Höhere Mathematik I, WS2013/14
M. Hortmann

Blatt 4

bitte heften Sie dieses Blatt vor Ihre Lösungen

Namen							**Gruppennr.**	**Tutor**
1a	1b	1c	2	3	4a	b	**Summe**	**bearbeitet**
1	1	1	1	1	1	1	5 Punkte=100%	

Aufgabe 1

Sei $(R,+,\cdot)$ ein Ring[1] und $a \in R$ ein beliebiges Element.
Das neutrale Element der Addition in R bezeichnen wir wie üblich mit 0.

a) Folgern Sie aus den definierenden Eigenschaften eines Rings daß $a \cdot 0 = 0 \cdot a = 0$.
b) Benutzen Sie dies, um zu zeigen, daß für jedes Element $b \in R$ gilt: $-(ab) = a(-b) = (-a)b$.

c) In diesem Aufgabenteil sei zusätzlich vorausgesetzt, daß R ein kommutativer Ring mit 1 ist. Außerdem sei auf R eine „totale Ordnung“ definiert, die wir wie üblich mit ≤ bezeichnen. Für eine Ordnung (auf R) gilt definitionsgemäß:

$\forall a \in R: a \leqslant a$
$\forall a, b \in R: a \leqslant b$ und $b \leqslant a \;\rightarrow\; a = b$
$\forall a, b, c \in R: a \leqslant b$ und $b \leqslant c \;\rightarrow\; a \leqslant c$

Bei einer totalen Ordnung gilt zusätzlich

$\forall a, b \in R: a \leqslant b$ oder $b \leqslant a$

Die auf R gegebene totale Ordnung sei mit den Ringoperationen folgendermaßen verträglich:

$\forall a, b, c \in R: a \leqslant b \;\rightarrow\; a + c \leqslant b + c$
$\forall a, b \in \mathbb{R}: 0 \leqslant a$ und $0 \leqslant b \rightarrow 0 \leqslant a \cdot b$

1 Es wird in 1a,b) nicht vorausgesetzt, daß die Multiplikation in R kommutativ sei oder ein neutrales Element besitze.

Unter diesen Voraussetzungen nennt man R einen „geordneten Ring“.
Beispielsweise bilden die ganzen, die rationalen und die reellen Zahlen einen geordneten Ring.

Man zeige – ausschließlich unter Benutzung der definierenden Eigenschaften eines geordneten Rings – daß für alle $a \in R$ gilt: $0 \leqslant a \cdot a$. [2]

Aufgabe 2

Die reellen Zahlen bilden mit Addition und Multiplikation einen Körper. Die übliche Ordnung $\leq$ auf macht $\mathbb{R}$ zu einem „geordneten Körper [3]“. Man zeigt leicht, daß aus $a, b \in \mathbb{R}, 0 \leqslant a, b$ und $a^2 \leqslant b^2$ folgt, daß $a \leqslant b$.

Man bilde rekursiv folgende Folge rationaler Zahlen:

$$x_0 := 1 \ , \ x_{n+1} := \begin{cases} x_n + 1/2^n & \text{falls} \quad \left(x_n + 1/2^n\right)^2 \leqslant 2 \\ x_n & \text{sonst} \end{cases} .$$

Bei dieser Konstruktion ergibt sich eine monoton wachsende Folge, wobei die Differenzen der Folgenglieder (locker gesprochen) beliebig klein werden, und die Quadrate der Folgenglieder schließlich beliebig nah an 2 liegen.

Berechnen Sie die Werte $x_1, \ldots, x_{12}$ sowohl in Ihrer Darstellung als Dezimalbrüche $1.d_1 d_2 \ldots d_k$ wie auch als Dualbrüche $1.b_1 b_2 \ldots b_n$. Beispielsweise erhalte ich:
$x_{10} = 1.4140625$ als Dezimalbruch und als Dualbruch $x_{10} = 1.0110101$.
Beachten Sie, wie die Fallunterscheidung in der obigen Rekursion in der Dualbruchentwicklung gespiegelt wird.

Aufgabe 3

Sei $(R, +, \cdot)$ ein Ring mit 1, wobei $1 \neq 0$ [4].
Finden Sie eine Matrix $A \in M_3(R)$, für die gilt: $A^3 = 0$, $A^2 \neq 0$ [5].

Aufgabe 4

a) Benutzen Sie den Euklidischen Algorithmus, um den Bruch $\frac{146839691}{8598823}$ zu kürzen.

b) Erinnern Sie sich an die Aufgabe 5 von Blatt 2. Dort wurde zur Primzahl p=2147483659 der Körper $\mathbb{Z}_p$ mit der Addition und Multiplikation „modulo p“ betrachtet, und durch reines Durchprobieren der Elemente von $\mathbb{Z}_p$ das zu 135 multiplikativ Inverse gefunden.

Finden Sie nun dieses Inverse durch folgende Rechnung:

---

2 d.h. Quadrate in einem geordneten Ring sind nie negativ. Weil $1 \cdot 1 = 1$ folgt damit auch $0 \leq 1$.
3 Ein Körper ist ja ein spezieller Ring. Ist dieser Ring geordnet, so nennt man auch den Körper geordnet.
4 Hier bezeichnet 0 das neutrale Element der Addition in R .
5 Hier bezeichnet 0 die Nullmatrix.

Gehen Sie vor wie beim Euklidischen Algorithmus zur Berechnung von ggT(p,135):
Da p eine Primzahl ist, muß dieser ggT gleich 1 sein. Beginnen Sie also mit $r_0 := p$, $r_1 := 135$ und berechnen rekursiv $r_{k+1} := r_{k-1} \% r_k$, indem Sie die Division mit Rest $r_{k-1} = q_k r_k + r_{k+1}$ durchführen. Irgendwann erreichen Sie $r_n = 1$ [6] .

Setzen Sie nun schon zu Beginn $s_0 := 0$ und $s_1 = 1$ und berechnen parallel zu den Resten r_{k+1} nach jeder der obigen Divisionen weitere Werte $s_{k+1} := s_{k-1} - q_k s_k$.

Falls man gleichzeitig auch noch $t_0 := 1$, $t_1 := 0$, $t_{k+1} := t_{k-1} - q_k t_k$ berechnen würde, so ließe sich durch Induktion leicht zeigen, daß immer gilt $t_k r_0 + s_k r_1 = r_k$, also beim letzten Schritt

$$t_n p + s_n 135 = 1$$

Daraus ergibt sich sofort, daß s_n „modulo p“ , also $s_n \% p$ das Inverse von 135 im Körper $\mathbb{Z}_p$ ist. Man sieht auch, daß man für letzteres Ergebnis die zweite Folge (t_k) gar nicht benötigt und sich daher ihre Berechnung sparen kann.

Berechnen Sie also die Folge (s_k), und machen Sie die Probe, daß Ihre Rechnung das Ergebnis $\left(\left(s_n \% p\right) \cdot 135\right) \% p = 1$ liefert.

Sinn der Übung: mit dieser Methode, dem sog. „Erweiterten Euklidischen Algorithmus“ können Sie die Inversen beliebiger Elemente im Körper $\mathbb{Z}_p$ auch bei sehr großen Werten von p schnell berechnen!

6 In diesem Beispiel ist dies bei n=5 der Fall.