for each $p, q \in \mathscr{J}$ **with** $p \neq q$ **do**
    $r :=$ residue of division of $\mathrm{S}_{\prec}(p, q)$ by $\mathscr{G}$, with $\mathscr{G}$ ordered arbitrarily
    if $r \neq 0$ **then**
      $\mathscr{G} := \mathscr{G} \cup \{r\}$
    end if
  end for each
  if $\mathscr{J} = \mathscr{G}$ **then**
    return $\mathscr{G}$
  end if
end loop

18 Aufgabe. Implementieren Sie eine Intrinsic

```
Buchberger(I::SetEnum) -> SetEnum ,
```

die zu einer endlichen Teilmenge $\mathscr{I} \subseteq K[\boldsymbol{X}] \setminus \{0\}$ eine Gröbner-Basis nach 17 berechnet.

19 Aufgabe. Sei $I := \langle x^2 + y - 1, xy - x \rangle \subseteq \mathbb{Q}[x, y]$. Welche der folgenden Polynome liegen in I?

(a) $x^2 + y^2 - y$.
(b) $3xy^2 - 4xy + x + 1$.

20 Aufgabe. Bestimmen Sie alle $(x, y) \in \mathbb{C}^2$ die gleichzeitig folgende Gleichungen erfüllen:

$$-x^2y + xy^2 + 6x - y^2 - y - 6 = 0$$
$$x^2y - x^2 - xy^2 - x + 6y - 6 = 0 .$$