Universität des Saarlandes
Fachbereich 9, Mathematik
Prof. Dr. R. Berger

4. Übung zur Linearen Algebra I, WS 1998/99

Zur nächsten Aufgabe:

Euklid *(um 300 v.u.Z) versuchte in seinem Haupwerk "Elemente" das gesamte mathematische Wissen seiner Zeit darzustellen und dabei von Axiomen auszugehen. Seine Bücher blieben bis ins 19. Jahrhundert ein Standardwerk. Auch gab er die erste Darstellung einer Primzahltheorie. So bewies er bereits, daß es unendlich viele Primzahlen gibt (vgl. Aufgabe 13 c)).*
Kettenbrüche, auch unendliche Kettenbrüche, wurden bereits im Altertum bei den 'alten Griechen' betrachtet. Die Pythagoräer konnten sogar in einigen Fällen eine 'Lösung' angeben.
Die erste bekannte Anwendung der Fibonaccizahlen ist eine "worst-case"-Analyse des euklidischen Algorithmus aus dem Jahre 1845 (s. Teil d)).

Aufgabe 19: *(3+1+2+4=10 Punkte)*

a) Bestimme mit Hilfe des **euklidischen Algorithmus** den größten gemeinsamen Teiler (kurz 'ggT') von 301 und 210, sowie von -1553 und 2701.

b) Ist der ggT eindeutig bestimmt?

c) Durch den ersten Schritt des euklidischen Algorithmus erhält man für zwei ganze Zahlen n_1, n_2 eine Darstellung $n_1 = q_1 \cdot n_2 + n_3$. Umgeformt ergibt dies $\frac{n_1}{n_2} = q_1 + \frac{n_3}{n_2} = q_1 + \frac{1}{\frac{n_2}{n_3}}$. Analog ergibt sich für n_2 und n_3 die Darstellung $n_2 = q_2 \cdot n_3 + n_4$. Umgeformt und eingesetzt erhalten wir den Bruch

$$\frac{n_1}{n_2} = q_1 + \frac{1}{q_2 + \frac{n_4}{n_3}}$$

Da der euklidische Algorithmus terminiert, endet dieser *Kettenbruch* irgendwann.

Also verhilft der euklidische Algorithmus zu einer Darstellung der Brüche als Kettenbrüche. Schreibe die beiden Brüche $\frac{301}{210}$ und $\frac{2701}{1553}$ als Kettenbrüche.

d) Seien $a, b \in \mathbb{N}$ und $k \geq 1$ so beschaffen, daß der euklidische Algorithmus genau k Schritte bis zu seiner Terminierung braucht. Zeige, daß die kleinsten Zahlen a und b, welche dieser Bedingung genügen, $a = F_{k+1}$ und $b = F_k$ sind, wobei F_{k+1} und F_k Fibonaccizahlen sind.

Hinweis: *Benutze Teil c)*

Eine Beschreibung des euklidischen Algorithmus findet man wohl in jedem Buch zum Thema "Einführung in die Algebra" oder "Computeralgebra". Die nachfolgende Liste ist eine kleine Auswahl aus den in der Fachbereichsbibliothek vorhandenen Werken:

R. Allenby: *Rings, Fields and Groups*
M. Mignotte: *Mathematics for Computer Algebra*
Scheja/Storch: *Lehrbuch der Algebra*
J. Wolfart: *Einführung in die Zahlentheorie und Algebra*

Aufgabe 20: *(1+6+1+2=10 Punkte)*

Sei X eine nichtleere Menge.

a) Die Potenzmenge $\mathcal{P}(X)$ mit der Vereinigung als 'Addition' und dem Durchschnitt als 'Multiplikation' ist kein Ring. Warum nicht?

b) Es ist aber möglich, $\mathcal{P}(X)$ mit einer Ringstruktur zu versehen, wenn man die 'Addition' in a) durch die **symmetrische Differenz**

$$A + B := (A \cup B) \setminus (A \cap B) = (A \setminus B) \cup (B \setminus A) \qquad \forall\, A, B \in \mathcal{P}(X)$$

ersetzt. Der so gebildete Ring heißt der (volle) **Mengenring** von X.

