Mathematische Grundlagen der Informatik II, SS 2002
Aufgabenblatt 2

Aufgabe 1. Rechnen mit komplexen Zahlen

a) Stelle $\frac{2+4i}{5+i}$ in der Form $a+bi$ mit $a,b\in\mathbb{Q}$ dar.

b) Berechne $\left(\sqrt{\sqrt{2}+1} \;+\; \sqrt{\sqrt{2}-1}\; i\right)^4$. Schließe aus dem Ergebnis, welchen Winkel die komplexe Zahl $\sqrt{\sqrt{2}+1} \;+\; \sqrt{\sqrt{2}-1}\; i$ mit der reellen Achse bildet.

c) Welchen Winkel muß eine komplexe Zahl *z* mit der x-Achse bilden, wenn $z^3=-1$ gelten soll? Was kann man über $|z|$ sagen? Ausgehend von diesen Vorüberlegungen finde eine solche Zahl!

d) Berechne das Produkt $(a+bi)\cdot(c+di)$ in $\mathbb{C}$ und das Matrizenprodukt $\begin{pmatrix} a & -b \\ b & a \end{pmatrix}\begin{pmatrix} c & -d \\ d & c \end{pmatrix}$ in $M_2(\mathbb{R})$. Was fällt auf?

Aufgabe 2

Man zeige, dass die Vektoren $\begin{pmatrix}1\\3\\2\end{pmatrix}, \begin{pmatrix}4\\3\\1\end{pmatrix}, \begin{pmatrix}2\\3\\0\end{pmatrix} \in K^3$ linear unabhängig sind, wenn $K=\mathbb{R}$, dagegen linear abhängig, wenn $K=\mathbb{Z}_5$.

Aufgabe 3

Sei $U\subset {\mathbb{Z}_5}^3$ der von $\begin{pmatrix}1\\2\\1\end{pmatrix}, \begin{pmatrix}3\\1\\1\end{pmatrix}$ erzeugte Unterraum (d.h. $U=\left\{\lambda\begin{pmatrix}1\\2\\1\end{pmatrix}+\mu\begin{pmatrix}3\\1\\1\end{pmatrix} \;\middle|\; \lambda,\mu\in K\right\}$)

Gilt $\begin{pmatrix}1\\2\\0\end{pmatrix}\in U$? Man gebe einen Vektor in ${\mathbb{Z}_5}^3$ an, der nicht in *U* liegt.

Aufgabe 4

Seien $U_1,U_2\subset {\mathbb{Z}_5}^3$ die von $\begin{pmatrix}1\\2\\1\end{pmatrix}, \begin{pmatrix}3\\1\\1\end{pmatrix}$ bzw. $\begin{pmatrix}2\\3\\4\end{pmatrix}, \begin{pmatrix}3\\1\\2\end{pmatrix}$ erzeugten Unterräume. Man finde einen Vektor $v\in U_1\cap U_2,\ v\neq 0$.

Freiwillige Zusatzaufgabe (Ergänzung des Vorlesungsstoffes)

Euklidischer Algorithmus

In einem Ring *R* heißt ein Element *a* Teiler eines Elementes *b*, wenn es ein Element $q \in R$ gibt mit $qa=b$. Ist *b* Teiler von *a*, so sagt man auch „*b* teilt *a*“ und schreibt $b \mid a$. Ein Element $c \in R$ heißt „größter gemeinsamer Teiler von *a* und *b*“, wenn für jeden Teiler *d* von *a* und *b* gilt: $d|c$. Man nennt einen größten gemeinsamen Teiler von *a*, *b* ggT(*a*,*b*). In der Schule hat man i.a. gelernt, den größten gemeinsamen Teiler zweier Element von $\mathbb{Z}$ zu bestimmen, oft mittels der Primfaktorzerlegung von *a*,*b*. Diese Aufgabe beschäftigt sich mit einem effektiven Verfahren, den größten gemeinsamen Teiler in sog. „Euklidischen Ringen“ zu bestimmen, dazu gehören $\mathbb{Z}$ und Polynomringe mit Koeffizienten in einem Körper; das Verfahren, der „Euklidische Algorithmus“ kommt ohne Primfaktorzerlegung aus und funktioniert auch für sehr große Zahlen, für die man z.B. die Primfaktorzerlegung gar nicht mehr finden könnte. Man gewinnt gleichzeitig eine Methode, das multiplikativ Inverse eines Elements in $\mathbb{Z}_p$ zu bestimmen!

