Institut für Mathematik, Freie Universität Berlin
Wintersemester 2020/21

Erste Woche von Computeralgebra

Andrea Petracci
andrea.petracci [at] fu-berlin.de

aktualisiert am 12. März 2021 um 13:00 Uhr

Wenn Sie Fehler in diesem Document finden, geben Sie mir Bescheid bitte!

Inhaltsverzeichnis

Einleitung

Seit Jahrhunderten war die Zahlentheorie eine völlig theoretische und „nutzlose“ Disziplin, die die Neugierde nur der Mathematiker kitzelte und ihre Begier nach Kenntnis und Schönheit befriedigte. Mit der Einführung der Computer und der Kryptographie hat die Zahlentheorie unentbehrliche Mittel und Verwendungen geliefert. Zum Beispiel nutzt

eine der berühmtesten kryptographischen Methoden (das RSA-Kryptosystem) die Tatsache aus, dass es sehr schwierig (Computer-zeitintensiv) ist, die Primfaktorzerlegung einer großen ganzen Zahl zu finden.

Während dieser Woche sieht man einen listigen Algorithmus, der die Faktorisierung eines Polynoms mit Koeffizienten in einem endlichen Körper findet. Er ist der Berlekamp-Algorithmus [Ber67] und man implementiert ihn in Singular [DGPS20].

Notation und Terminologie

$\mathbb{Z}$ ist der Ring der ganzen Zahlen. $\mathbb{N}$ ist die Menge der nicht negativen ganzen Zahlen. $\mathbb{N}^+$ ist die Menge der positiven ganzen Zahlen. Alle in diesem Skript betrachtete Ringe sind kommutativ mit Einheit.

1 Singular und ein bisschen Programmierung

Für diesen Abschnitt können Sie das Handbuch von Singular auf `https://www.singular.uni-kl.de/index.php/singular-manual.html` oder den Appendix C in [GP08] lesen. Eine andere Möglichkeit ist die erste zwei Kapitel im Buch [Koe06], aber es benutzt ein anderes Computeralgebrasystem. Auf jeden Fall glaube ich, dass das hilfreichste Ding ist, Singular zu starten und die Aufgaben zu lösen, die ich unten vorschlage.

1.1 Installation

Gehen Sie auf die Webseite `https://www.singular.uni-kl.de` und installieren Sie Singular auf Ihrem Rechner, indem Sie den Anweisungen im Abschnitt „Download“ gemäß Ihrem Betriebssystem folgen. Auf dieser Webseite gibt es ein Handbuch von Singular, in dem Sie ertragreich nachschlagen können.

Außerdem ist es gut, wenn Sie einen Text-Editor haben, z.B. Emacs mit Linux oder Sublime Text (`https://www.sublimetext.com`) mit jedem Betriebssystem. Mit dem Text-Editor können Sie die Sequenz der Befehle in einem .m-File schreiben und dann können Sie sie in Singular kopieren.

1.2 Grundbefehle

Wenn Sie $2 + 2$ in Singular berechnen wollen, sollen Sie

```
2+2;
```

schreiben und Enter drücken. Das Semikolon zeigt das Ende des Befehls an. Dasselbe passiert mit $1 - 3$, mit $2 \cdot 8$ (schreiben Sie `2*8;`) und mit 3^4 (schreiben Sie `3^4;`). Wenn Sie eine Division machen wollen, sollen Sie die rationalen Zahlen ins Spiel bringen; wir werden das nachher machen.

Der Befehl

```
int a = 2;
```

führt eine Variable mit den folgenden Eigenschaften ein: ihrer Name ist a, ihrer Typ ist `int` (d.h. integer, ganze Zahl) und ihrer Wert ist 2. Dies Befehl ist eine *Deklaration*.[1] Wenn Sie eine Variable eingeführt (deklariert) haben, können Sie in algebraischen Ausdrücken benutzen oder neue Variablen einzuführen.

[1] `https://www.singular.uni-kl.de/Manual/4-2-0/sing_35.htm`

Beispiel 1.1. Betrachte man die folgenden Befehle.

```
int n = 3;
n^2;
```

Der erste Befehl führt n ein, das eine ganze Zahl ist und gleich 3 ist. Der zweite Befehl berechnet das Quadrat von n und zeigt es. Wenn man `int m = n+2;` als dritten Befehl hinzufügt, führt man eine neue Variable m, die eine ganze Zahl ist und gleich $n + 2$ ist. Da der Wert von n gleich 3 ist, ist der Wert von m gleich 5.

Nachdem eine Variable eingeführt wird, kann ihr Wert verändert werden. Man macht das mit einem Gleichheitszeichen =. Dies Befehl ist eine *Zuweisung* (assignment).

Beispiel 1.2. Am Ende von

```
int n = 3;
n = 1;
```

ist der Wert von n gleich 1. Trotzdem war der Wert von n gleich 3, sobald der erste Befehl durchgeführt wird und vordem der zweite Befehl durchgeführt wird.

Beispiel 1.3. Am Ende von

```
int n = 2;
int m = n^2;
n + m;
```

hat man $2 + 2^2 = 6$.

Aufgabe 1.2.1. Was sind die Werten von n und m am Ende der folgenden Befehle?

```
int n = 2;
int m = n^2 + 7;
n = 3;
```

Anfangs benutzen Sie nur Ihr Gehirn und dann testen Sie Ihre Idee mit dem Rechner, indem Sie `n;` und `m;` schreiben.

Aufgabe 1.2.2. Wiederholen Sie die vorherige Aufgabe mit den folgenden Befehle.

```
int n = 2;
int m = n + 1;
n = m + 1;
m = n + 1;
```

Bemerkung 1.4. Man nehme an, dass man eine Variable n hat. In einer Zuweisung von n, kann n im algebraischen Ausdruck erscheinen, mit dem das neue n definiert wird. Zum Beispiel, die Befehle

```
int n = 2;
n = n^2 + 1;
```

bedeuten: nach dem ersten Befehl gilt $n = 2$, dann berechnet man $n^2 + 1 = 2^2 + 1 = 5$ und diese Zahl wird der neue Wert von n, so am Ende gilt $n = 5$.

Das Befehl `n++;` ist eine Abkürzung für `n = n + 1;`.

Aufgabe 1.2.3. Was sind die Werten von n, von m und von s am Ende der folgenden Befehle?

```
int n = 0;
int m = 1;
int s = n + m;
n = m;
m = s;
s = n + m;
n = m;
m = s;
s = n + m;
n = m;
m = s;
s = n + m;
n = m;
m = s;
s = n + m;
```

Aufgabe 1.2.4. Was sind die Werten von n und von m am Ende der folgenden Befehle?

```
int n = 0;
int m = 1;
m = n + m;
n = m - n;
m = n + m;
n = m - n;
m = n + m;
n = m - n;
m = n + m;
n = m - n;
```

1.3 Boolesche Ausdrücken

Man betrachte den Befehl

```
5 > 3;
```

und man bemerke, dass Singular 1 erwidert. Hier bedeutet 1 „wahr“. Die Antwort (d.h. der Wahrheitswert) von

```
2 < 1;
```

ist 0 und bedeutet „falsch“. Der Befehl

```
2 == 1;
```

fragt, ob 2 gleich 1 ist, und die Antwort ist natürlich falsch, d.h. 0. Ein boolescher Ausdruck ist eine Kombination von ähnlichen Ausdrücken durch die Logikoperatoren `not` (nicht), `and` (und), `or` (oder).

Beispiel 1.5. Die Antwort von `((5 >= 3) and (1 == 3)) or (not(2 <= 1));` ist 1.

In den booleschen Ausdrücken können Variablen erscheinen.

Beispiel 1.6. Am Ende von

```
int a = 2;
a == 3;
```

haben wir 0. Nämlich ist der Wert von a gleich 2, aber nicht gleich 3.

Bemerkung 1.7. Man betrachte die Befehle

```
int a = 2;
a = 3;
```

und man bemerke, dass der Wert von a am Ende gleich 3 ist. Im vorherigen Beispiel ist der Wert von a am Ende gleich 2, weil der Befehl `a == 3;` a nicht verändert. Deshalb gibt es einen fundamentalen Unterschied zwischen `=` und `==`.

1.4 Bedingte Anweisungen

Wenn Sie einen Befehl ausführen wollen, nur falls eine manche Bedingung erfüllt ist, sollen Sie *if* gemäß der folgenden Syntax benutzen.[2]

```
if (BEDINGUNG) {
    ANWEISUNG(EN)
}
```

Hier ist die Bedingung einer boolesche Ausdruck.

Beispiel 1.8. Man betrachte

```
int n = 5;
if (n >= 4) {
     n++;
}
```

Am Anfang ist der Wert von n gleich 5. Da $5 \geq 4$ gilt, ist die Bedingung erfüllt, deshalb tritt man zwischen die geschweifte Klammern ein und der Befehl `n++` wird ausgeführt; so am Ende ist der Wert von n gleich 6.

Wenn man

```
int n = 5;
if (n >= 10) {
     n++;
}
```

geschrieben hätte, wäre man zwischen die geschweifte Klammern nicht eingetreten und der Wert von n wäre gleich 5 geblieben.

Mit

```
if (BEDINGUNG) {
   ANWEISUNG1
}
else {
   ANWEISUNG2
}
```

wird die Anweisung 1 ausgeführt, wenn die Bedingung erfüllt ist, und die Anweisung 2 wird ausgeführt, wenn die Bedingung nicht erfüllt ist.

[2] `https://www.singular.uni-kl.de/Manual/4-2-0/sing_390.htm`

1.5 Iteration

Wenn man eine Anweisung recht oft wiederholen will, kann man *while* gemäß der folgenden Syntax benutzen.[3]

```
while (BEDINGUNG) {
   ANWEISUNG
}
```

Der Bedeutung ist: wenn die Bedingung nicht erfüllt ist, passiert nichts. Wenn die Bedingung erfüllt ist, tritt man zwischen die geschweifte Klammern ein und die Anweisung wird ausgeführt, und dann startet man wieder, d.h. man sich fragt, ob die Bedingung erfüllt ist. Dies Wiederholungsprozess findet statt, solange die Bedingung erfüllt ist. Sobald die Bedingung nicht erfüllt ist, endet dies Prozess.

Beispiel 1.9. Man betrachte

```
int n = 0;
while (n < 3) {
   n = n + 2;
}
```

Am Anfang ist der Wert von n gleich 0. Da $0 < 3$ gilt, tritt man zwischen die geschweifte Klammern ein. Dann wird n um 2 erhöht. Jetzt ist der Wert von n gleich 2. Da $2 < 3$ gilt, tritt man zwischen die geschweifte Klammern ein und deshalb wird n um 2 erhöht. Jetzt ist der Wert von n gleich 4. Da $(4 < 3)$ falsch ist, tritt man nicht zwischen die geschweifte Klammern ein und der Prozess endet. Am Ende ist der Wert von n gleich 4.

Beispiel 1.10. Man will das Produkt aller natürlichen Zahlen (ohne Null) kleiner und gleich 4 mit einem iterativen Prozess berechnen. Mit anderen Worten will man die Fakultät (factorial) von 4 berechnen. Die Idee ist in Singular zu implementieren, was man ohne dem Rechner täte. Man betrachte

```
int i = 1;
int s = 1;
while (i <= 4) {
   s = s*i;
   i++;
}
s;
```

Wir haben zwei Variablen i und s, die gleich 1 sind. Da $1 \leq 4$ gilt, ist die Bedingung von while erfüllt, deshalb werden die Anweisungen zwischen den geschweiften Klammern ausgeführt, so $s = 1 \cdot 1$ und i wird um 1 erhöht.

Jetzt $s = 1$ und $i = 2$. Da $2 \leq 4$ gilt, tritt man zwischen die Klammern von while ein, deshalb $s = 1 \cdot 2$ und i wird um 1 erhöht.

Jetzt $s = 2$ und $i = 3$. Da $3 \leq 4$ gilt, tritt man zwischen die Klammern von while ein, deshalb $s = 2 \cdot 3$ und i wird um 1 erhöht.

Jetzt $s = 6$ und $i = 4$. Da $4 \leq 4$ gilt, tritt man zwischen die Klammern von while ein, deshalb $s = 6 \cdot 4$ und i wird um 1 erhöht.

Jetzt $s = 24$ und $i = 5$. Da $5 \leq 4$ nicht gilt, endet der while-Prozess.

[3] https://www.singular.uni-kl.de/Manual/4-2-0/sing_396.htm

Bemerkung 1.11. Es ist grundlegend, dass jeder while-Prozess endet. Deshalb muss die while-Bedingung irgendwann falsch werden. Zum Beispiel ist

```
int n = 0;
while (n >= 0) {
   n++;
}
```

absurd. Sie sollen sorgfältig sein!

Aufgabe 1.5.1. Man schreibe eine Sequenz von Befehlen in Singular, die die Summe der ersten 100 positiven ganzen Zahlen berechnet.

Aufgabe 1.5.2. Sei $(F_n)_{n\in\mathbb{N}}$ die Fibonacci-Folge, d.h. die durch

$$\begin{cases} F_0 = 0 \\ F_1 = 1 \\ F_n = F_{n-1} + F_{n-2} \qquad \text{wenn } n \geq 2. \end{cases}$$

definierte Folge natürlicher Zahlen. Man schreibe eine Sequenz von Befehlen in Singular, die F_9 berechnet.

1.6 Funktionen

Sie sollten wissen, was eine Funktion in Mathematik ist. Auch in Singular gibt es Funktionen; sie folgen der folgenden Syntax.

```
proc NAME(INPUT) {
   ANWEISUNGEN
   return(OUTPUT);
}
```

Nachdem eine Funktion definiert wird, kann man sie mit `NAME(ETWAS)` aufrufen.

Beispiel 1.12. Wir wollen eine Funktion konstruieren, deren Name `Factorial` ist, die eine ganze positive Zahl n als Input nimmt, und die $n!$ (die Fakultät von n) als Output gibt.

Wenn n eine gewählte Zahl wäre, könnte man benutzen, was man in Aufgabe 1.10 gemacht hat. Nämlich, wenn $n = 4$ gilt, wird die Fakultät von n von

```
int n = 4;
int i = 1;
int s = 1;
while (i <= n) {
   s = s*i;
   i++;
}
s;
```

berechnet.

Um die Funktion zu konstruieren, die mit jedem n funktioniert, genügt es, die Deklaration von n zu entfernen, n als Input zu stellen, und s als Output zu stellen:

```
proc Factorial(int n) {
   int i = 1;
   int s = 1;
   while (i <= n) {
      s = s*i;
      i++;
   }
   return(s);
}
```

Wenn man 7! berechnen will, soll man

```
Factorial(7);
```

schreiben, nachdem man die Funktion `Factorial` definiert hat.

Aufgabe 1.6.1. Konstruieren Sie eine Funktion, deren Name `gaussSum` ist, die $n \in \mathbb{N}^+$ als Input nimmt und die summe der ersten n ganzen positiven Zahlen als Output gibt. (Sie können eine while-Prozess in die Funktion einzufügen)

Aufgabe 1.6.2. Sei $(F_n)_{n\in\mathbb{N}}$ die Fibonacci-Folge, die in Aufgabe 1.5.2 definiert wurde. Konstruieren Sie eine Funktion, deren Name `Fibonacci` ist, die $n \in \mathbb{N}$ als Input nimmt und die F_n als Output gibt.

Eine Funktion kann mehrere Inputs haben.

Aufgabe 1.6.3. Man schreibe eine Funktion `summeZwischen`, die zwei ganze Zahlen $m, n \in \mathbb{Z}$ mit $m \leq n$ nimmt und die die Summe aller ganzen Zahlen zwischen m und n (m und n aingerechnet) berechnet.

In einer Funktion kann es mehrere return-Befehle geben; trotzdem, sobald ein return-Befehl ausgeführt wird, endet die Funktion und die nachfolgenden return-Befehle werden ignoriert. Jede Funktion hat für jeden Input einen einzigen Output, wie es in Mathematik passiert.