Zeige, daß dieser Ring ein kommutativer unitärer Ring mit Charakteristik 2 ist.

(*Der Nachweis der Assoziativität bei der Addition ist aufwendig. Du darfst ihn durch Mengenschnittbilder* (Venn-Diagramme) *führen.*)

c) Wie viele Elemente hat $\mathcal{P}(X)$, falls X eine endliche Menge ist?

d) Wie sehen die Verknüpfungstafeln der Addition und Multiplikation in $(\mathcal{P}(X), +, \cap)$ für $|X| = 1$ aus?

Wer Probleme mit den Mengenoperationen hat, kann etwa in
***Lamprecht:** Einführung in die Algebra*
***Dallmann/Elster:** Einführung in die höhere Mathematik*
nachschlagen.

Aufgabe 21:*(4+4+2+2=12 Punkte)*

Seien R und S unitäre kommutative Ringe.

a) Sei $\mathfrak{a}$ eine Teilmenge von R. Zeige, daß $\mathfrak{a}$ genau dann ein Ideal von R ist, wenn $\mathfrak{a}$ den folgenden Bedingungen genügt:

(i) $\mathfrak{a} \neq \emptyset$
(ii) $a, b \in \mathfrak{a} \Rightarrow a + b \in \mathfrak{a}$
(iii) $r \in R, a \in \mathfrak{a} \Rightarrow ra \in \mathfrak{a}$

b) Seien $\mathfrak{a}$ und $\mathfrak{b}$ Ideale von R. Weise nach, daß $\mathfrak{a} + \mathfrak{b} := \{a + b | a \in \mathfrak{a} \text{ und } b \in \mathfrak{b}\}$ ein Ideal von R ist. Zeige, daß es sogar das kleinste Ideal ist, welches $\mathfrak{a}$ und $\mathfrak{b}$ enthält.

c) Sei $\varphi : R \to S$ ein Ringhomomorphismus und $a \in R$ dergestalt, daß $\varphi(a)$ kein Nullteiler in S ist. Zeige, daß dann $\varphi(1_R) = 1_S$ gilt, wobei 1_R die Eins in R und 1_S die Eins in S ist.

d) Gibt es in Teil c) ein solches Ringelement $a \in R$ immer,

(i) wenn S nullteilerfrei ist?
(ii) oder wenn φ surjektiv ist?

Zur nächsten Aufgabe:

Am Montag wird von 16-18 Uhr jemand im Rechnerraum sitzen, an den Du Dich bei Fragen zu der nachfolgenden Mapleaufgabe wenden kannst. Wenn Du irgendwann in den Rechnerraum möchtest und die Tür verschlossen ist, kannst Du entweder in der Mathematikbibliothek oder bei Holger die Türöffnung begehren.

Aufgabe 22:*(4+2+2=8 Punkte)*

a) Schreibe in Maple ein Programm zur Berechung des größten gemeinsamen Teilers zweier ganzen Zahlen, welches auf dem euklidischen Algorithmus basiert.

b) Modifiziere Dein Programm so, daß jeder Schritt des euklidischen Algorithmus ausgegeben wird. Überprüfe Deine Berechnungen in Aufgabe 19 a).

c) Als Euklid bewies, daß es unendlich viele Primzahlen gibt, bildete er das Produkt aller Primzahlen und addierte eins (vgl. Scheja/Storch, Band I, Satz 10.8). Teste mit Maple, ob $2 + 1, 2 \cdot 3 + 1, 2 \cdot 3 \cdot 5 + 1, \cdots$ eine Primzahl ist. Es reicht, die ersten zehn Zahlen zu überprüfen.

Hinweis: *Maple besitzt die Funktion* `isprime`*, welche angibt ob eine Zahl prim ist, sowie eine Funktion* `ifactor`*, welche eine Zahl in Primfaktoren zerlegt.*

Abgabe der Übungen ist am Freitag, 27.11.1998 vor der Vorlesung!

Wer mit den Aufgaben oder dem Vorlesungsstoff absolut nicht klar kommt und eine Erklärung haben möchte, soll **fragen**! Zusätzlich noch einmal die Aufforderung, die jeden Mittwoch um 16^{15} Uhr stattfindende **Fragestunde** zu besuchen!!