Maple-Praktikum für Lehramt 2017 - Blatt 6

Dieses Blatt wird in Kalenderwoche 22 (ab 29. Mai) testiert.

Aufgaben: 5

```
> restart;
```

In diesem Blatt wollen wir uns mit euklidischen Ringen beschäftigen. Dazu sollten Sie zunächst noch einmal einige grundlegenden Begriffe wiederholen.

ÜBUNG [01]:

Geben Sie folgende Definitionen an. Sie dürfen annehmen, dass alle auftauchenden Ring kommutativ sind.
1.) Integritätsbereich,
2.) euklidische Funktion und euklidischer Ring,
3.) Einheit,
4.) Teiler,
5.) Ideal,
6.) Hauptidealring.

Sehr bekannte Beispiele für euklidische Ringe sind die ganzen Zahlen $\mathbb{Z}$ und der Polynomring $K[x]$ für einen Körper K. Um diese soll es in der folgenden Aufgabe gehen. Dabei arbeiten Sie mit dem euklidischen Algorithmus, mit dem der größte gemeinsame Teiler zweier Ringelemente bestimmt werden kann.

Definition: Sei R ein euklidischer Ring. Für zwei Elemente $a, b \in R \setminus \{0\}$ heißt $d \in R$ *größter gemeinsamer Teiler* von a und b, geschrieben $d = ggT(a, b)$, falls d Teiler von a und b ist und von jedem gemeinsamen Teiler von a und b geteilt wird.

ÜBUNG [02]:

1.) Zeigen Sie, dass $\mathbb{Z}$ und $K[x]$ für einen Körper K euklidische Ringe sind, indem Sie jeweils die euklidische Funktion angeben.
2.) Schreiben Sie Prozeduren `eukAlgInt` und `eukAlgPoly`, die den ggT zweier gegebener Ringelemente mit dem euklidischen Algorithmus berechnen. Dabei soll `eukAlgInt` auf dem Ring $\mathbb{Z}$ der ganzen Zahlen und `eukAlgPoly` auf dem Ring $\mathbb{Q}[x]$ der Polynome über den rationalen Zahlen arbeiten. Sie dürfen dabei die Funktionen irem, rem, `iquo` und quo verwenden, nicht aber die in Maple enthaltenen Funktionen zur Bestimmung des ggT.
3.) Bestimmen Sie den größten gemeinsamen Teiler der ganzen Zahlen 12 und 18.

4.) Bestimmen Sie den größten gemeinsamen Teiler der ganzen Zahlen 3681405 und 190281.
5.) Bestimmen Sie den größten gemeinsamen Teiler der Polynome $-20\,x^6-18\,x^5-34\,x^4-23\,x^3-6\,x^2-24\,x+4$ und $8\,x^5+12\,x^4+36\,x^3+20\,x^2+28\,x-5$ im Polynomring $\mathbb{Q}[x]$.

Mit dem größten gemeinsamen Teiler lassen sich endlich erzeugte Ideale als Hauptideale schreiben, denn der ggT der Erzeuger des Ideals erzeugt bereits das gesamte Ideal. In der folgenden Übung soll dieser Satz verallgemeinert werden.

ÜBUNG [03]:

Zeigen Sie, dass jeder euklidische Ring ein Hauptidealring ist. Beachten Sie insbesondere, dass Sie für ein Ideal nicht unbedingt ein endliches Erzeugensystem kennen. *Hinweis: Sie können aus einem gegebenen Ideal $\{0\} \neq I \subseteq R$ ein minimales Element bezüglich der euklidischen Funktion wählen.*

In der linearen Algebra haben Sie Faktorräume eines Vektorraums kennengelernt. Eine ähnliche Konstruktion ist auch mit Ringen möglich. Dabei spielen Ideale eine wichtige Rolle.

Definition: Sei R ein kommutativer Ring und $I \subseteq R$ ein Ideal. Dann ist der *Faktorring* R/I definiert als $R/I := \{r+I | r \in R\}$.