Beispiel 1.13. In Mathematik schreibt man die Funktion

```
proc f(int n) {
   if (n == 0) {
      return(3);
   }
   return(1);
   return(-1);
}
```

als $f\colon \mathbb{Z} \to \mathbb{Z}$

$$f(n) = \begin{cases} 3 & \text{wenn } n = 0, \\ 1 & \text{wenn } n \neq 0. \end{cases}$$

Die innerhalb einer Funktion deklarierte Variablen existieren nicht außerhalb der Funktion, d.h. man kann nicht

```
proc Katze(int n) {
  int i = 1;
  return(n^2);
}
i^3;
```

schreiben.

1.7 Rekursion

Eine Funktion kann while-Prozesse und bedingte Anweisungen innerhalb von sich selbst haben, sie kann eine andere Funktion aufrufen, aber sie kann sich selbst auch aufrufen. Das ist eine rekursive Definition einer Funktion: man soll den Rekursionsanfang (Anker der Rekursion) und den Rekursionsschritt haben.

Beispiel 1.14. Mann will eine Funktion konstruieren, die die Fakültat eines $n \in \mathbb{N}^+$ (wie in Aufgabe 1.12) berechnet und die Rekursion benutzt. Man betrachte die Funktion

```
proc Fact(int n) {
   if (n == 1) {
      return(1);
   }
   return(n*Fact(n-1));
}
```

und man rufe sie mit `Fact(4)` auf, dann $\text{Fact}(4) = 4 \cdot \text{Fact}(3) = 4 \cdot 3 \cdot \text{Fact}(2) = 4 \cdot 3 \cdot 2 \cdot \text{Fact}(1) = 4 \cdot 3 \cdot 2 \cdot 1 = 24$.

Bemerkung 1.15. In den Beispielen 1.12 un 1.14 hat man zwei Arten gesehen, um die Fakultät einer ganzen positiven Zahlen zu berechnen. Die Iteration benutzt die Formel

$$n! = \prod_{i=1}^{n} i$$

und die Rekursion benutzt

$$\begin{cases} 1! = 1 \\ n! = n \cdot (n-1)! \qquad \text{wenn } n > 1. \end{cases}$$

Aufgabe 1.7.1. Wiederholen Sie Aufgabe 1.6.1, indem Sie die while-Prozess vermeiden und Sie die Rekursion verwenden.

Aufgabe 1.7.2. Wiederholen Sie Aufgabe 1.6.2, indem Sie die while-Prozess vermeiden und Sie die Rekursion verwenden.

Bemerkung 1.16. Die rekursiv definierte Funtionen müssen einen Output mit endlich viele Schritten geben. Deshalb wird die durch

```
proc Hund(int n) {
   if (n == 0) {
      return(0);
   }
   return((Hund(n+1))^2);
}
```

definierte Funktion keinen Output geben, wenn sie mit `Hund(1)` aufgerufen wird. Sie sollen sorgfältig sein!

1.8 Zusatzaufgaben

Aufgabe 1.8.1. Konstruieren Sie eine Funktion `Spur`, die die Spur (trace) einer quadratischen Matrix berechnet. Es sollte nützlich sein, `https://www.singular.uni-kl.de/Manual/4-0-3/sing_128.htm` zu besuchen.

Aufgabe 1.8.2. Konstruieren Sie eine rekursive Funktion `Determinante`, die die Determinante einer quadratischen Matrix durch Laplacesche Entwicklungen berechnet.

Aufgabe 1.8.3. Konstruieren Sie eine Funktion `Rang`, die den Rang einer quadratischen Matrix durch den folgenden Satz berechnet. Der Rang einer Matrix ist r dann, genau wenn es einen von 0 verschiedenen Minor (Unterdeterminante) mit Ordnung r gibt und alle Minoren mit Ordnung $r+1$ null sind.

2 Ganze Zahlen

Die Themata dieses Abschnittes können in jedem Buch über elementare Zahlentheorie gefunden werden. Ich könnte die folgenden Literaturangaben empfehlen: Kapitel 1-5 in [MSP11], Kapitel 1-7 in [Chi09], Kapitel I.2, I.3, II.1 in [Kob94].

2.1 Der Ring $\mathbb{Z}$

Der Buchstabe $\mathbb{Z}$ nennt die Menge der ganzen Zahlen:

$$\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}.$$

$\mathbb{Z}$ ist ein kommutativer Ring, d.h. es gibt zwei Operationen $+$ und $\cdot$, sodass die folgenden Eigenschaften gelten:

- $(\mathbb{Z}, +)$ ist eine abelsche Gruppe,
- $\cdot$ ist assoziativ und kommutativ,
- 1 ist ein neutrales Element für $\cdot$,
- zwischen $+$ und $\cdot$ gilt die Distributivität.

Man bemerke, dass 1 und -1 die einzigen Elemente von $\mathbb{Z}$ sind, die ein multiplikatives Invers haben.

In §1.2 hat man gesehen, dass die Deklaration einer Variable, die ein Element von $\mathbb{Z}$ ist, durch

```
int a = 9;
```

gemacht wird.

Eine Haupteigenschaft von $\mathbb{Z}$ ist, dass man die Division zwischen zwei ganzen Zahlen machen kann (angenommen, dass die zweite Zahl nicht null ist). Sie sollten wissen, wie man das praktisch macht. Die präzise theoretische Formulierung ist:

Satz 2.1 (Division/Teilung)**.** *Seien $a \in \mathbb{Z}$ und $b \in \mathbb{Z}$ zwei ganze Zahlen mit $b \neq 0$. Dann gibt es eindeutig bestimmte $q \in \mathbb{Z}$ und $r \in \mathbb{Z}$ mit $a = qb + r$ und $0 \leq r < |b|$. q wird Quotient genannt und r wird Rest genannt.*

Zum Beispiel: $17 = 3 \cdot 5 + 2$, so der Rest von 17 durch 5 ist 2.

Wenn $a \in \mathbb{Z}$ und $b \in \mathbb{Z}$ mit $a \geq 0$ und $b \neq 0$, wird der Quotient von a durch b durch den Befehl

```
a div b;
```

berechnet und der Rest der Division von a durch b wird durch die folgenden äquivalenten Befehle

```
a mod b;
a % b;
```

berechnet. Wenn $a < 0$ ist die Antwort von `a mod b` gleich $-r$, wobei r der Rest von $-a$ durch b ist. Zum Beispiel sind die boolesche Ausdrücken

```
17 mod 5 == 2;
17 mod -5 == 2;
-17 mod 5 == -2;
-17 mod -5 == -2;
```

wahr in Singular.

Definition 2.2. Seien a und b zwei ganze Zahlen. b *teilt* a (oder a ist durch b *teilbar*, oder b ist ein *Divisor/Teiler* von a), wenn es eine ganze Zahl c gibt, sodass $a = bc$ gilt.

$$b|a \qquad \Leftrightarrow \qquad \exists c \in \mathbb{Z} : a = bc.$$

Bemerkung 2.3. Jede ganze Zahl teilt 0.

Bemerkung 2.4. Wenn $b \neq 0$, hat man $b|a$ genau dann, wenn der Rest von a durch b gleich 0 ist.

Definition 2.5. Eine *Primzahl* ist $p \in \mathbb{Z}$ mit $p \neq 0$, $p \neq \pm 1$, sodass ± 1 und $\pm p$ die einzigen Divisoren von p sind.

Mit anderen Worten, ist $p \in \mathbb{Z}$ eine Primzahl genau dann, wenn die folgenden Eigenschaften erfüllt sind:

- $p \neq 0$,
- $p \neq \pm 1$,
- jedes Mal wenn $p = ab$ mit $a, b \in \mathbb{Z}$, dann gilt $a = \pm 1$ oder $b = \pm 1$.

Man erinnere sich daran, dass 1 und -1 die einzigen ganzen Zahlen mit multiplikatives Invers sind.

Normalerweise betrachten wir nur positive Primzahlen, aber theoretisch sind -2, -3, -5, usw. Primzahlen.

In $\mathbb{Z}$ gilt die Primfaktorzerlegung:

Satz 2.6 (Fundamentalsatz der Arithmetik)**.** *Sei $n \in \mathbb{Z}$ mit $n \neq 0$. Dann gibt es $c \in \{\pm 1\}$, Primzahlen $p_1, \ldots, p_s$ und $\alpha_1, \ldots, \alpha_s \in \mathbb{N}^+$ mit $2 \leq p_1 < \cdots < p_s$ und $n = cp_1^{\alpha_1} \cdots p_s^{\alpha_s}$. Außerdem c, $p_1, \ldots, p_s$ und $\alpha_1, \ldots, \alpha_s$ sind eindeutig bestimmt.*

Man bemerke, dass s gleich 0 sein kann; in diesem Umstand gilt $n = c \in \{\pm 1\}$.

$2^2 \cdot 3$ ist die Primfaktorzerlegung von 12. $1 \cdot 12$ ist eine triviale Zerlegung von 12. $2 \cdot 6$ und $3 \cdot 4$ sind nicht triviale Zerlegungen von 12.

Bemerkung 2.7. Es ist sehr aufwändig, die Primfaktorzerlegung einer ganzen Zahl zu berechnen. Man denke daran, dass viele kryptographische Methoden (z.B. das RSA-Kryptosystem) sich bis heute auf die Tatsache stützen, dass es sehr schwierig (Computerzeitintensiv) ist, die Primfaktoren einer großen ganzen Zahl zu finden.

Satz 2.8 (Euklid)**.** *Es gibt unendlich viele positive Primzahlen.*

Beweis. Wenn es nur endlich viele positive Primzahlen $p_1, \ldots, p_n$ gäbe, dann wäre die Zahl $p_1 \cdots p_n + 1$ durch keine Primzahl teilbar und sie widerspräche den Fundamentalsatz der Arithmetik. □

Aufgabe 2.1.1. Schreiben Sie eine Funktion `istPrim`, die kontrolliert, ob eine positive ganze Zahlen eine Primzahl ist.

Aufgabe 2.1.2. Schreiben Sie eine Funktion `SummeErsterPrimzahlen`, die die Summe der ersten k positiven Primzahlen berechnet, wobei k eine beliebige natürliche Zahl ist. Zum Beispiel soll die Antwort von `SummeErsterPrimzahlen(3)` gleich $2 + 3 + 5 = 10$ sein.

2.2 Größter gemeinsamer Teiler

Definition 2.9. Seien $a \in \mathbb{Z}$ und $b \in \mathbb{Z}$. Der *größte gemeinsame Teiler* (greatest common divisor) von a und b ist das einzige $d \in \mathbb{Z}$, das die folgenden Eigenschaften erfüllt:

- $d \geq 0$,
- d ist ein gemeinsamer Teiler von a und b, d.h. d teilt a und b,
- immer wenn c ist ein gemeinsamer Teiler von a und b, dann ist c ein Teiler von d.

Er existiert, ist eindeutig und wird mit $\gcd(a, b)$ bezeichnet.

Aufgabe 2.2.1. Überlegen Sie und berechnen Sie $\gcd(8, 12)$, $\gcd(-8, 12)$, $\gcd(-8, -12)$, $\gcd(7, 1)$, $\gcd(-7, 1)$, $\gcd(3, 6)$, $\gcd(12, 0)$, $\gcd(0, 0)$.

Wenn man die Primfaktorzerlegung von zwei ganzen Zahlen a und b kennt, ist es sehr einfach, den größten gemeinsamen Teiler von a und b zu berechnen: seien $p_1, \ldots, p_s$ positive paarweise verschiedene Primzahlen, seien $\alpha_1, \ldots, \alpha_s \in \mathbb{N}$ und $\beta_1, \ldots, \beta_s \in \mathbb{N}$; wenn

$$a = cp_1^{\alpha_1} \cdots p_s^{\alpha_s} \qquad \text{und} \qquad b = c' p_1^{\beta_1} \cdots p_s^{\beta_s}$$

mit $c, c' \in \{\pm 1\}$, dann gilt

$$\gcd(a, b) = p_1^{\min\{\alpha_1, \beta_1\}} \cdots p_s^{\min\{\alpha_s, \beta_s\}}.$$

Trotzdem ist es sehr zeitintensiv und aufwändig, die Primfaktorzerlegung großer Zahlen zu berechnen. Jetzt will man einen einfachen Algorithmus erklären, um den größten gemeinsamen Teiler von zwei ganzen Zahlen zu berechnen: er ist der Euklidische Algorithmus.

Hilfssatz 2.10. *Seien $a, b, q, r \in \mathbb{Z}$ mit $a = qb + r$. Dann $\gcd(a, b) = \gcd(b, r)$.*

Beweis. Man beweist die Gleichung

$$\{c \in \mathbb{Z} \mid c|a \text{ und } c|b\} = \{c \in \mathbb{Z} \mid c|b \text{ und } c|r\}.$$

$\supseteq$) wenn $c|b$ und $c|r$, ist $a = qb + r$ durch c teilbar. $\subseteq$) wenn $c|a$ und $c|b$, ist $r = a - qb$ durch c teilbar.

$\gcd(a, b)$ ist der Maximum der Linksmenge. $\gcd(b, r)$ ist der Maximum der Rechtsmenge. □

Beispiel 2.11 (Euklidischer Algorithmus)**.** Man will $\gcd(2002, 420)$ berechnen. Wir teilen 2002 durch 14, wie in Satz 2.1: man hat $2002 = 4 \cdot 420 + 322$. Nach Hilfssatz 2.10 gilt $\gcd(2002, 420) = \gcd(420, 322)$.

Jetzt teilen wir 420 durch 322: $420 = 1 \cdot 322 + 98$. Nach Hilfssatz 2.10 gilt $\gcd(420, 322) = \gcd(322, 98)$.

Jetzt teilen wir 322 durch 98: $322 = 3 \cdot 98 + 28$. Nach Hilfssatz 2.10 gilt $\gcd(322, 98) = \gcd(98, 28)$.

Jetzt teilen wir 98 durch 28: $98 = 3 \cdot 28 + 14$. Nach Hilfssatz 2.10 gilt $\gcd(98, 28) = \gcd(28, 14)$.

Jetzt teilen wir 28 durch 14: $28 = 2 \cdot 14 + 0$. Nach Hilfssatz 2.10 gilt $\gcd(28, 14) = \gcd(14, 0) = 14$.

Deshalb $\gcd(2002, 420) = 14$.

Aufgabe 2.2.2. Man konstruiere eine rekursive Funktion `ggT`, die zwei ganze Zahlen a und b als Input nimmt und $\gcd(a, b)$ als Output ergibt. Man benutze den Euklidischen Algorithmus, der in Beispiel 2.11 erklärt wurde. Warum endet dies Algorithmus?

Satz 2.12 (Lemma von Bézout)**.** *Seien $a \in \mathbb{Z}$ und $b \in \mathbb{Z}$. Dann gibt es $\lambda \in \mathbb{Z}$ und $\mu \in \mathbb{Z}$, sodass $\gcd(a, b) = \lambda a + \mu b$ gilt.*

Beweis. Es ist eine Konsequenz des Euklidischen Algorithmus. Wir folgen dem Beispiel 2.11 rückwärts:

$$\begin{aligned} 14 &= 1 \cdot 98 - 3 \cdot 28 \\ &= 1 \cdot 98 - 3 \cdot (322 - 3 \cdot 98) = (-3) \cdot 322 + 10 \cdot 98 \\ &= (-3) \cdot 322 + 10 \cdot (420 - 322) = 10 \cdot 420 - 13 \cdot 322 \\ &= 10 \cdot 420 - 13 \cdot (2002 - 4 \cdot 420) = -13 \cdot 2002 + 62 \cdot 420, \end{aligned}$$

deshalb $\gcd(2002, 420) = -13 \cdot 2002 + 62 \cdot 420$. □

2.3 Der Ring $\mathbb{Z}/m\mathbb{Z}$

Wir fangen mit einem Beispiel an.