Sei *R* ein kommutativer Ring.
Es gebe eine Abbildung $d : R \to \mathbb{N}_0 := \mathbb{N} \cup \{0\}$ mit folgenden Eigenschaften:

$d(x) = 0 \Leftrightarrow x = 0$

$\forall a,b \in R, b \neq 0 \; \exists q,r \in R : \; a = qb + r$ (Division mit Rest)

(Die Abbildung *d* soll die „Größe“ eines Elements messen, im Beispiel $R = \mathbb{Z}$ wählt man $d(x) := |x|$).

Unter den obigen Bedingungen heißt *R* ein **Euklidischer Ring**. Offenbar ist z.B. $\mathbb{Z}$ ein Euklidischer Ring. Ist *K* ein Körper, so kann man für die Abbildung *d* den Grad eines Polynoms wählen. Auf der Schule hat man i.a. gelernt, die Polynomdivision mit Rest durchzuführen, so dass auch *K*[*X*] ein Euklidischer Ring ist.

Sei nun *R* ein Euklidischer Ring .
Wir wählen $a,b \in R,\ a,b \neq 0$ und geben einen Algorithmus, der uns ggT(*a*,*b*) liefert und darüber $x, y \in R$, so dass $xa + yb = \text{ggT}(a,b)$. Wir werden anschließend sehen, wozu diese Gleichung nützlich ist.

Sind also $a,b \in R,\ a,b \neq 0$, so setze man $r_0 := a,\ r_1 := b,\ s_0 := 1,\ s_1 := 0,\ t_0 := 0,\ t_1 := 1$ und bestimme rekursiv die folgenden Größen:

$r_{n-1} := q_n r_n + r_{n+1}$, d.h. man führe mit r_{n-1}, r_n die obige „Division mit Rest“ aus und nenne den „Rest“ r_{n+1}.

$s_{n+1} := s_{n-1} - q_n s_n$ (q_n ist hier der in der vorigen Zeile gewonnen Quotient)

$t_{n+1} := t_{n-1} - q_n t_n$

Man breche das Verfahren ab, sobald $r_{n+1} = 0$ wird. Dies muß zwangsläufig geschehen, da ja $d(r_n)$ mit jedem Durchlauf der obigen Schleife kleiner wird.

Es ist nicht schwer, durch Induktion zu zeigen, dass alle $r_k, 2 \le k \le n$ Teiler von *a,b* sind und dass r_n (also der letzte *r*-Term $\neq 0$) der größte gemeinsame Teiler von *a,b* ist. (Dazu benötigt man natürlich nicht die s_k, t_k.)

a) Man zeige durch Induktion: $r_k = s_k a + t_k b$ für $0 \le k \le n$

Für *k=n* hat man damit die Aussage: ggT(*a,b)*= $s_n a + t_n b$, d.h. man kann den größten gemeinsamen Teiler als „Linearkombination“ von *a,b* darstellen.

b) Man berechne mit Hilfe des Euklidischen Algorithmus den größten gemeinsamen Teiler von 1404081 und 1117597 und löse gleichzeitig die Gleichung

ggT(1404081, 1117597) = $x \cdot 1404081 + y \cdot 1117597$ mit $x, y \in \mathbb{Z}$.

c) Ist *p* eine Primzahl, so gilt offenbar für jedes $a \in \mathbb{N}$, $a < p$: ggT(*a,p*) =1. Da man nun mit Hilfe des Euklidischen Algorithmus die Gleichung $xp + ya = 1$ lösen kann, muß im Körper $\mathbb{Z}_p$ gelten: *ya*=1! Man kann also in diesem Körper das Inverse von *a* bestimmen!

$p = 7564981$ ist eine Primzahl. Man berechne das Inverse von 21 in $\mathbb{Z}_p$!