Mathematik I, Logik und Algebra, WS2010/11
M. Hortmann

Blatt 11 (letztes Übungsblatt)

bitte heften Sie dieses Blatt vor Ihre Lösungen

Namen										**Gruppe**	**Tutor**
1a	b	2a	b	c	d	e	f	3a	b	**Summe**	**bearbeitet**
1	1	1	1	1	1	1	1	1	1	8 Punkte=100%	

Ist K ein Körper und sind f, g Polynome in $K[X]$, g nicht das Nullpolynom, so können wir mit Hilfe Divisionsalgorithmus für Polynome einen Quotienten $q \in K[X]$ und einen Rest $r \in K[X]$ finden, so daß $f = q\,g + r$, wobei grad $r <$ grad g. Dies schließt den Fall ein, daß r das Nullpolynom ist, die Polynom-Division also aufgeht.

Man kann jetzt mit demselben Verfahren wie in $\mathbb{Z}$ durch wiederholte Division mit Rest den größten gemeinsamen Teiler zweier Polynome in $K[X]$ bestimmen (Euklidischer Algorithmus), oder zu zwei Polynomen $f, g \in K[X]$ weitere Polynome $s, t \in K[X]$ bestimmen, so daß $\mathrm{ggT}(f, g) = s\,f + t\,g$ (Erweiterter Euklidischer Algorithmus)

Aufgabe 1

Das Polynom $f = X^5 + 2X + 1 \in \mathbb{Z}_3[X]$ ist irreduzibel.
Sei $g = X^6 + 2X^5 + 2X^2 + 1$ ein weiteres Polynom in $\mathbb{Z}_3[X]$.

a) Rechnen Sie mit Hilfe des Euklidischen Algorithmus nach, daß ggT(f,g)=1.
b) Finden Sie mit dem Erweiterten Euklidischen Algorithmus Polynome $s, t \in \mathbb{Z}_3[X]$ mit $s\,f + t\,g = 1$. (Probe!)

Aufgabe 2

Auf $R := \mathbb{Z} \times \mathbb{Z}$ erhält man folgendermaßen die Struktur eines Integritätsrings (Ring mit 1, kommutativ, nullteilerfrei): Die Addition geschieht komponentenweise in $\mathbb{Z}$, die Multiplikation wird folgendermaßen definiert: $(a, b) \cdot (c, d) := (ac - bd, ad + bc)$.

a) Man zeige: in R bildet die Teilmenge $Z := \{(a, 0) \mid a \in \mathbb{Z}\}$ einen Unterring.
b) Die Abbildung $\mathbb{Z} \to Z$, $a \mapsto (a, 0)$ ist ein injektiver Ringhomomorphismus.

Wegen b) kann man in R die Elemente von Z mit Elementen von $\mathbb{Z}$ identifizieren. Wir schreiben also kurz a für das Element $(a,0)$, z.B. 0=(0,0) und 1=(1,0) und -1=(-1,0) .

c) Man finde in R zwei Elemente, deren Produkt mit sich selbst gleich -1 ist.

d) Für $z=(a,b)\in R$ setze man $N(z):=a^2+b^2$ und zeige für $z, w\in R$: $N(z\,w)=N(z)\,N(w)$.

e) Man finde Elemente $z, w\in R$ mit $zw = 2$ und $N(z)\neq 1$ und $N(w)\neq 1$.

f) Man zeige, daß sich nicht entsprechend zwei Elemente mit zw=3 finden lassen.

Aufgabe 3

Sei $n=p\cdot q\in\mathbb{N}$, wobei $p,q>1$ und ggT(p,q)=1.

Die Abbildung $\Phi:\mathbb{Z}_n\to\mathbb{Z}_p\times\mathbb{Z}_q$ mit $k\mapsto(k\,\%\,p,\,k\,\%\,q)$ ist ein Ringhomomorphismus.

Mit Hilfe des Erweiterten Euklidischen Algorithmus findet man $x, y\in\mathbb{Z}$ mit $xp+yq=1$.

Setzt man jetzt v=xp und u=yq, so ergibt sich daraus u%q=0, u%p=1 , v%q=1 , v%p=0.

Es ist also $\Phi(u)=(1,0)$ und $\Phi(v)=(0,1)$

Fassen wir jetzt $a\in\mathbb{Z}_p$ und $b\in\mathbb{Z}_q$ als natürliche Zahlen auf mit $0\leqslant a<p$ und $0\leqslant b<q$,
so ergibt sich $\Phi(a\cdot u+b\cdot v)=(a,b)$, und wir haben somit ein Urbild für ein beliebiges Element von $\mathbb{Z}_p\times\mathbb{Z}_q$ gefunden. Der Ringhomomorphismus Φ ist also surjektiv. Da $\mathbb{Z}_n$ und $\mathbb{Z}_p\times\mathbb{Z}_q$ beide dieselbe Elementezahl besitzen, ist er sogar bijektiv.

Man setze nun p=1061 und q=1543, so daß n=1637123.

a) Man bestimme nach obiger Methode $u\in\mathbb{Z}_n$ mit $\Phi(u)=(1,0)$ und $v\in\mathbb{Z}_n$ mit $\Phi(v)=(0,1)$
b) Man bestimme nach obiger Methode ein Element $x\in\mathbb{Z}_n$ mit $\Phi(x)=(37,98)$.