Beispiel 2.13. Eine erste Definition von $\mathbb{Z}/3\mathbb{Z}$ ist, dass $\mathbb{Z}/3\mathbb{Z}$ die Menge $\{0, 1, 2\}$ ist. Auf dieser Menge gibt es zwei Operationen $+$ und $\cdot$, die durch die Tabellen

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\cdot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

definiert werden. Man könnte beweisen, dass $\mathbb{Z}/3\mathbb{Z}$ ein kommutativer Ring mit $+$ und $\cdot$ ist. 0 ist das neutrale Element von $+$ und 1 ist das neutrale Element von $\cdot$.

Man beobachte den folgenden: für jede $a, b \in \mathbb{Z}/3\mathbb{Z}$, ist die Summe $a + b$ in $\mathbb{Z}/3\mathbb{Z}$ gleich der Rest von $a + b$ (die Summe in $\mathbb{Z}$) geteilt durch 3. Zum Beispiel gilt $2 + 2 = 4$ in $\mathbb{Z}$, und der Rest von 4 geteilt durch 3 ist 1, deshalb gilt $2 + 2 = 1$ in $\mathbb{Z}/3\mathbb{Z}$.

Das gleich passiert mit dem Produkt: für jede $a, b \in \mathbb{Z}/3\mathbb{Z}$, ist das Produkt $a \cdot b$ in $\mathbb{Z}/3\mathbb{Z}$ gleich der Rest von $a \cdot b$ (das Produkt in $\mathbb{Z}$) geteilt durch 3. Zum Beispiel gilt $2 \cdot 2 = 4$ in $\mathbb{Z}$, der Rest von 4 geteilt durch 3 ist 1, deshalb gilt $2 \cdot 2 = 1$ in $\mathbb{Z}/3\mathbb{Z}$.

Da $1 + 2 = 2 + 1 = 0$ in $\mathbb{Z}/3\mathbb{Z}$ gilt, ist 2 das additive Inverse von 1, d.h. $2 = -1$ in $\mathbb{Z}/3\mathbb{Z}$. Entsprechend $-2 = 1$ in $\mathbb{Z}/3\mathbb{Z}$.

Man sollte denken, dass $\mathbb{Z}/3\mathbb{Z}$ aus $\mathbb{Z}$ gewonnen wird, indem man zwingt, dass 3 gleich 0 ist. Nämlich gilt $2+2=3+1$ in $\mathbb{Z}$; deshalb, da $3=0$ in $\mathbb{Z}/3\mathbb{Z}$, muss $2+2=0+1=1$ in $\mathbb{Z}/3\mathbb{Z}$ gelten. Gleichartig $2^3=8=2\cdot 3+2$ in $\mathbb{Z}$, deshalb $2^3=2$ in $\mathbb{Z}/3\mathbb{Z}$. Mit anderen Worten, immer wenn Sie ein Vielfaches von 3 finden, können Sie zwingen, dass es gleich 0 ist. In $\mathbb{Z}/3\mathbb{Z}$ hat man die folgenden Gleichungen:

$$\begin{aligned}\cdots &= -9 = -6 = -3 = 0 = 3 = 6 = 9 = 12 = \cdots\\ \cdots &= -10 = -7 = -4 = -1 = 2 = 5 = 8 = 11 = \cdots\\ \cdots &= -11 = -8 = -5 = -2 = 1 = 4 = 7 = 10 = 13 = \cdots .\end{aligned}$$

Man betrachte die Funktion $\mathbb{Z}\to\mathbb{Z}/3\mathbb{Z}$, die durch

$$a \mapsto \text{ der Rest von } a \text{ geteilt durch } 3$$

definiert wird. Diese Funktion ist ein surjektiver Ringhomomorphismus und ihr Kern ist die Menge aller Vielfachen von 3.

Jetzt generalisiert man das Beispiel 2.13. Sei m eine positive ganze Zahl. $\mathbb{Z}/m\mathbb{Z}$ ist die Menge $\{0,1,\ldots,m-1\}$. Es gibt zwei Operationen $+$ und $\cdot$, die durch

$$\begin{aligned}a +_{\mathbb{Z}/m\mathbb{Z}} b &:= \text{ der Rest von } a +_{\mathbb{Z}} b \text{ durch } m,\\ a \cdot_{\mathbb{Z}/m\mathbb{Z}} b &:= \text{ der Rest von } a \cdot_{\mathbb{Z}} b \text{ durch } m.\end{aligned}$$

für alle $a,b\in\mathbb{Z}/m\mathbb{Z}$ definiert werden. 0 ist das neutrale Element von $+$ und 1 ist das neutrale Element von $\cdot$. $\mathbb{Z}/m\mathbb{Z}$ wird aus $\mathbb{Z}$ gewonnen, indem man zwingt, dass m gleich 0 ist. In $\mathbb{Z}/m\mathbb{Z}$ gelten die folgenden Gleichungen:

$$\begin{aligned}\cdots &= -3m = -2m = -m = 0 = m = 2m = 3m = \cdots ,\\ \cdots &= -3m+1 = -2m+1 = -m+1 = 1 = m+1 = 2m+1 = 3m+1 = \cdots ,\\ \cdots &= -3m+2 = -2m+2 = -m+2 = 2 = m+2 = 2m+2 = 3m+2 = \cdots ,\\ &\vdots\\ \cdots &= -3m-1 = -2m-1 = -m-1 = -1 = m-1 = 2m-1 = 3m-1 = \cdots .\end{aligned}$$

Die durch

$$a \mapsto \text{ der Rest von } a \text{ geteilt durch } m$$

definierte Funktion

$$\mathbb{Z}\to\mathbb{Z}/m\mathbb{Z}$$

ist ein surjektiver Ringhomomorphismus und ihr Kern ist die Menge aller Vielfachen von m.

Beispiel 2.14. In $\mathbb{Z}/6\mathbb{Z}$ gelten: $2\neq 0$, $3\neq 0$, aber $2\cdot 3=0$. Deshalb ist $\mathbb{Z}/6\mathbb{Z}$ kein Integritätsring.

Aufgabe 2.3.1. In $\mathbb{Z}/11\mathbb{Z}$ was ist das multiplikative Inverse von 3? Von 2? Von 7? Von 10?

Aufgabe 2.3.2. In $\mathbb{Z}/8\mathbb{Z}$ was ist das multiplikative Inverse von 3? Von 2? Von 6? Von 5?

Aufgabe 2.3.3. Man berechne $3^2, 3^3, 3^4, 3^5, 3^{1000}$ und $5^2, 5^3, 5^4, 5^5, 5^6, 5^7, 5^8, 5^9, 5^{1000}$ in $\mathbb{Z}/18\mathbb{Z}$ ohne dem Rechner!

Sei $m \in \mathbb{N}^+$. Wenn Sie Singular benutzen wollen, um in $\mathbb{Z}/m\mathbb{Z}$ auszurechnen, sollen Sie

```
int m = 8;
ring r = (integer, m), x, dp;
```

schreiben. Diese zwei Befehle konstruieren den Ring $\mathbb{Z}/8\mathbb{Z}$.[4] Wenn nach diesen Befehlen man `5` oder `18` schreibt, betrachtet Singular diese Zahlen als Elemente von $\mathbb{Z}$ und nicht von $\mathbb{Z}/8\mathbb{Z}$. Wenn Sie Singular dazu zwingen wollen, diese Zahlen als Elemente von $\mathbb{Z}/8\mathbb{Z}$ zu betrachten, sollen Sie

```
number(5);
number(18);
```

schreiben.

Beispiel 2.15. Man betrachte die Befehle

```
ring r = (integer, 27), x, dp;
2^18;
2^18 mod 27;
number(2)^18;
number(2^18);
(2^18 mod 27) == number(2)^18;
```

Der erste Befehl konstruiert den Ring $\mathbb{Z}/27\mathbb{Z}$. Der zweite Befehl berechnet 2^{18} in $\mathbb{Z}$ und die Antwort ist 262144. Der dritte Befehl berechnet den Rest der Teilung (in $\mathbb{Z}$) von 262144 durch 27. Die vierte und fünfte Befehle berechnen 2^{18} in $\mathbb{Z}/27\mathbb{Z}$, aber `number(2)^18` ist viel besser, weil er die große Zahl $2^{18} \in \mathbb{Z}$ nicht berechnet.

Aufgabe 2.3.4. Wiederholen Sie Aufgabe 2.3.1 mit Singular.

Aufgabe 2.3.5. Wiederholen Sie Aufgabe 2.3.2 mit Singular.

Aufgabe 2.3.6. Wiederholen Sie Aufgabe 2.3.3 mit Singular.

Definition 2.16. Ein kommutativer Ring, der nicht der Nullring ist, ist ein *Körper*, wenn in ihm jedes von Null verschiedene Element ein Inverses bezüglich der Multiplikation besitzt.

Beispiel 2.17. $\mathbb{Z}$ ist kein Körper, weil 2 kein multiplikatives Inverses hat. Die Menge $\mathbb{Q}$ der rationalen Zahlen ist ein Körper. Die Menge $\mathbb{R}$ der reellen Zahlen ist ein Körper. Die Menge $\mathbb{C}$ der komplexen Zahlen ist ein Körper.

Beispiel 2.18. Man betrachte den im Beispiel 2.13 definierten Ring $\mathbb{Z}/3\mathbb{Z}$. 1 und 2 sind die einzigen von 0 verschiedenen Elemente von $\mathbb{Z}/3\mathbb{Z}$. Da $1^2 = 1$ und $2^2 = 1$ in $\mathbb{Z}/3\mathbb{Z}$, haben 1 und 2 multiplikative Inverse in $\mathbb{Z}/3\mathbb{Z}$. Deshalb ist $\mathbb{Z}/3\mathbb{Z}$ ein Körper.

Beispiel 2.19. In Aufgabe 2.3.2 haben Sie gesehen, dass 2 kein multiplikatives Inverses in $\mathbb{Z}/8\mathbb{Z}$ hat. Deshalb ist $\mathbb{Z}/8\mathbb{Z}$ kein Körper.

Satz 2.20. *Sei $m \in \mathbb{N}^+$. $\mathbb{Z}/m\mathbb{Z}$ ist ein Körper genau dann, wenn m eine Primzahl ist.*

[4] Wahrlich konstruieren diese zwei Befehle den Ring $\mathbb{Z}/8\mathbb{Z}[x]$ von Polynomen in der Variable x mit Koeffizienten in $\mathbb{Z}/8\mathbb{Z}$.

Beweis. $\Rightarrow$: man nehme an, dass m keine Primzahl ist. Wir wollen beweisen, dass $\mathbb{Z}/m\mathbb{Z}$ kein Körper ist. Es möglich, $a \in \mathbb{Z}$ und $b \in \mathbb{Z}$ zu finden, mit $1 < a < m$, $1 < b < m$ und $m = ab$. Jetzt betrachte man a und b als Elemente in $\mathbb{Z}/m\mathbb{Z}$. Die Gleichung $ab = m$ in $\mathbb{Z}$ wird $ab = 0$ in $\mathbb{Z}/m\mathbb{Z}$. Wenn a ein multiplikatives Inverses c in $\mathbb{Z}/m\mathbb{Z}$ hätte, dann gölte $0 = 0 \cdot c = (ab)c = (ac)b = 1 \cdot b = b$, aber das ist nicht möglich, weil $1 < b < m$ und b kein Vielfach von m ist. Deshalb hat a kein multiplikatives Inverses in $\mathbb{Z}/m\mathbb{Z}$. Deshalb ist $\mathbb{Z}/m\mathbb{Z}$ kein Körper.

$\Leftarrow$: man nehme an, dass m eine Primzahl ist. Sei a ein von 0 verschiedenes Element von $\mathbb{Z}/m\mathbb{Z}$. a ist kein Vielfaches von m. Da m prim ist, gilt $\gcd(a, m) = 1$. Lemma von Bézout (Satz 2.12) impliziert, dass es $\lambda, \mu \in \mathbb{Z}$ mit $\lambda a + \mu m = 1$ gibt. Da $\lambda a + \mu m = 1$ in $\mathbb{Z}$ gilt, gilt $\lambda a = 1$ in $\mathbb{Z}/m\mathbb{Z}$. Deshalb ist λ das multiplikative Inverse von a in $\mathbb{Z}/m\mathbb{Z}$. Wir haben beweist, dass jedes $\neq 0$ Element von $\mathbb{Z}/m\mathbb{Z}$ ein multiplikative Inverse hat. □

Der Ring $\mathbb{Z}/m\mathbb{Z}$ verdient ein spezielles Symbol, wenn m prim ist:

Definition 2.21. Sei p eine Primzahl. Der Körper $\mathbb{Z}/p\mathbb{Z}$ ist mit $\mathbb{F}_p$ bezeichnet.

Man könnte beweisen, dass $\mathbb{F}_p$ der einzige Körper mit p Elemente ist.

In Singular gibt es eine kleine Abkürzung, um $\mathbb{F}_p$ zu definieren. Zum Beispiel konstruieren die Befehle

```
int p = 5;
ring r = p, x, dp;
```

den Ring $\mathbb{F}_5$.[5]

Aufgabe 2.3.7. Wählen Sie Ihre Lieblingsprimzahl p. Mit Hilfe von Singular berechnen Sie $a^p - a$ in $\mathbb{F}_p$ für jedes $a \in \mathbb{F}_p$.

Aufgabe 2.3.8. Kontrollieren Sie, dass 2017 eine Primzahl ist, und berechnen Sie die folgenden Elemente in $\mathbb{F}_{2017}$: a^{252}, a^{288}, a^{504}, a^{672}, a^{1008}, a^{2016} for $a = 2, 5, 50$.

Aufgabe 2.3.9. Kontrollieren, dass 997 prim ist, und finden Sie explizit ein Erzeugendes der multiplikativen Gruppe $\mathbb{F}_{997}^* = \mathbb{F}_{997} \setminus \{0\}$. Außerdem berechnen Sie die Zahl der Erzeugender von $\mathbb{F}_{997}^*$.

3 Polynome mit Koeffizienten in einem Körper

Die Themata dieses Abschnittes können in jedem Buch über elementare Algebra gefunden werden. Ich könnte Kapitel 13-16, 23 in [Chi09] empfehlen.

3.1 Der Ring $\mathbb{K}[x]$

Sei $\mathbb{K}$ ein Körper, z.B. $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ oder $\mathbb{F}_p$. Wir betrachten eine Variable (oder Unbestimmte) x und Polynome in x mit Koeffizienten in $\mathbb{K}$:

$$a_d x^d + a_{d-1} x^{d-1} + \cdots + a_1 x + a_0 = \sum_{i=0}^{d} a_i x^i \tag{1}$$

mit $a_d, \ldots, a_0 \in \mathbb{K}$ und $d \in \mathbb{N}$. Alle Exponenten sind natürliche Zahlen.

$\mathbb{K}[x]$ bezeichnet die Menge aller Polynome in der Variable x und mit Koeffizienten im Körper $\mathbb{K}$. $\mathbb{K}[x]$ ist ein Ring: Summen und Produkte von Polynomen sind einfach zu

[5] Wahrlich konstruieren sie $\mathbb{F}_5[x]$.

definieren. $\mathbb{K}[x]$ ist ein $\mathbb{K}$-Vektorraum mit unendliche Dimension: eine Basis ist $\{x^n \mid n \in \mathbb{N}\}$.

Ein Polynom ist *konstant* genannt, wenn es ein Element von $\mathbb{K}$ ist.

