Übungsblatt 2 - Algebra 1 - Jovan Petrov - üG3

Aufgabe 1

(a) $p(x) = (x^2+1) \in \mathbb{Z}/3\mathbb{Z}[x]$ ist irreduzibel.

Beweis: $x^2+1 = (ax+b)(cx+d)$ für $a,b,c,d \in \mathbb{Z}/3\mathbb{Z}$

$\Leftrightarrow x = ba^{-1}$ und $x = dc^{-1}$ Nullstellen von p in $\mathbb{Z}/3\mathbb{Z}$

Also ist (x^2+1) g.d. reduzibel, wenn es Nullstellen im Körper $\mathbb{Z}/3\mathbb{Z}$ hat. Wir überprüfen alle Elemente von $\mathbb{Z}/3\mathbb{Z}$ als potenzielle Nullstellen von x^2+1

x	$[0]$	$[1]$	$[2]$
x^2+1	$[1]$	$[2]$	$[1]$

Da also x^2+1 keine Nullstellen in $\mathbb{Z}/3\mathbb{Z}$ hat ist x^2+1 in $(\mathbb{Z}/3\mathbb{Z})[x]$ irreduzibel.

Wir betrachten $(\mathbb{Z}/3\mathbb{Z})[x]/(x^2+1)(\mathbb{Z}/3\mathbb{Z})[x]$

Offensichtlich sind die Verknüpfungen $+, \cdot$ wohldefiniert und $+$ erfüllt die Körperaxiome.

Sei $p \in (\mathbb{Z}/3\mathbb{Z})[x]$ mit $p \notin [0]_{\sim(x^2+1)}$. Dann existieren (nach dem Euklidischen Alg.) Polynome $m(x), n(x)[x] \in (\mathbb{Z}/3\mathbb{Z})[x]$ mit

$$1 \overset{(x^2+1) \text{ irred.}}{=} ggT(p(x),(x^2+1)) = m(x)p(x) + n(x)(x^2+1)$$

$$[1]_{\sim(x^2+1)} = [m(x)p(x) + n(x)(x^2+1)]_{\sim(x^2+1)} = [m(x)]_{\sim x^2+1}[p(x)]_{\sim x^2+1} + [n(x)(x^2+1)]_{\sim x^2+1}$$

$$= [m(x)][p(x)]$$

Also hat jede Äquivalenzklasse $\neq [0]$ ein inverses Element bez. der Multiplikation. $\Rightarrow (\mathbb{Z}/3\mathbb{Z})[x]/(x^2+1)$ - Körper.

Jedes Element des Körpers ist aus der Form $[ax+b]$ mit $a,b \in \mathbb{Z}/3\mathbb{Z}$. Da es jeweils 3 Möglichkeiten für a und b gibt, hat der Körper genau $3 \cdot 3 = 9$ Elemente.

(b) Wie wir in (a) gesehen haben, ist x^2+1 in $\mathbb{Z}/p\mathbb{Z}[x]$, p-Primzahl, g.d. irreduzibel wenn es in $\mathbb{Z}/p\mathbb{Z}$ keine Nullstellen hat.

Für eine Primzahl p überprüfen wir ob hier irgendein Element von $\mathbb{Z}/p\mathbb{Z}$ x^2+1 eine Nullstelle hat.

Wir können hier ein $x \in \mathbb{Z}$ feststellen

$$[-x]^2_{\nu_p} + 1 = [-1]^2[x]^2 + 1 = [x]^2 + 1 .$$

Es genügt somit nur die ersten $\frac{p-1}{2}$ Elemente von $\mathbb{Z}/p\mathbb{Z}$ zu überprüfen.

- $p = 5$:

x	0	1	2
x^2+1	1	2	⓪

$\Rightarrow x^2+1$ hat eine Nullstelle $\Rightarrow x^2+1$ - reduzibel

- $p = 7$:

x	0	1	2	3
x^2+1	1	2	5	3

$\Rightarrow x^2+1$ hat keine N.-stelle $\Rightarrow x^2+1$ - irreduzibel

- $p = 11$:

x	0	1	2	3	4	5
x^2+1	1	2	5	10	6	5

$\Rightarrow x^2+1$ - keine N.-stelle $\Rightarrow$ irreduzibel

- $p = 13$:

x	0	1	2	3	4	5	6
x^2+1	1	2	5	10	4	⓪	11

$\Rightarrow x^2+1$ - hat N.-stelle $\Rightarrow$ reduzibel

- $p = 17$:

x	0	1	2	3	4	5	6	7	8
x^2+1	1	2	5	10	⓪	9	3	16	14

$\Rightarrow x^2+1$ - hat N.-stelle $\Rightarrow$ reduzibel