ÜBUNG [04]:

Sei R ein euklidischer Ring und $I \subseteq R$ ein Ideal.
1.) Wie können Sie für ein $a \in R$ entscheiden, ob $a+I \in R/I$ eine Einheit ist und mit welchem Algorithmus können Sie gegebenenfalls das Inverse bestimmen?

In den folgenden Aufgabenteilen dürfen Sie nicht ^(-1) benutzen, aber die Funktion in Maple, die den Algorithmus aus 1.) durchführt.
2.) Sei $R := \mathbb{Z}$ und $I := (3^{115}-1)\mathbb{Z} \subseteq \mathbb{Z}$. Ist 14348906000 invertierbar in R/I und wenn ja, was ist das Inverse?
3.) Sei $R := \mathbb{Z}$ und $I := (3^{115}-1)\mathbb{Z} \subseteq \mathbb{Z}$. Ist 24650347049580675039961314533739438130747265123976009 69 invertierbar in R/I und wenn ja, was ist das Inverse?

4.) Sei $R := \mathbb{Q}[x]$, $f := 8x^5 + 12x^4 + 36x^3 + 20x^2 + 28x - 5 \in R$ und $I := f\mathbb{Q}[x] \subseteq \mathbb{Q}[x]$. Ist $1 + x + f^{42} + I$ invertierbar in R/I und wenn ja, was ist das Inverse?
5.) Unter welcher Bedingung an $n \in \mathbb{N}$ ist in $R = \mathbb{Z}/n\mathbb{Z}$ jedes Element ungleich 0 invertierbar? Erfüllt $n = 2^{2^7} + 1$ diese Bedingung?
6.) Unter welcher Bedingung an $f \in \mathbb{Q}[x]$ ist in $R = \mathbb{Q}[x]/f\mathbb{Q}[x]$ jedes Element ungleich 0 invertierbar? Erfüllt das $f = \frac{x^{37} - 1}{x - 1}$ (Das ist ein Polynom!) dieses Bedingung?

In der nächsten Übung soll es um den chinesischen Restsatz gehen. Er kann benutzt werden, um Systeme von Kongruenzen zu lösen.

Satz (chinesischer Restsatz): Sei R ein euklidischer Ring und seien $m_1, ..., m_n \in R \setminus \{0\}$ paarweise teilerfremd. Für Element $c_1, ..., c_n \in R$ gibt es ein Element $c \in R$, so dass simultan die Kongruenzen $c \equiv c_i \bmod m_i$ für $i = 1, ...n$ gelten.

ÜBUNG [05]:

Verwende die Bezeichnungen aus obigem Satz. Sei weiter $P := \prod_{i=1}^{n} m_i$ sowie $P_i := P/m_i$ und $x_i \in R$ mit $x_i P_i \equiv 1 \bmod m_i$ für $i = 1, ..., n$.

1.) Warum existieren solche x_i immer und warum erfüllt $c := \sum_{i=1}^{n} c_i x_i P_i$ die gewünschten Kongruenzen? Wie können die x_i aus $m_1, ..., m_n$ berechnet werden? Warum ist c eindeutig modulo P?
2.) Schreiben Sie eine Prozedur für den Fall $R = \mathbb{Z}$ in Maple, die zwei Listen $[m_1, ..., m_n]$ (paarweise teilerfremd) und $[c_1, ..., c_n]$ als Eingabe erhält und eine Lösung $c \in \mathbb{Z}$ der simultanen Kongruenzen $c \equiv c_i \bmod m_i$ für $i = 1, ..., n$ zurückgibt. Schreiben Sie Ihre Funktion so, dass die Ausgabe beragsmäßig möglichst klein ist, also zwischen $-\frac{P+1}{2}$ und $\frac{P+1}{2}$ liegt. Was ist das kleinste $c \in \mathbb{N}$, so dass für $i = 1, ..., 100$ gilt $c \equiv i \bmod p_i$, wobei p_i die i-te Primzahl ist?
3.) Bestimmen Sie ein $c \in \mathbb{Z}$ mit $c \equiv 74540892843699 \bmod 800187484459$, $c \equiv 437395175522 \bmod 22424170465$ und $c \equiv 21501059632462 \bmod 427552056869$.