Der *Grad* eines Polynoms als in (1) ist d wenn $a_d \neq 0$; a_d heißt *Leitkoeffizient* und $a_d x^d$ heißt *Leitterm*. Der Grad des Nullpolynoms wird als $-\infty$ definiert. Das Symbol von Grade ist deg. Die folgenden Eigenschaften gelten: seien $f, g \in \mathbb{K}[x]$, dann

- $\deg(f+g) \leq \max\{\deg f, \deg g\}$
- $\deg f \neq \deg g \;\Rightarrow\; \deg(f+g) = \max\{\deg f, \deg g\}$
- $\deg(fg) = \deg f + \deg g$
- $\deg(f) = -\infty \;\Leftrightarrow\; f = 0$
- $\deg(f) = 0 \;\Leftrightarrow\; f \in \mathbb{K}^* = \mathbb{K} \setminus \{0\} \;\Leftrightarrow\; f$ besitzt ein multiplikatives Inverses in $\mathbb{K}[x]$
- $\deg(f) \geq 1 \;\Leftrightarrow\; f \in \mathbb{K}[x] \setminus \mathbb{K}$, d.h. f ist nicht konstant.

Ein Polynom heißt *monisch*, wenn es nicht null ist und sein Leitkoeffizient gleich 1 ist. Jedes von Null verschiede Polynom in $\mathbb{K}[x]$ ist gleich das Produkt $a \cdot f$, wobei $a \in \mathbb{K}^*$ eine nicht nulle Konstante ist und f ein monisches Polynom ist. Selbstredend ist a der Leitkoeffizient von $a \cdot f$, wenn f monisch ist.

Beispiel 3.1. Mit Singular wird der Ring $\mathbb{Q}[x]$ durch

```
ring r = 0, x, dp;
```

konstruiert. Das Polynom $f = 3x^7 + 9 \in \mathbb{Q}[x]$ wird durch die Deklaration

```
poly f = 3*x^7 + 9;
```

konstruiert. Man kann

```
poly f = number(3)*x^7 + number(9);
```

auch schreiben. Sein Leitterm ist die Antwort von

```
lead(f);
```

und

```
deg(f);
```

ergibt seinen Grad. Man kann Polynome addieren und multiplizieren. Durch `==` kann man fragen, ob zwei Polynome gleich sind. Wenn man $\mathbb{F}_p[x]$ hätte betrachten wollen, hätte man anfangs

```
ring r = p, x, dp;
```

schreiben sollen.

Der Koeffizient von x^i in einem Polynom f ist

```
coeffs(f,x)[i+1,1];
```

Aufgabe 3.1.1. Wählen Sie Ihre Lieblingsprimzahl p. Mit Singular berechnen Sie die Produkte $\prod_{0 \leq i < p}(x-i)$ and $\prod_{0 < i < p}(x-i)$ in $\mathbb{F}_p[x]$.

Der Ring $\mathbb{K}[x]$ hat Eigenschaften, die sehr ähnlich wie die von $\mathbb{Z}$ sind. Man kann die Teilung von zwei Polynomen machen, wie im Satz 2.1:

Satz 3.2 (Division/Teilung)**.** *Sei $\mathbb{K}$ ein Körper und seien $f, g \in \mathbb{K}[x]$ mit $g \neq 0$. Dann gibt es eindeutig bestimmte $q, r \in \mathbb{K}[x]$ mit $f = qg + r$ und $\deg(r) < \deg(g)$. q wird Quotient genannt und r wird Rest genannt.*

Beispiel 3.3. In $\mathbb{Q}[x]$ teilt man $f = x^5 - 2x^3 + 3x + 7$ durch $g = x^2 - 1$. Anfangs schreibt man alle Koeffizienten von f bis dem Grade von f, d.h. 5. So

$$x^5 \quad +0x^4 \quad -2x^3 \quad +0x^2 \quad +3x \quad +7 \qquad x^2 - 1$$

Man teilt den Leitterm von f durch den Leitterm von g: $x^5/x^2 = x^3$ und dann addiert man $-x^3 g = -x^5 + x^3$

$$\begin{array}{cccccc|c} x^5 & +0x^4 & -2x^3 & +0x^2 & +3x & +7 & x^2 - 1 \\ \cline{7-7} -x^5 & & +x^3 & & & & x^3 \\ \cline{1-5} & & -x^3 & & +3x & +7 & \end{array}$$

Man teilt den Leitterm von $-x^3 + 3x + 7$ durch den Leitterm von g: $-x^3/x^2 = -x$ und dann addiert man $-(-xg) = x^3 - x$:

$$\begin{array}{cccccc|c} x^5 & +0x^4 & -2x^3 & +0x^2 & +3x & +7 & x^2 - 1 \\ \cline{7-7} -x^5 & & +x^3 & & & & x^3 - x \\ \cline{1-5} & & -x^3 & & +3x & +7 & \\ & & x^3 & & -x & & \\ \cline{3-5} & & & & 2x & +7 & \end{array}$$

Deshalb $x^5 - 2x^3 + 7 = (x^2 - 1)(x^3 - x) + 2x + 7$. Der Rest ist $2x + 7$ und der Quotient ist $x^3 - x$.

Aufgabe 3.1.2. Indem man Beispiel 3.3 imitiert, mache man die Division von $x^6 + 5x^3 + 3x + 2$ durch $x^2 + 3x + 2$ in $\mathbb{F}_7[x]$ ohne Rechner.

Aufgabe 3.1.3. Indem man Beispiel 3.3 imitiert, konstruiere man eine Funktion, deren Name `polyDivision` ist und die den Rest und den Quotient einer Teilung von zwei Polynomen berechnet.

Natürlich gibt es in $\mathbb{K}[x]$ den Begriff von Teiler/Divisor oder Vielfach/Teilbar. Definition 2.2, Bemerkung 2.3 und Bemerkung 2.4 gelten für $\mathbb{K}[x]$ auch.

Das Analog einer Primzahl (Definition 2.5) ist ein irreduzibles Polynom:

Definition 3.4. Ein Polynom $f \in \mathbb{K}[x]$ heißt *irreduzibel*, wenn die folgenden Eigenschaften erfüllt sind:

- f ist nicht konstant,
- jedes Mal wenn $f = gh$ mit $g, h \in \mathbb{K}[x]$, dann gilt $\deg g = 0$ oder $\deg h = 0$.

Beispiel 3.5. Jedes Polynom mit Grade 1 ist irreduzibel.

Beispiel 3.6. Für jeden Körper $\mathbb{K}$, ist das Polynom $x^2 - 1 \in \mathbb{K}[x]$ reduzibel, weil $x^2 - 1 = (x - 1)(x + 1)$ gilt.

Beispiel 3.7. Das Polynom $x^2 - 2$ ist irreduzibel in $\mathbb{Q}[x]$, aber es ist reduzibel in $\mathbb{R}[x]$, weil $x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$ gilt.

Beispiel 3.8. Das Polynom $x^2 + 1$ ist irreduzibel in $\mathbb{R}[x]$, aber es ist reduzibel in $\mathbb{C}[x]$, weil $x^2 + 1 = (x - \mathrm{i})(x + \mathrm{i})$ gilt.

In §3.2 und in §3.3 sieht man einige Regeln, um die Irreduzibilität eines Polynoms zu untersuchen.

Auch in $\mathbb{K}[x]$ gilt die Primfaktorzerlegung wie im Satz 2.6:

Satz 3.9 (Primfaktorzerlegung in $\mathbb{K}[x]$)**.** *Sei $\mathbb{K}$ ein Körper und sei $f \in \mathbb{K}[x]$ mit $f \neq 0$. Dann gibt es $c \in \mathbb{K}^*$, monische paarweise verschiedene irreduzible Polynome $f_1, \ldots, f_s \in \mathbb{K}[x]$ und $\alpha_1, \ldots, \alpha_s \in \mathbb{N}^+$ mit $f = c f_1^{\alpha_1} \cdots f_s^{\alpha_s}$. Außerdem c, $f_1, \ldots, f_s$ und $\alpha_1, \ldots, \alpha_s$ sind eindeutig bestimmt.*

In §4.2 sieht man einen Algorithmus, um die Primfaktorzerlegung in $\mathbb{F}_p[x]$ zu finden.

Beispiel 3.10. Die Primfaktorzerlegung von $f = x^3 + x^2 \in \mathbb{Q}[x]$ ist $x^3 + x^2 = x^2(x + 1)$. Die Primfaktoren von f sind x und $x + 1$. x hat Vielfachheit 2. $x + 1$ hat Vielfachheit 1.

In $\mathbb{K}[x]$ gibt den größten gemeinsamen Teiler auch:

Definition 3.11. Sei $\mathbb{K}$ ein Körper. Der *größte gemeinsame Teiler* (greatest common divisor) von $a, b \in \mathbb{K}[x]$ ist das einzige $f \in \mathbb{K}[x]$, das die folgenden Eigenschaften erfüllt:

- f ist monisch oder $f = 0$,
- f ist ein gemeinsamer Teiler von a und b, d.h. f teilt a und b,
- immer wenn g ist ein gemeinsamer Teiler von a und b, dann ist g ein Teiler von f.

Er existiert, ist eindeutig bestimmt und wird mit $\gcd(a, b)$ bezeichnet.

Wenn man die Primfaktorzerlegung von zwei Polynome a und b kennt, ist es sehr einfach, den größten gemeinsamen Teiler von a und b zu berechnen. Trotzdem gibt es den Euklidischen Algorithmus, der viel schneller ist und nicht erfordert, die Primfaktorzerlegung zu kennen.

Aufgabe 3.1.4. Indem man Aufgabe 2.2.2 imitiert, konstruiere man eine Funktion `PolyggT`, die zwei Polynome a und b als Input nimmt und $\gcd(a, b)$ als Output ergibt. Warum endet dies Algorithmus?

Aufgabe 3.1.5. Mithilfe von Singular berechnen Sie den größten gemeinsamen Teiler von den folgenden Polynomen in $\mathbb{F}_5[x]$: $x^8 + x^7 + 2x^6 - 2x^2 - 2x + 1$ und $x^6 + x^4 + 2x + 1$.

Satz 3.12 (Lemma von Bézout)**.** *Sei $\mathbb{K}$ ein Körper und seien $f, g \in \mathbb{K}[x]$. Dann gibt es $\lambda \in \mathbb{K}[x]$ und $\mu \in \mathbb{K}[x]$, sodass $\gcd(f, g) = \lambda f + \mu g$ gilt.*

Bemerkung 3.13. Zusammenfassend gibt es viele Ähnlichkeiten zwischen $\mathbb{Z}$ und $\mathbb{K}[x]$, wobei $\mathbb{K}$ ein Körper ist.

	$\mathbb{Z}$	$\mathbb{K}[x]$
Teilung	Satz 2.1	Satz 3.2
	Primzahlen	Irreduzible Polynome
Primfaktorzerlegung	Satz 2.6	Satz 3.9
größerer gemeinsamer Teiler	Definition 2.9	Definition 3.11
Euklidischer Algorithmus	Beispiel 2.11	Aufgabe 3.1.4
Lemma von Bézout	Satz 2.12	Satz 3.12

Die fundamentale Eigenschaft ist die Teilung und alle andere Eigenschaften sind ihre Konsequenzen. Die Ringe, wo die Eigenschaft der Teilung erfüllt ist, heißen euklidische.

3.2 Nullstellen

Hier kümmert man sich darum, einige Regeln zu geben, um zu untersuchen, ob ein Polynom irreduzibel ist. Die erste Bemerkung ist, dass ein Polynom mit Grade 1 klar irreduzibel ist.

Sei $\mathbb{K}$ ein Körper. Man betrachte ein Polynom

$$f = a_d x^d + \cdots + a_1 x + a_0 \in \mathbb{K}[x].$$

Für jedes $\alpha \in \mathbb{K}$ kann man das Element

$$f(\alpha) = a_d \alpha^d + \cdots + a_1 \alpha + a_0 \in \mathbb{K}$$

betrachten. $f(\alpha)$ wird durch die Einsetzung von x in α gewonnen. $f(\alpha)$ heißt den Wert des Polynoms f an der Stelle α.

Aufgabe 3.2.1. Schreiben Sie eine Funktion `Auswertung`, die den Wert von $f \in \mathbb{K}[x]$ in einem Element $a \in \mathbb{K}$ berechnet.

Definition 3.14. Eine *Nullstelle* eines Polynoms $f \in \mathbb{K}[x]$ ist ein Element $\alpha \in \mathbb{K}$ mit $f(\alpha) = 0$.

Beispiel 3.15. Die Nullstellen von $x^2 - 1$ in $\mathbb{Q}$ sind 1 und -1. $x^2 + x + 8$ hat keine Nullstelle in $\mathbb{R}$.

Beispiel 3.16. Das Polynom $x^2 - 2 \in \mathbb{Q}[x]$ hat keine Nullstelle in $\mathbb{Q}$, aber es hat zwei Nullstellen in $\mathbb{R}$: $\sqrt{2}$ und $-\sqrt{2}$.

Beispiel 3.17. Man betrachte das Polynom $f = x^2 + x + 3$ in $\mathbb{F}_5[x]$. Die folgenden Gleichungen gelten in $\mathbb{F}_5$:

$$\begin{aligned} f(0) &= 0^2 + 0 + 3 = 3 \\ f(1) &= 1^2 + 1 + 3 = 5 = 0 \\ f(2) &= 2^2 + 2 + 3 = 9 = 4 \\ f(3) &= 3^2 + 3 + 3 = 15 = 0 \\ f(4) &= 4^2 + 4 + 3 = 3. \end{aligned}$$

Deshalb f hat zwei Nullstellen in $\mathbb{F}_5$: 1 und 3.

Aufgabe 3.2.2. Finden Sie die Nullstellen von $x^2 + 8x - 2$ in $\mathbb{Q}$, in $\mathbb{R}$, in $\mathbb{F}_2$, in $\mathbb{F}_3$, in $\mathbb{F}_5$, in $\mathbb{F}_7$.

Aufgabe 3.2.3. Konstruieren Sie eine Funktion `hatNullstelle`, die testet, ob ein Polynom in $\mathbb{F}_p[x]$ eine Nullstelle in $\mathbb{F}_p$ hat.

Wenn ein nicht konstantes Polynom eine Nullstelle hat, dann ist es reduzibel:

Satz 3.18. *Sei $\mathbb{K}$ ein Körper, sei $f \in \mathbb{K}[x]$ nicht konstant und sei $\alpha \in \mathbb{K}$. α ist eine Nullstelle von f (d.h. $f(\alpha) = 0$) genau dann, wenn $x - \alpha$ ein Teiler von f ist.*

Bei dieser Gelegenheit, wenn der Grad von f größer als 1 ist, dann ist f reduzibel in $\mathbb{K}[x]$.

Beweis. Man teilt f durch $x - \alpha$ und hat $f = (x - \alpha) \cdot q + r$ mit $q, r \in \mathbb{K}[x]$ und $\deg r < \deg x - \alpha = 1$. So $\deg r = -\infty$ (d.h. $r = 0$) oder $\deg r = 0$ (d.h. $r \in \mathbb{K}^*$). Deshalb $r \in \mathbb{K}$ ist konstant. Außerdem $f(\alpha) = (\alpha - \alpha) \cdot q(\alpha) + r = r$. Deshalb

$$f(\alpha) = 0 \quad \Leftrightarrow \quad r = 0 \quad \Leftrightarrow \quad x - \alpha \mid f. \qquad \square$$

Beispiel 3.19. Man betrachte das Polynom $x^2 + x + 9 \in \mathbb{F}_{11}[x]$. Eine Nullstelle ist 1, denn $1^2 + 1 + 9 = 11 = 0$ in $\mathbb{F}_{11}$. Das Polynom $x^2 + x + 9$ ist durch $x - 1$ teilbar, denn $x^2 + x + 9 = (x - 1)(x + 2)$.

Beispiel 3.20. Das Polynom $x^4 + 2x^2 + 1 \in \mathbb{R}[x]$ hat keine Nullstelle in $\mathbb{R}$, aber es ist reduzibel in $\mathbb{R}[x]$ (und in $\mathbb{Q}[x]$ auch): $x^4 + 2x^2 + 1 = (x^2 + 1)^2$.

Ein Polynom mit Grade 2 oder 3 ist reduzibel genau dann, wenn es eine Nullstelle hat:

Satz 3.21. *Sei $\mathbb{K}$ ein Körper und sei $f \in \mathbb{K}[x]$ ein Polynom mit Grade 2 oder 3. f ist irreduzibel in $\mathbb{K}[x]$ genau dann, wenn es keine Nullstelle in $\mathbb{K}$ hat.*

Beweis. $\Rightarrow$) wenn es eine Nullstelle in $\mathbb{K}$ hätte, dann wäre es reduzibel in $\mathbb{K}[x]$ nach Satz 3.18.

$\Leftarrow$) man nehme an, dass f keine Nullstelle in $\mathbb{K}$ hat. Nach Kontraposition nehme man an, dass f reduzibel ist; so $f = gh$ mit $1 \leq \deg g < \deg f$ und $1 \leq \deg h < \deg f$. Da $\deg g + \deg h = \deg f \leq 3$ gilt, hat zumindest eines zwischen g und h hat Grad 1. Das bedeutet, dass f einen Divisor mit Grade 1 hat. Dies Divisor ist $ax + b$ mit $a \in \mathbb{K}^*$ und $b \in \mathbb{K}$. Deshalb $-\frac{b}{a} \in \mathbb{K}$ ist eine Nullstelle von f. □

Aufgabe 3.2.4. Ist $x^2 + x + 8$ irreduzibel in $\mathbb{Q}[x]$? In $\mathbb{R}[x]$? In $\mathbb{F}_2[x]$? In $\mathbb{F}_3[x]$? In $\mathbb{F}_5[x]$?

Aufgabe 3.2.5. Ist $x^3 + 2x^2 + x - 1$ irreduzibel in $\mathbb{Q}[x]$? In $\mathbb{R}[x]$? In $\mathbb{F}_2[x]$? In $\mathbb{F}_3[x]$? In $\mathbb{F}_5[x]$?

Aufgabe 3.2.6. Ist x^2+1 irreduzibel in $\mathbb{Q}[x]$? In $\mathbb{R}[x]$? In $\mathbb{F}_2[x]$? In $\mathbb{F}_3[x]$? In $\mathbb{F}_5[x]$? In $\mathbb{F}_p[x]$, wobei p eine beliebige Primzahl ist? (Für die letzte Frage können Sie Singular benutzen, um alle Primzahlen $p \leq 100$ zu testen; auf diese Art sollten Sie eine Vermutung anstellen.)

Aufgabe 3.2.7. Ist $x^2 + x + 1$ irreduzibel in $\mathbb{Q}[x]$? In $\mathbb{R}[x]$? Für welche Primzahlen ist $x^2 + x + 1$ irreduzibel in $\mathbb{F}_p[x]$? (Man sehe den Ratschlag in Aufgabe 3.2.6)

Aufgabe 3.2.8. Ist $x^4 + 1$ irreduzibel in $\mathbb{Q}[x]$? In $\mathbb{R}[x]$? In $\mathbb{F}_2[x]$? In $\mathbb{F}_3[x]$? In $\mathbb{F}_5[x]$? In $\mathbb{F}_7[x]$?

Aufgabe 3.2.9. Ist $x^4 + 4$ irreduzibel in $\mathbb{Q}[x]$?

Aufgabe 3.2.10. Hier arbeitet man in $\mathbb{F}_2[x]$, aber wenn Sie Singular benutzen, wäre es gut, wenn Sie etwas schreiben, das in $\mathbb{F}_p[x]$ für eine beliebige Primazahl p funktioniert.

a) Finden Sie alle monische irreduzible Polynome mit Grade 2 in $\mathbb{F}_2[x]$.

b) Berechnen Sie das Produkt aller monischen irreduziblen Polynome in $\mathbb{F}_2[x]$ mit Grade 1 oder 2.

c) Finden Sie alle monische irreduzible Polynome mit Grade 3 in $\mathbb{F}_2[x]$.

d) Berechnen Sie das Produkt aller monischen irreduziblen Polynome in $\mathbb{F}_2[x]$ mit Grade 1 oder 3.

Aufgabe 3.2.11. Ist x^4+x+1 irreduzibel in $\mathbb{F}_2[x]$? Ist $x^4-8x^3-100000000x^2-17x+1977$ irreduzibel in $\mathbb{Q}[x]$?

3.3 Quadratfreie Polynome

Definition 3.22. Sei $\mathbb{K}$ ein Körper. Ein Polynom $f \in \mathbb{K}[x]$ heißt *quadratfrei*, wenn die Vielfachheit jedes Primfaktors von f gleich 1 ist. Mit anderen Worten, ist f quadratfrei, wenn die folgende Implikation gilt:

$$g \in \mathbb{K}[x] \text{ irreduzibel und } g \text{ teilt } f \quad \Rightarrow \quad g^2 \text{ teilt nicht } f.$$

Beispiel 3.23. Jedes irreduzible Polynom ist quadratfrei.

Beispiel 3.24. $x^2 - 1 \in \mathbb{Q}[x]$ ist quadratfrei, denn $x^2 - 1 = (x-1)(x+1)$ und $x-1$ und $x+1$ sind verschieden und irreduzibel.

Beispiel 3.25. $x^3 + x^2 = x^2(x+1) \in \mathbb{K}[x]$ ist nicht quadratfrei für jeden Körper $\mathbb{K}$.

Beispiel 3.26. $x^2 - 1 \in \mathbb{F}_2[x]$ ist nicht quadrat frei, denn $x^2 - 1 = (x+1)^2$ gilt in $\mathbb{F}_2[x]$.

Definition 3.27. Sei $\mathbb{K}$ ein Körper und sei

$$f = a_d x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + a_0 = \sum_{i=0}^{d} a_i x^i \in \mathbb{K}[x]$$

ein Polynom. Die *Ableitung* von f ist das Polynom

$$f' = d a_d x^{d-1} + (d-1)a_{d-1}x^{d-2} + \cdots + a_1 = \sum_{i=1}^{d} i a_i x^{i-1} \in \mathbb{K}[x].$$

Beispiel 3.28. Die Ableitung von $x^5 + 7x^2 + 6x - 2 \in \mathbb{Q}[x]$ ist $5x^4 + 14x + 6 \in \mathbb{Q}[x]$.

Beispiel 3.29. Die Ableitung von $x^5 + 2x^4 + x^3 + 2x + 1 \in \mathbb{F}_3[x]$ ist $5x^4 + 8x^3 + 3x^2 + 2 = 2x^4 + 2x^3 + 2 \in \mathbb{F}_3[x]$.

Beispiel 3.30. Die Ableitung eines konstanten Polynoms ist null.

Beispiel 3.31. Die Ableitung von $x^{14}+5x^7+3 \in \mathbb{F}_7[x]$ ist 0. Nach dem kleinen fermatschen Satz gelten $5^7 = 5$ und $3^7 = 3$ in $\mathbb{F}_7$. Deshalb gilt $x^{14} + 5x^7 + 3 = x^{14} + 5^7x^7 + 3^7 = (x^2 + 5x + 3)^7$ in $\mathbb{F}_7[x]$.

Aufgabe 3.3.1. Schreiben Sie eine Funktion `Ableitung`, die die Ableitung eines Polynom berechnet.

Eigenschaften der Ableitung: seien $f, g \in \mathbb{K}[x]$

- $(f+g)' = f' + g'$;
- $(fg)' = f'g + fg'$;
- $\deg f' < \deg f$ wenn $f \neq 0$.

Satz 3.32. *Sei $\mathbb{K}$ ein Körper und sei $f \in \mathbb{K}[x]$ ein Polynom.*

(i) Man nehme $\operatorname{char}\mathbb{K} = 0$ an. $f' = 0$ gilt genau dann, wenn f konstant ist.

(ii) Man nehme $\operatorname{char}\mathbb{K} = p > 0$ an. $f' = 0$ gilt genau dann, wenn es in f nur Terme mit durch p teilbarem Grade gibt.

(iii) Man nehme $\mathbb{K} = \mathbb{F}_p$ an. $f' = 0$ gilt genau dann, wenn f die p-te Potenz eines Polynoms in $\mathbb{F}_p[x]$ ist. Daher, wenn $f' = 0$, ist f reduzibel.

Beweis. Sei f und f' als in Definition 3.27. So

$$f' = 0 \quad \Leftrightarrow \quad \forall i > 0,\ ia_i = 0 \text{ in } \mathbb{K}.$$

(i) Wenn $\operatorname{char}\mathbb{K} = 0$ gilt, ist dies äquivalent mit: $\forall i > 0,\ a_i = 0$ in $\mathbb{K}$, d.h. f ist konstant.

(ii) Wenn $\operatorname{char}\mathbb{K} = p$ ein Primzahl ist, ist die Bedingung oben äquivalent mit: für jedes nicht durch p teilbar $i > 0$, $a_i = 0$. D.h., in f erscheinen nur Potenzen von x^p.

(iii) Man nehme $\mathbb{K} = \mathbb{F}_p$ und $f' = 0$ an. Nach (ii) $f = \sum_j b_j x^{jp}$ mit $b_j \in \mathbb{F}_p$. Nach dem kleinen fermatschen Satz $b_j^p = b_j$. Deshalb $f = \sum_j b_j^p x^{jp} = (\sum_j b_j x^j)^p$. □

Korollar 3.33. *Sei $\mathbb{K}$ ein Körper mit $\operatorname{char}\mathbb{K} = 0$ oder $\mathbb{K} = \mathbb{F}_p$ für eine Primzahl p. Wenn $f \in \mathbb{K}[x]$ irreduzibel ist, dann gilt $f' \neq 0$.*[6]

Für die Körper, die man in diesem Kurse betrachtet, gibt es eine Characterisierung der quadratfreien Polynome:

Satz 3.34. *Sei $\mathbb{K}$ ein Körper und sei $f \in \mathbb{K}[x]$ ein nicht konstantes Polynom.*

1. *Wenn $\gcd(f, f') = 1$ gilt, dann ist f quadratfrei.*
2. *Wenn ($\operatorname{char}\mathbb{K} = 0$ oder $\mathbb{K} = \mathbb{F}_p$) und f quadratfrei ist, dann $\gcd(f, f') = 1$.*

Beweis. (1) Sei $f = cf_1^{\alpha_1} \cdots f_r^{\alpha_r}$ die Primfaktorzerlegung ($c \in \mathbb{K}^*$, $\alpha_i \in \mathbb{N}^+$, f_i monisch, irreduzibel und paarweise verschieden). Dann $f' = c\sum_{i=1}^r \alpha_i f_1^{\alpha_1} \cdots f_i^{\alpha_i - 1} \cdots f_r^{\alpha_r} f_i'$. So $f_1^{\alpha_1 - 1} \cdots f_r^{\alpha_r - 1}$ ist ein gemeinsamer Teiler von f und von f'. Da $\gcd(f, f') = 1$, gilt $\alpha_1 = \cdots = \alpha_r = 1$, d.h. f ist quadratfrei.

(2) Sei $f = cf_1 \dots f_r$ die Primfaktorzerlegung. Dann $f' = c\sum_{I=1}^r f_1 \cdots f_i' \cdots f_r$. Nach Kontraposition nehme man an, dass f_1 ein Teiler von f' ist. Dann $f_1 \mid f_1' f_2 \cdots f_r$, deshalb $f_1 \mid f_1'$. Aber $\deg f_1' < \deg f_1$. Deshalb $f_1' = 0$. Dies ist absurd nach Korollar 3.33. □

Aufgabe 3.3.2. Konstruieren Sie eine Funktion `IstQuadratfrei`, die testet, ob ein Polynom in $\mathbb{Q}[x]$ oder in $\mathbb{F}_p[x]$ quadratfrei ist.

Aufgabe 3.3.3. Bestimmen Sie die Primfaktorzerlegung von $x^9 - x^6 - 1 \in \mathbb{F}_3[x]$.

3.4 Der Ring $\mathbb{K}[x]/(f)$

Beispiel 3.35. Man betrachtet das Polynom $f = x^3 - x + 1 \in \mathbb{Q}[x]$. Man will einen neuen Ring $\mathbb{Q}[x]/(f)$ konstruieren. Eine erste Definition ist, dass $\mathbb{Q}[x]/(f)$ der $\mathbb{Q}$-Vektorraum von Polynomen in $\mathbb{Q}[x]$ mit Grade $< \deg(f) = 3$ ist. Mit anderen Worten ist $\mathbb{Q}[x]/(f)$ der $\mathbb{Q}$-Vektorraum mit Basis $\{1, x, x^2\}$. Deshalb hat $\mathbb{Q}[x]/(f)$ die Summe + und die Skalarmultiplikation.

Man will ein Produkt auf $\mathbb{Q}[x]/(f)$ konstruieren; zu diesem Zweck braucht man das Polynom f. Für jede $a, b \in \mathbb{Q}[x]/(f)$ betrachtet man das Produkt ab in $\mathbb{Q}[x]$; der Grade dieses Polynoms könnte größer als 2 sein, deshalb man nimmt den Rest der Teilung von ab durch f. Dies Rest hat immer einen Grad $< \deg(f) = 3$. Dies definiert ein Produkt auf $\mathbb{Q}[x]/(f)$.

[6] Leider gibt es Körper mit positiver Charakteristik, wo es irreduzible Polynome mit nulle Ableitung gibt. Sie heißen nicht perfekte Körper.

Man macht einen Beispiel. Man will das Produkt von x und x^2 berechnen. Ihr Produkt in $\mathbb{Q}[x]$ ist x^3, aber man muss den Rest von x^3 durch $f = x^3 - x + 1$ nehmen. Man hat $x^3 = 1 \cdot f + x - 1$. Deshalb gilt

$$x \cdot x^2 = x^3 = x - 1 \quad \text{in } \mathbb{Q}[x]/(f). \tag{2}$$

Man macht einen anderen Beispiel: was ist das Produkt von x^2 und x^2+1 in $\mathbb{Q}[x]/(f)$? Anfangs berechnet man das Produkt in $\mathbb{Q}[x]$: $x^2(x^2+1) = x^4+x^2$ in $\mathbb{Q}[x]$. Jetzt muss den Rest der Teilung von $x^4 + x^2$ durch $f = x^3 - x + 1$ berechnen: man hat

$$x^4 + x^2 = x(x^3 - x + 1) + 2x^2 - x, \tag{3}$$

so der Rest ist $2x^2 - x$. Deshalb $x^2(x^2 + 1) = 2x^2 - x$ in $\mathbb{Q}[x]/(f)$. Um dies zu berechnen, haben wir die Teilung (3) gemacht; aber der Quotient x war völlig nutzlos. Jetzt will ich erklären eine Art, um den Rest zu berechnen, ohne die Teilung machen. Die Idee ist, dass im Ring $\mathbb{Q}[x]/(x^3-x+1)$ die Gleichung $x^3 = x-1$ gilt; deshalb kann man diese Gleichung benutzen, immer wenn man x^3 findet, d.h. man kann x^3 durch $x-1$ ersetzen. Zum Beispiel gelten die folgenden Gleichungen im Ring $\mathbb{Q}[x]/(x^3 - x + 1)$

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

Auf diese Art bekommt das schon gewonnene Ergebnis.

Indem man diese letzte Art benutzt, kann man die Produkte im Ring $\mathbb{Q}[x]/(f)$ berechnen. Zum Beispiel gelten die folgenden Gleichungen im Ring $\mathbb{Q}[x]/(x^3 - x + 1)$

$$\begin{aligned}
&x^3 = x - 1\\
&x^4 = x \cdot x^3 = x(x - 1) = x^2 - x\\
&x^5 = x \cdot x^4 = x(x^2 - x) = x^3 - x^2 = x - 1 - x^2 = -1 + x - x^2 \quad \text{oder}\\
&x^5 = x^2 \cdot x^3 = x^2(x - 1) = x^3 - x^2 = x - 1 - x^2 = -1 + x - x^2\\
&x^6 = (x^3)^2 = (x - 1)^2 = 1 - 2x + x^2 \quad \text{oder}\\
&x^6 = x \cdot x^5 = x(-1 + x - x^2) = -x + x^2 - x^3 = -x + x^2 - (x - 1) = 1 - 2x + x^2
\end{aligned}$$

Jetzt generalisiere man den Beispiel 3.35. Sei $\mathbb{K}$ ein Körper und sei

$$f = x^d + a_{d-1}x^{d-1} + \cdots + a_1x + a_0 \tag{4}$$

ein monisches Polynom mit Grade $d \geq 1$. $\mathbb{K}[x]/(f)$ ist der $\mathbb{K}$-Vektorraum mit Basis $\{1, x, x^2, \ldots, x^{d-1}\}$. Diese Basis heißt die *monomielle Basis* von $\mathbb{K}[x]/(f)$. Zurzeit hat man die Summe un die Skalarmultiplikation definiert.

Das Produkt auf $\mathbb{K}[x]/(f)$ wird durch

$$a \cdot_{\mathbb{K}[x]/(f)} b := \text{ der Rest der Teilung von } a \cdot_{\mathbb{K}[x]} b \text{ durch } f$$

für alle $a, b \in \mathbb{K}[x]/(f)$ definiert. Man kann beweisen, dass $\mathbb{K}[x]/(f)$ ein Ring ist. Im Ring $\mathbb{K}[x]/(f)$ gilt die Gleichung

$$x^d = -a_{d-1}x^{d-1} - \cdots - a_1x - a_0.$$

Diese Gleichung ist sehr nützlich, um Berechnungen im Ring $\mathbb{K}[x]/(f)$ zu machen. Die durch

$$a \mapsto \text{ der Rest der Teilung von } a \text{ durch } f$$

definierte Funktion

$$\mathbb{K}[x] \to \mathbb{K}[x]/(f)$$

ist ein surjektiver Ringhomomorphismus und ihr Kern ist die Menge aller Vielfachen von f.

Beispiel 3.36. Man betrachtet das Polynom $f = x^5 + x + 1 \in \mathbb{F}_2[x]$. Deshalb gilt im Ring $\mathbb{F}_2[x]/(f)$ die Gleichung $x^5 + x + 1 = 0$. Man erinnere sich daran, dass $2 = 0$ und $1 = -1$ in $\mathbb{F}_2$ gelten. Deshalb gilt

$$x^5 = -x - 1 = x + 1 \quad \text{in } \mathbb{F}_2[x]/(f)$$

Jetzt berechnet man einige Potenzen von x in $\mathbb{F}_2[x]/(f)$:

$$x^6 = x \cdot x^5 = x(x+1) = x + x^2$$

$$x^7 = x \cdot x^6 = x(x + x^2) = x^2 + x^3$$

$$x^8 = x \cdot x^7 = x(x^2 + x^3) = x^3 + x^4$$

Beispiel 3.37. Man betrachtet das Polynom $f = x^5 - x^4 - 2x^3 - x^2 + x + 1 \in \mathbb{F}_5[x]$. Man will einige Potenzen von x in $\mathbb{F}_5[x]/(f)$ als Linearkombinationen der Basis $\{1, x, x^2, x^3, x^4\}$ darstellen.

Wir beginnen mit x^5. Wir wissen, dass die Gleichung

$$x^5 = -(-x^4 - 2x^3 - x^2 + x + 1) = x^4 + 2x^3 + x^2 - x - 1$$

in $\mathbb{F}_5[x]/(f)$ gilt. Dies stellt $x^5 \in \mathbb{F}_5[x]/(f)$ als Linearkombination von $1, x, x^2, x^3, x^4$ dar.

Was sollte man machen, um das gleiche mit x^{10} zu machen? Man sollte den Rest der Teilung von x^{10} durch f berechnen. Es ist langweilig dies ohne Rechner zu machen. Deshalb benutzt man Singular:

```
ring r = 5,x,dp;
poly f = x^5-x^4-2*x^3-x^2+x+1;
x^10 mod f;
```

Singular sagt, dass der Rest der Teilung von x^{10} durch f gleich $x^4 - 2x^3 + 2x^2 - 2x$ ist. Deshalb

$$x^{10} = x^4 - 2x^3 + 2x^2 - 2x \quad \text{in } \mathbb{F}_5[x]/(f).$$

Analog kann man die folgenden Gleichungen in $\mathbb{F}_5[x]/(f)$ erzielen:

$$x^{15} = 2x^4 + x^3 + x^2 + x + 1$$
$$x^{20} = 2x^4 + x^3 - 2x$$

Aufgabe 3.4.1. Man setzt Beispiel 3.37 fort. Man betrachte das Polynom $f = x^5 - x^4 - 2x^3 - x^2 + x + 1 \in \mathbb{F}_5[x]$ und den Ring $A = \mathbb{F}_5[x]/(f)$. Man betrachte die monomielle Basis von A: $\{1, x, x^2, x^3, x^4\}$. Man stelle $x^{15} \in A$ und $x^{20} \in A$ als Linearkombination der Elementen der monomiellen Basis von A dar.

Das analoge von Satz 2.20 ist:

Satz 3.38. *Sei $\mathbb{K}$ ein Körper und sei $f \in \mathbb{K}[x]$ ein Polynom. Der Ring $\mathbb{K}[x]/(f)$ ist ein Körper genau dann, wenn f irreduzibel ist.*

Aufgabe 3.4.2. Man zeige, dass der Ring $\mathbb{F}_3[x]/(x^2 + x + 2)$ ein Körper mit 9 Elementen ist.

Aufgabe 3.4.3. Gibt es Nullteiler im Ring $\mathbb{Q}[x]/(x^2 - 2)$? Und in $\mathbb{R}[x]/(x^2 - 2)$?

Aufgabe 3.4.4. Sei $\mathbb{K}$ ein Körper und sei $f \in \mathbb{K}[x]$ ein Polynom mit Grade ≥ 1. Man betrachte den Ring $A = \mathbb{K}[x]/(f)$. Man beweise die folgenden Aussagen.

- Jedes nilpotente Element von A ist null genau dann, wenn f quadratfrei ist.
- Jeder Nichtnullteiler in A hat ein multiplikatives Inverses in A.
- Jeder Nullteiler in A ist nilpotent genau dann, wenn f einen einzigen monischen Primfaktor hat.

Aufgabe 3.4.5. Sei p eine Primzahl. Man betrachte den Ring $A = \mathbb{F}_p[x]/(x^2+1)$. Man beweise:

- wenn $p = 2$, dann ist A isomorph zu $\mathbb{F}_2[x]/(x^2)$;
- wenn $p \equiv 1 \mod 4$, dann ist A isomorph zu $\mathbb{F}_p \times \mathbb{F}_p$;
- wenn $p \equiv 3 \mod 4$, dann ist A ein Körper mit p^2 Elementen.

Aufgabe 3.4.6. Sei $\mathbb{K}$ ein Körper und sei $f \in \mathbb{K}[x]$ ein monisches Polynom mit Grade $d \geq 1$ als in (4). Man betrachte den Ring $A = \mathbb{K}[x]/(f)$, der ein $\mathbb{K}$-Vektorraum der Dimension d ist. Man betrachte den Linearendomorphismus $T\colon A \to A$, die durch die Multiplikation mit x definiert wird. Was ist die Abbildungsmatrix (Darstellungsmatrix) von T bezüglich der monomiellen Basis von A? Was ist das charakteristische Polynom von T? Was ist das minimale Polynom von T?

4 Primfaktorzerlegung in $\mathbb{F}_p[x]$

In diesem Abschnitt folgt man hauptsächlich dem Kapitel 26.C in [Chi09]. Eine andere Literaturangabe ist Kapitel 8.1-8.3 in [Koe06]. Eine erschöpfende Quelle ist Kapitel 4.6 in [Knu98].

In §3 hat man Polynome mit Koeffizienten in beliebigen Körpern betrachtet.[7] Ab sofort betrachtet man nur Polynome mit Koeffizienten in $\mathbb{F}_p$, wo p eine beliebige Primzahl ist. Die Zauberei von $\mathbb{F}_p$ (und genereller von der Ringen der Charakteristik p) besteht in der Existenz eines Ringhomomorphismus mit speziellen Eigenschaften.

4.1 Der Frobeniushomomorphismus

Sei p eine Primzahl. Sei A ein Ring der Charakteristik p, d.h. die Gleichung $p = 0$ gilt in A. Beispiele sind: $A = \mathbb{F}_p$, $A = \mathbb{F}_p[x]$, oder $A = \mathbb{F}_p[x]/(f)$ mit $f \in \mathbb{F}_p[x]$. Der *Frobeniushomomorphismus* von A ist die Funktion

$$\mathrm{Fr}_A\colon A \to A,$$

die durch $a \mapsto a^p$ definiert wird. Er ist ein Ringhomomorphismus, weil

$$\mathrm{Fr}_A(1) = 1^p = 1,$$
$$\mathrm{Fr}_A(a+b) = (a+b)^p = a^p + \sum_{i=1}^{p-1} \binom{p}{i} a^i b^{p-i} + b^p = a^p + b^p = \mathrm{Fr}_A(a) + \mathrm{Fr}_A(b),$$
$$\mathrm{Fr}_A(ab) = (ab)^p = a^p b^p = \mathrm{Fr}_A(a)\mathrm{Fr}_A(b)$$

gelten.

[7] Die einzigen Ausnahmen sind Korollar 3.33 und Satz 3.34(2).

Beispiel 4.1. Man betrachte das Polynom $f = x^5 + x + 1 \in \mathbb{F}_2[x]$ und den Ring $A = \mathbb{F}_2[x]/(f)$. (Wir setzen den Beispiel 3.36 fort.) Man weiß, dass A ein $\mathbb{F}_2$-Vektorraum der Dimension 5 ist. Die monomielle Basis von A ist $\{1, x, x^2, x^3, x^4\}$. Sei $\mathrm{Fr}_A \colon A \to A$ der Frobeniushomomorphismus. Insbesondere ist Fr_A ein $\mathbb{F}_2$-lineare Endomorphismus des $\mathbb{F}_2$-Vektorraumes A. Was ist die Abbildungsmatrix (Darstellungsmatrix) von Fr_A bezüglich der monomiellen Basis von A?

Man bezeichne diese Matrix mit Q. Deshalb ist Q eine quadratische Matrix mit Koeffizienten in $\mathbb{F}_2$, mit 5 Zeilen und 5 Spalten. Wir haben

$$\begin{aligned}
\mathrm{Fr}_A(1) &= 1 \\
\mathrm{Fr}_A(x) &= x^2 \\
\mathrm{Fr}_A(x^2) &= x^4 \\
\mathrm{Fr}_A(x^3) &= x^6 = x \cdot x^5 = x(x+1) = x + x^2 \\
\mathrm{Fr}_A(x^4) &= x^8 = x^2 \cdot x^6 = x^2(x + x^2) = x^3 + x^4.
\end{aligned}$$

Deshalb

$$Q = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix} \in M_5(\mathbb{F}_2). \tag{5}$$

Aufgabe 4.1.1. Man setzt den Beispiel 3.37 fort. Sei $f = x^5 - x^4 - 2x^3 - x^2 + x + 1 \in \mathbb{F}_5[x]$ und sei $A = \mathbb{F}_5[x]/(f)$. Was ist die Abbildungsmatrix Q vom Frobeniushomomorphismus $\mathrm{Fr}_A \colon A \to A$ bezüglich der monomiellen Basis von A?

Aufgabe 4.1.2. Man konstruiere eine Funktion `Frobenius`, die ein monisches Polynom $f \in \mathbb{F}_p[x]$ als Input nimmt und die Abbildungsmatrix Q vom Frobeniushomomorphismus von $\mathbb{F}_p[x]/(f)$ bezüglich der monomiellen Basis als Output gibt.

Es kann nützlich sein, zu wissen, wie die Matrizen zu manipulieren: `https://www.singular.uni-kl.de/Manual/4-0-3/sing_129.htm`. Zum Beispiel ist `matrix m[d][d];` eine Deklaration einer quadratischen Matrix mit d Zeilen; die Anfangseinträge sind null. Der Befehl `m[i,j] = 1;` ist eine Anweisung und diktiert, dass das Element in der i-ten Zeile und der j-ten Spalte gleich 1 ist. Wenn Sie eine Matrix `m` in Singular sehen wollen, sollen Sie den Befehl `print(m);` benutzen.

Testen Sie Ihre Funktion mit einigen Polynomen.

4.2 Der Berlekamp-Algorithmus

Beispiel 4.2. Man setzt den Beispiel 4.1 fort. Man betrachte das Polynom $f = x^5 + x + 1 \in \mathbb{F}_5[x]$, den Ring $A = \mathbb{F}_5[x]/(f)$ und die Matrix Q in (5), die die Abbildungsmatrix vom Frobeniushomomorphismus von A bezüglich der monomiellen Basis von A ist.

Man will den Eigenraum von Q zum Eigenwert 1 betrachten:

$$\ker(Q - I),$$

wobei I die Einheitsmatrix ist. Man hat

$$Q - I = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 \end{pmatrix}$$

Wir wollen das folgende lineare Gleichungssystem lösen:

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

d.h.

$$\begin{cases} 0 = 0 \\ b_1 + b_3 = 0 \\ b_1 + b_2 + b_3 = 0 \\ b_3 + b_4 = 0 \\ b_2 = 0 \end{cases}$$

d.h.

$$\begin{cases} b_1 = b_3 = b_4 \\ b_2 = 0 \end{cases}$$

Eine Basis von $\ker(Q - I)$ ist aus den Vektoren

$$\begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \quad b = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \\ 1 \end{pmatrix}$$

bestanden. Der erste Vektor entspricht $1 \in A$ und ist nutzlos. Der zweite Vektor b entspricht $h = x + x^3 + x^4 \in A$. Da $Qb = b$ gilt, gilt $\mathrm{Fr}_A(h) = h$, d.h. gilt die Gleichung $h^2 = h$ in A. Man hat

$$h(h-1) = 0 \quad \text{in } A = \mathbb{F}_2[x]/(f).$$

Dies bedeutet, dass der Rest der Teilung von $h(h-1)$ durch f gleich 0 ist. Deshalb f teilt $h(h-1)$ in $\mathbb{F}_2[x]$, d.h.

$$f = \gcd(f, h(h-1)). \tag{6}$$

Man bemerke, dass h und $h-1$ relativisch prim sind, d.h. $\gcd(h, h-1) = 1$. Deshalb $\gcd(f, h(h-1)) = \gcd(f, h) \cdot \gcd(f, h-1)$. Mit der Gleichung 6 haben wir

$$f = \gcd(f, h) \cdot \gcd(f, h-1) \tag{7}$$

Dies ist eine wichtige Gleichung! Aus $\deg h < \deg f$ deduziert man $\deg \gcd(f, h) < \deg f$ und $\deg \gcd(f, h-1) < \deg f$. Deshalb ist (7) eine nicht-triviale Zerlegung von f, d.h. weder $\gcd(f, h)$ noch $\gcd(f, h-1)$ sind konstant.

Man kann berechnen:

$$\gcd(f, h) = \gcd(x^5 + x + 1, x + x^3 + x^4) = x^3 + x^2 + 1,$$
$$\gcd(f, h-1) = \gcd(x^5 + x + 1, 1 + x + x^3 + x^4) = x^2 + x + 1.$$

Deshalb

$$f = (x^3 + x^2 + 1)(x^2 + x + 1).$$

Die zwei Faktoren haben keine Nullstelle in $\mathbb{F}_2$, deshalb sie sind irreduzibel in $\mathbb{F}_2[x]$ aus Satz 3.21. Deshalb ist dies die Primfaktorzerlegung von f.

Aufgabe 4.2.1. Man setzt Aufgabe 4.1.1 fort. Sei $f = x^5 - x^4 - 2x^3 - x^2 + x + 1 \in \mathbb{F}_5[x]$, sei $A = \mathbb{F}_5[x]/(f)$ und sei Q die Abbildungsmatrix vom Frobeniushomomorphismus $\mathrm{Fr}_A \colon A \to A$ bezüglich der monomiellen Basis von A.

- Bestimmen Sie eine Basis des Eigenraumes $\ker(Q - I)$ zum Eigenwert 1. (Die Einheitsmatrix I wird durch `1` in Singular bezeichnet. Wenn B eine Matrix ist, konstruiert der Befehl `matrix M = syz(B)` eine neue Matrix M, deren Spalten ein Erzeugendensystem vom Vektorraum $\ker(B)$ bilden.)
- Wählen Sie einen Vektor

$$b \in \ker(Q - I) \smallsetminus \mathrm{Span} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

  und betrachten Sie das entsprechende Polynom $h \in \mathbb{F}_5[x]$ mit Grade ≥ 1 und < 5. Überzeugen Sie sich davon, dass f ein Teiler von $h^5 - h$ ist und dass die Gleichung

$$f = \gcd(f, h) \cdot \gcd(f, h-1) \cdot \gcd(f, h-2) \cdot \gcd(f, h-3) \cdot \gcd(f, h-4).$$

  gilt.
- Finden Sie die Primfaktorzerlegung von f.

Aufgabe 4.2.2. Indem man Beispiel 4.2 und Aufgabe 4.2.1 imitiert, finden Sie die Primfaktorzerlegung von $x^5 - 3x^4 + 4x^3 + 2x^2 + 3x + 5 \in \mathbb{F}_{11}[x]$.

Aufgabe 4.2.3. Indem man Beispiel 4.2 und Aufgabe 4.2.1 imitiert, was passiert mit dem Polynom $x^4 - 3x^2 - 3 \in \mathbb{F}_7[x]$?

Satz 4.3 (Berlekamp [Ber67])**.** *Sei p eine Primzahl und sei $f \in \mathbb{F}_p[x]$ ein monisches Polynom mit Grade $d \geq 1$. Für jedes $j = 0, \ldots, d-1$ sei $r_{0,j} + r_{1,j}x + \cdots + r_{d-1,j}x^{d-1}$ der Rest in der Teilung von x^{jp} durch f in $\mathbb{F}_p[x]$. Man betrachte die quadratische Matrix*

$$Q = \begin{pmatrix} r_{0,0} & r_{0,1} & \cdots & r_{d-1,0} \\ r_{1,0} & r_{1,1} & \cdots & r_{d-1,1} \\ \vdots & \vdots & \ddots & \vdots \\ r_{d-1,0} & r_{d-1,1} & \cdots & r_{d-1,d-1} \end{pmatrix}$$

mit d Zeilen, mit d Spalten und mit Einträgen in $\mathbb{F}_p$. Dann die folgenden Aussagen gelten.

1. *$r_{0,0} = 1$ und $r_{1,0} = \cdots = r_{d-1,0} = 0$. Die erste Spalte von Q ist*

$$\begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

   und ist in $\ker(Q - I)$ enthalten, d.h. sie ist ein Eigenvektor von Q mit Eigenwert 1.
2. *Die Zahl von verschiedenen monischen irreduziblen Faktoren von f ist gleich $\dim_{\mathbb{F}_p} \ker(Q - I)$, d.h. die geometrische Vielfachheit vom Eigenwert 1 von Q.*

3. f ist irreduzibel genau dann, wenn $\gcd(f, f') = 1$ *und* $\dim_{\mathbb{F}_p} \ker(Q - I) = 1$.

4. Wenn

$$\begin{pmatrix} b_0 \\ b_1 \\ \vdots \\ b_{d-1} \end{pmatrix} \in \ker(Q - I) \smallsetminus \operatorname{Span} \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

gilt und $h = b_0 + b_1 x + \cdots + b_{d-1} x^{d-1}$ *hat Grad* ≥ 1*, dann gilt*

$$f = \gcd(f, h) \cdot \gcd(f, h - 1) \cdot \ldots \cdot \gcd(f, h - (p - 1)) \tag{8}$$

und diese Zerlegung von f ist nicht trivial.

Die Matrix Q ist die Abbildungsmatrix der Frobeniushomomorphismus vom Ringe $\mathbb{F}_p[x]/(f)$ bezüglich der monomiellen Basis.

Beweis. (1) das ist klar, denn $x^0 = 1$ und sein Rest in der Teilung durch f ist 1.

(2) das ist auszulassen, weil ich keinen einfachen Beweis kenne. Außerdem liest man in der Mehrheit der Quellen, dass f quadratfrei sein muss, aber diese Annahme ist nutzlos (man sehe [GMT89, Proposition 3])). Hier skizziere ich einen Beweis, der ein bisschen kommutative Algebra benutzt. Ich befürchte, dass er der Mehrheit von Ihnen zu schwierig ist.

Set $A = \mathbb{F}_p[x]/(f)$; this is a finite $\mathbb{F}_p$-algebra. Since Q is the matrix that represents the Frobenius endomorphism of A with respect to the monomial basis of A, it is clear that the eigenspace $\ker(Q - I)$ is $B = \{a \in A \mid a^p = a\}$. One should observe that B is a $\mathbb{F}_p$-subalgebra of A, called the Berlekamp subalgebra of A. So we need to show that the number of prime ideals of the artinian ring A coincides with $\dim_{\mathbb{F}_p} B$. By the Chinese remainder theorem, A is isomorphic to the product of local finite $\mathbb{F}_p$-algebras $A_1 \times \cdots \times A_r$: and the subalgebra B is $B_1 \times \cdots \times B_r$, where B_i is the Berlekamp subalgebra of A_i. So we conclude if we show that each B_i is $\mathbb{F}_p$.

In other words, it is enough to show that if A is a local finite $\mathbb{F}_p$ algebra then its Berlekamp subalgebra B is $\mathbb{F}_p$. Each element b of B satisfies $b^p = b$, so it is clear that every nilponent contained in B is zero. Since A is local, every non-nilpotent element in A is invertible. Therefore every non-zero element in B is invertible in A, in particular a non-zero-divisor in B. Therefore B is an integral domain. As all elements of B satisfy the polynomial equation $X^p - X = 0$, B has at most p elements. This implies that B contains at most p elements. But on the other hand B contains $\mathbb{F}_p$, therefore $B = \mathbb{F}_p$.

(3) f ist irreduzibel genau dann, wenn f quadratfrei ist und einen einzigen monischen irreduziblen Faktor hat. Man endet nach (2) und Satz 3.34.

(4) Sei $b \in (\mathbb{F}_p)^n$ der in (4) betrachtete Vektor und sei $h = b_0 + b_1 x + \cdots + b_{d-1} x^{d-1} \in \mathbb{F}_p[x]$ der betrachtete Polynom. Da $b \notin \operatorname{Span}(e_1)$, hat h Grad ≥ 1.

Man betrachte den Ring $A = \mathbb{F}_p[x]/(f)$. Die Matrix Q ist die Darstellungsmatrix von dem Frobeniushomomorphismus $\mathrm{Fr}_A \colon A \to A$ bezüglich der Basis $\{1, x, \ldots, x^{d-1}\}$. Der Eigenraum $\ker(Q - I)$ entspricht $B = \{a \in A \mid \mathrm{Fr}_A(a) = a\} = \{a \in A \mid a^p = a\}$. Da $b \in \ker(Q - I)$, hat man

$$h^p = h \text{ in } \mathbb{F}_p[x]/(f),$$

d.h.

$$f \quad \text{teilt} \quad h^p - h = \prod_{i=0}^{p-1} (h - i) \quad \text{in } \mathbb{F}_p[x].$$

Die Polynome $h - i$, für $i = 0, \ldots, p-1$, sind paarweise teilerfremd (relativ prim). Dies impliziert die Gleichung (8). Diese ist eine nicht triviale Zerlegung, denn der Grad jedes Faktors ist $\leq \deg h \leq d - 1$. □

Aufgabe 4.2.4. Konstruieren Sie eine Funktion `ZahlIrreduziblerFaktoren`, die mithilfe Teiles 2 in Satz 4.3 die Zahl von verschiedenen monischen irreduziblen Faktoren eines Polynoms in $\mathbb{F}_p[x]$ berechnet.

Aufgabe 4.2.5. Konstruieren Sie eine Funktion `IstIrreduzibel`, die mithilfe Teiles 3 in Satz 4.3 testet, ob ein Polynom in $\mathbb{F}_p[x]$ irreduzibel ist.

Bemerkung 4.4. Man erinnere sich an der Aufgabe 2.1.1, wo eine Funktion konstruiert wurde, um zu testen, ob eine ganze Zahl prim ist. In jener Funktion musste man viele etwaige Teiler; man könnte eine ähnliche Funktion für Polynome konstruieren. Trotzdem ist die Funktion in Aufgabe 4.2.5 viel besser, weil sie keine Teiler testet, deshalb sie ist schnell.

Aufgabe 4.2.6. Für welche Primzahlen p ist $x^4 + 1$ irreduzibel in $\mathbb{F}_p[x]$? Testen Sie viele Primzahlen mithilfe von Singular und stellen Sie eine Vermutung an.

Aufgabe 4.2.7. Wählen Sie Ihre Lieblingsprimzahl p und Ihr Lieblingspolynom $f \in \mathbb{F}_p[x]$, sodass f monisch ist. Benutzen die in diesem Abschnitte erklärten Ideen und versuchen Sie, die Primfaktorzerlegung von f zu finden.

4.3 Zusammenfassende Aufgaben

Satz 4.5. *Sei $\mathbb{K}$ ein Körper mit* $\operatorname{char}\mathbb{K} = 0$ *oder $\mathbb{K} = \mathbb{F}_p$ für eine Primzahl p. Sei $f \in \mathbb{K}[x]$ ein Polynom mit Grade* $\deg f \geq 1$ *und sei $g = \gcd(f, f')$. Dann gilt genau eine unten den folgenden Aussagen.*

1. $\deg g = 0$, $g = 1$ *und f ist quadratfrei.*
2. $1 \leq \deg g < \deg f$ *und die Zerlegung $f = g \cdot (f/g)$ ist nicht trivial.*
3. $\deg g = \deg f$, $f' = 0$, $\mathbb{K} = \mathbb{F}_p$ *für eine Primzahl p und es gibt $r \in \mathbb{N}^+$ und $a_0, \ldots, a_r \in \mathbb{F}_p$ mit*
$$f = \sum_{i=0}^{r} a_i x^{ip} = \left(\sum_{i=0}^{r} a_i x^i \right)^p .$$

Beweis. Da f nicht null ist, ist g nicht null und $\deg g \leq \deg f$. Es gibt 3 Möglichkeiten:

1. $\deg g = 0$. Deshalb g ist eine Konstant $\neq 0$. Da g monisch ist, gilt $g = 1$. Aus Satz 3.34 ist f quadratfrei.
2. $1 \leq \deg g < \deg f$. Es ist klar, dass $1 \leq \deg(f/g) < \deg f$ gilt. Deshalb ist $f = g \cdot (f/g)$ eine nicht triviale Zerlegung.
3. $\deg g = \deg f$. Da $\deg f' < \deg f$, impliziert dies, dass $f' = 0$. Man benutze den Beweis in Satz 3.32(iii).

□

Wenn es einen einzigen irreduziblen Faktor gibt, kann die Satz 4.3(4) nicht verwendet werden. So wie bestimmt man die Primfaktorzerlegung? Man berechnet den ggT mit der Ableitung und es gibt mehrere Möglichkeiten gemäß dem Satze 4.5.

Beispiel 4.6. Man betrachte $f = x^{12} + 2x^{10} + 2x^2 - 1 \in \mathbb{F}_5[x]$. Wenn man die Funktionen in Aufgabe 4.2.4 benutzt, entdeckt man, dass f eine Potenz eines irreduziblen Polynoms ist. Man kann nicht den Berlekamp-Algorithmus benutzen, um die Primfaktorzerlegung von f zu bestimmen.

Man will Satz 4.5 benutzen. Mit Singular berechnet man $g = \gcd(f, f') = x^{10} + 2$. Außerdem $f/g = x^2 + 2$. Jetzt soll man $g = x^{10} + 2$ und $x^2 + 2$ zerlegen. Um das zu tun, könnte man Satz 4.5 mit g und mit f/g verwenden.

Trotzdem ist der Fall von $x^2 + 2$ einfach. Man sieht, dass $x^2 + 2$ irreduzibel ist, weil es keine Nullstelle in $\mathbb{F}_5$ hat.

Man berechnet $\gcd(g, g') = g$ und $g' = 0$. Wir sind im Fall 3 in Satz 4.5, so g ist die 5-te Potenz eines Polynoms: $g = (x^2 + 2)^5$.

Deshalb $f = (x^2 + 2)^6$.

Wir haben zwei Algorithmen umrissen:

- Der Satz von Berlekamp (Satz 4.3) funktioniert mit Polynomen mit Koeffizienten in $\mathbb{F}_p$. Der Teil 4 dieses Satzes funktioniert nicht, wenn das Polynom die Potenz eines irreduziblen Polynoms ist. Eine wiederholte Benutzung dieses Satzes ergibt eine Zerlegung, in der die Faktoren Potenzen von paarweise relativische primen irreduziblen Polynomen sind.
- Der Satz 4.5 funktioniert mit Polynomen mit Koeffizienten in einem Körper der Charakteristik 0 oder in $\mathbb{F}_p$. Eine wiederholte Benutzung dieses Satzes ergibt eine Zerlegung, in der die Faktoren quadratfrei sind; aber die Faktoren können nicht relativisch prim sein.

Diese zwei Algorithmen haben Vor- und Nachteile und sie ergänzen einander, um die Primfaktorzerlegung aller Polynome in $\mathbb{F}_p[x]$ zu finden.

Beispiel 4.7. Man betrachte das Polynom

$$f = x^7 + 3x^5 + 4x^4 + 3x^3 - 3x^2 + x + 4 \in \mathbb{F}_{11}[x].$$

Wir benutzen den Berlekamp-Satz. Mit der Funktion `ZahlIrreduziblerFaktoren` entdeckt, dass f zwei irreduzible Faktoren hat. Mit der Funktion `Frobenius` berechnet man die Abbildungsmatrix des Frobeniushomomorphismus von $\mathbb{F}_{11}[x]/(f)$:

$$Q = \begin{pmatrix} 1 & -2 & 3 & 2 & 4 & 4 & 0 \\ 0 & -1 & 3 & 1 & 3 & -2 & 2 \\ 0 & 1 & 2 & -4 & -3 & -1 & 5 \\ 0 & -5 & -5 & 5 & -5 & 4 & 4 \\ 0 & -3 & 3 & -3 & -4 & -3 & -4 \\ 0 & -5 & 3 & 5 & 3 & 5 & 2 \\ 0 & 5 & 5 & 3 & 2 & 2 & 3 \end{pmatrix}$$

Eine Basis von $\ker(Q - I)$ ist von den Spalten der Matrix

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \\ 0 & 1 \\ 0 & 0 \\ 0 & 2 \\ 0 & 0 \\ 0 & 1 \end{pmatrix}$$

gebildet. Indem man die zweite Spalte wählt, betrachtet man das Polynom $h = x^2 + 2x^4 + x^6$. Man kann kontrollieren, dass

$$f_1 = x^4 + 2x^2 + 1 \quad \text{und} \quad f_2 = x^3 + x + 4$$

die enzigen nicht trivialen Polynome in $\{\gcd(f, h - i) \mid 0 \leq i < 11\}$ sind. Eine Konsequenz der Tatsache, dass die $h-i$ relativisch prim sind, ist $\gcd(f_1, f_2) = 1$. Außerdem wusste man, dass f genau zwei irreduzible Faktoren hat. Deshalb ist f_1 die Potenz eines irreduziblen Polynoms und f_2 ist die Potenz eines anderen irreduziblen Polynoms.

Man kann nicht den Berlekamp-Satz mit f_1 oder mit f_2 verwenden. Wir benutzen Satz 4.5.

Anfangs mit f_1. Man berechnet $\gcd(f_1, f_1') = x^2 + 1$. Klar $f_1 / \gcd(f_1, f_1') = x^2 + 1$. Deshalb $f_1 = (x_2 + 1)^2$. Ist $x^2 + 1$ irreduzibel? Ja, weil $x^2 + 1$ quadrat frei ist, denn $\gcd(x^2 + 1, (x^2 + 1)') = \gcd(x^2 + 1, 2x) = 1$.

Jetzt mit f_2. $\gcd(f_2, f_2') = 1$. Deshalb ist f_2 irreduzibel.

Deshalb ist

$$f = (x^2 + 1)^2(x^3 + x + 4)$$

die Primfaktorzerlegung von f.

Die Befehle für diesen Beispiel sind unten.

```
ring r = 11,x,dp;
poly f = x7+3x5+4x4+3x3-3x2+x+4;
ZahlIrreduziblerFaktoren(f);
matrix Q = Frobenius(f);
print(Q);
matrix K = syz(Q-1);
print(K);
poly h = x^2 + 2*x^4 + x^6;
int i = 0;
while (i<11){
   gcd(f,h-i);
   i++;
}
poly f1 = x4+2x2+1;
poly f2 = x3+x+4;
gcd(f1,diff(f1,x));
gcd(f2,diff(f2,x));
```

Beispiel 4.8. Im Beispiel 4.7 hat man den Berlekamp-Satz und dann Satz 4.5 verwendet. Hier betrachtet man das gleiche Polynom $f \in \mathbb{F}_{11}[x]$, aber man verwendet Satz 4.5 anfangs und dann den Berlekamp-Satz.

Man berechnet $a_1 = \gcd(f, f') = x^2 + 1$ und $a_2 = f/a_1 = x^5 + 2x^3 + 4x^2 + x + 4$. Man hat $\gcd(a_1, a_1') = 1$ und $\gcd(a_2, a_2') = 1$. Deshalb sind a_1 und a_2 quadratfrei.

Jetzt verwendet den Berlekamp-Satz mit a_1 und a_2.

Mit `ZahlIrreduziblerFaktoren(a1);` sieht man, dass a_1 irreduzibel ist.

Mit `ZahlIrreduziblerFaktoren(a2);` sieht man, dass a_2 zwei irreduzible Faktoren

hat. Die Abbildungsmatrix des Frobeniushomomorphismus von $\mathbb{F}_{11}[x]/(a_2)$ ist

$$Q_{a_2} = \begin{pmatrix} 1 & -4 & 2 & 4 & 3 \\ 0 & -5 & 2 & -5 & 3 \\ 0 & 5 & -4 & -5 & 5 \\ 0 & -4 & 2 & 5 & 3 \\ 0 & -2 & 4 & 2 & 3 \end{pmatrix}$$

Eine Basis von $\ker(Q - I)$ ist von den Spalten der Matrix

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \\ 0 & 1 \\ 0 & 0 \end{pmatrix}$$

gebildet. Indem man die zweite Spalte wählt, betrachtet man das Polynom $h_1 = x + x^3$. Man kann kontrollieren, dass

$$x^2 + 1 \quad \text{und} \quad x^3 + x + 4$$

die enzigen nicht trivialen Polynome in $\{\gcd(a_2, h_1 - i) \mid 0 \leq i < 11\}$ sind. Mit der Funktion `IstIrreduzibel` sieht man, dass diese zwei Polynome irreduzibel sind.

Zusammenfassend hat man:

$$a_2 = (x^2 + 1)(x^3 + x + 4),$$
$$f = a_1 a_2 = (x^2 + 1)((x^2 + 1)(x^3 + x + 4)) = (x^2 + 1)^2(x^3 + x + 4).$$

Die Befehle für diesen Beispiel sind unten.

```
ring r = 11,x,dp;
poly f = x7+3x5+4x4+3x3-3x2+x+4;
poly a1 = gcd(f,diff(f,x));
poly a2 = f/a1;
gcd(a1,diff(a1,x));
gcd(a2,diff(a2,x));
ZahlIrreduziblerFaktoren(a1);
matrix Q = Frobenius(a2);
print(Q);
matrix K = syz(Q-1);
print(K);
poly h1 = x + x^3;
int i = 0;
while (i<11){
gcd(f,h1-i);
i++;
}
```

Aufgabe 4.3.1. Finden Sie die Primfaktorzerlegung der folgenden Polynome.

1. $f = x^4 + 2x + 1$ in $\mathbb{F}_3[x]$;
2. $f = x^3 + 4$ in $\mathbb{F}_5[x]$;

3. $f = x^4 + 3$ in $\mathbb{F}_7[x]$.

Aufgabe 4.3.2. Finden Sie die Primfaktorzerlegung von $x^6 + 2x^5 - x^4 + x^3 + 2x^2 + 1$ in $\mathbb{F}_3[x]$, $\mathbb{F}_5[x]$, $\mathbb{F}_{101}[x]$ und $\mathbb{F}_{2017}[x]$.

Aufgabe 4.3.3. Finden Sie die Primfaktorzerlegung des Polynoms $x^6+8x^5+11x^4+12x^3+x^2-2x-4$ in $\mathbb{F}_2[x]$, $\mathbb{F}_3[x]$, $\mathbb{F}_5[x]$, $\mathbb{F}_7[x]$ und $\mathbb{F}_{11}[x]$.

Aufgabe 4.3.4. Finden Sie die Primfaktorzerlegung des Polynoms $x^{37}+x^{23}+x^{17}+x^6+1 \in \mathbb{F}_2[x]$. Natürlich ist das Polynom h zu groß, sodass es nicht möglich ist, ohne Rechner es zu handhaben. Deshalb schreiben Sie einige Befehle, um h zu konstruieren.

5 Zusatzaufgaben

Die Aufgaben in diesem Abschnitt sind wahlfrei und die in diesen Aufgaben konstruierten Singular-Funktionen können **nicht** in der Prüfung benutzt werden. Trotzdem kann man in der Prüfung die bis jetzt konstruierten Funktionen verwenden, z.B. `hatNullstelle`, `IstQuadratfrei`, `Frobenius`, `IstIrreduzibel`, `ZahlIrreduziblerFaktoren`.

Die Singular-Befehle `diff`, `mod`, `gcd`, `syz` können in der Prüfung benutzt werden. Mächtigere Singular-Befehle über die Faktorisierung der Polynome sind in der Prüfung verboten.

Aufgabe 5.0.1. Dies ist die Forsetzung von Aufgabe 3.2.10. Hier arbeitet man in $\mathbb{F}_2[x]$, aber wenn Sie Singular benutzen, wäre es gut, wenn Sie etwas schreiben, das in $\mathbb{F}_p[x]$ für eine beliebige Primazahl p funktioniert.

i) Finden Sie alle monische irreduzible Polynome mit Grade 4 in $\mathbb{F}_2[x]$.

ii) Berechnen Sie das Produkt aller monischen irreduziblen Polynome in $\mathbb{F}_2[x]$ mit Grade 1, 2 und 4.

iii) Finden Sie alle monische irreduzible Polynome mit Grade 5 in $\mathbb{F}_2[x]$.

iv) Berechnen Sie das Produkt aller monischen irreduziblen Polynome in $\mathbb{F}_2[x]$ mit Grade 1 und 5.

Aufgabe 5.0.2. Wiederholen Sie Aufgabe 3.2.10 und Aufgabe 5.0.1 für $\mathbb{F}_3[x]$. Stellen Sie eine Vermutung an: wenn p eine Primzahl ist und $n \in \mathbb{N}^+$ eine positive ganze Zahl ist, was ist das Produkt aller monischen irreduziblen Polynome in $\mathbb{F}_p[x]$ mit Grade, der ein Divisor von n ist? Testen Sie Ihre Vermutung mit Ihre Lieblingsprimzahl p und Ihre Lieblingszahl $n \in \mathbb{N}^+$.

Aufgabe 5.0.3. Sei p eine ungerade Primzahl und sei $a \in \mathbb{F}_p \setminus \{0\}$. Man betrachte das Polynom $f = x^2 - a$ in $\mathbb{F}_p[x]$.

a) Zeigen Sie, dass f quadratfrei ist.

b) Zeigen Sie, dass der Rest der Teilung von x^p durch f gleich $a^{\frac{p-1}{2}}x$ ist.

c) Bestimmen Sie die Matrix $Q_f \in \mathrm{Mat}_2(\mathbb{F}_p)$.

d) Beweisen Sie, dass $f = x^2 - a$ irreduzibel in $\mathbb{F}_p[x]$ ist genau dann, wenn $a^{\frac{p-1}{2}} \neq 1$ in $\mathbb{F}_p$ gilt.

e) Beweisen Sie, dass a ein Quadrat in $\mathbb{F}_p$ ist genau dann, wenn $a^{\frac{p-1}{2}} = 1$ gilt.

Aufgabe 5.0.4. Sei $p \geq 5$ eine Primzahl und sei $a \in \mathbb{F}_p \setminus \{0\}$. Man betrachte das Polynom $f = x^3 - a$ in $\mathbb{F}_p[x]$.

a) Man beweise, dass f quadratfrei ist.

b) Für jedes $k \in \mathbb{Z}$, $k \geq 0$, beweisen Sie, dass der Rest der Teilung von x^k durch f gleich

$$\begin{cases} a^{\frac{k}{3}} & \text{wenn } k \equiv 0 \mod 3, \\ a^{\frac{k-1}{3}} x & \text{wenn } k \equiv 1 \mod 3, \\ a^{\frac{k-2}{3}} x^2 & \text{wenn } k \equiv 2 \mod 3 \end{cases}$$

ist.

c) Bestimmen Sie die Matrix $Q_f \in \mathrm{Mat}_3(\mathbb{F}_p)$ in den drei Fällen $p \equiv 1 \mod 3$ or $p \equiv 2 \mod 3$.

d) Man beweise die folgenden Aussagen:

i) wenn $p \equiv 1 \mod 3$ und $a^{\frac{p-1}{3}} = 1$ in $\mathbb{F}_p$, dann ist f das Produkt von 3 linearen Faktoren in $\mathbb{F}_p[x]$;

i') wenn $p \equiv 1 \mod 3$ und $a^{\frac{p-1}{3}} \neq 1$ in $\mathbb{F}_p$, dann ist f irreduzibel in $\mathbb{F}_p[x]$;

ii) wenn $p \equiv 2 \mod 3$, dann ist f das Produkt von einem linearem Faktor und von einem quadratischen irreduziblen Faktor in $\mathbb{F}_p[x]$.

Aufgabe 5.0.5. Sei $f \in \mathbb{F}_p[x]$ und seien $f_1, \ldots, f_r$ die irreduziblen Faktoren von f, deren Exponent in der Primfaktorzerlegung von f durch p nicht teilbar ist. Man zeige, dass $f = f_1 \cdots f_r \cdot \gcd(f, f')$ gilt.

Aufgabe 5.0.6. Es wäre gut, dass Sie lernen, wie Liste von Dingen zu handhaben; insbesondere Liste von Paaren (f, m), wobei f ein Polynom ist und m eine positive ganze Zahl ist. Die Zahl m im Paare (f, m) sollte als die Vielfachheit des Polynoms f betrachtet werden. Es sollte nützlich sein, auf `https://www.singular.uni-kl.de/Manual/4-2-0/sing_123.htm` zu gehen.

- Konstruieren Sie eine rekursive Funktion `PolyListePutzen`, die eine Liste von Paaren (f, m) als Input nimmt und eine Liste von Paaren als Output ergibt, in der alle Polynome f paarweise verschieden sind und die Vielfachheiten addiert werden.
- Konstruieren Sie eine Funktion `PolyListeVereinigung`, die zwei Listen von Paaren als Input nimmt und ihre Vereinigung als Output ergibt.

Aufgabe 5.0.7. Hier $\mathbb{K} = \mathbb{Q}$ oder $\mathbb{K} = \mathbb{F}_p$. Mithilfe einer wiederholten Verwendung des Satzes 4.5, konstruieren Sie eine Funktion `QuadratFreiZerlegung`, die ein monisches nicht konstantes Polynom $f \in \mathbb{K}[x]$ als Input nimmt, und die als Output eine Liste von Paaren (g_i, e_i) gibt, wobei jedes g_i ein monisches quadratfreies Polynom ist und $e_i \in \mathbb{N}^+$ mit $f = \prod_i g_i^{e_i}$.

Aufgabe 5.0.8. Mithilfe einer wiederholten Verwendung des Teiles 4 im Satz 4.3, konstruieren Sie eine Funktion `BerlekampFuerQuadratfrei`, die ein monisches quadratfreies Polynom $f \in \mathbb{F}_p[x]$ als Input nimmt und die die Liste der irreduziblen Faktoren von f als Output ergibt. (Da man annimmt, dass f quadratfrei ist, gibt es keine wiederholte Faktore.)

Testen Sie Ihre Funktion mit Ihrem quadratfreien Lieblingspolynom.

Aufgabe 5.0.9. Hier implementiert man in Singular einen Algorithmus für die Primfaktorzerlegung von Polynomen in $\mathbb{F}_p[x]$. Mithilfe der Betrachtungen in §4 und der vorherigen Aufgaben, konstruieren Sie eine Funktion `PrimfaktorZerl`, die ein monisches Polynom $f \in \mathbb{F}_p[x]$ als Input nimmt und eine Liste von Paaren (f_i, m_i) als Output gibt, wobei die f_i paarweise verschiedene monische Polynome sind und die m_i positive ganze Zahlen sind, sodass $f = \prod_i f_i^{m_i}$ gilt.

Aufgabe 5.0.10. Ist das Polynom $x^{36} + 300x^{23} - 2100x^{17} + 11x^{10} - 4x^5 + 2x^2 + 1 \in \mathbb{Q}[x]$ irreduzibel?

Literatur

[Ber67] E. R. Berlekamp, *Factoring polynomials over finite fields*, Bell System Tech. J. **46** (1967), 1853–1859.

[Chi09] Lindsay N. Childs, *A concrete introduction to higher algebra*, Third, Undergraduate Texts in Mathematics, Springer, New York, 2009.

[DGPS20] Wolfram Decker, Gert-Martin Greuel, Gerhard Pfister, and Hans Schönemann, SINGULAR *4-2-0 — A computer algebra system for polynomial computations*, 2020.

[GMT89] Patrizia Gianni, Victor Miller, and Barry Trager, *Decomposition of algebras*, Symbolic and algebraic computation (Rome, 1988), 1989, pp. 300–308.

[GP08] Gert-Martin Greuel and Gerhard Pfister, *A* **singular** *introduction to commutative algebra*, extended, Springer, Berlin, 2008. With contributions by Olaf Bachmann, Christoph Lossen and Hans Schönemann.

[Knu98] Donald E. Knuth, *The art of computer programming. Vol. 2*, Addison-Wesley, Reading, MA, 1998. Seminumerical algorithms, Third edition.

[Kob94] Neal Koblitz, *A course in number theory and cryptography*, Second, Graduate Texts in Mathematics, vol. 114, Springer-Verlag, New York, 1994.

[Koe06] Wolfram Koepf, *Computeralgebra*, Springer-Verlag Berlin Heidelberg, 2006. Eine algorithmisch orientierte Einführung.

[MSP11] Stefan Müller-Stach and Jens Piontkowski, *Elementare und algebraische Zahlentheorie*, Second, Vieweg + Teubner, Wiesbaden, 2011. Ein moderner Zugang zu klassischen Themen.