WS 2011/12

Zentralübung zur Vorlesung Diskrete Strukturen (Prof. Mayr)

Dr. Werner Meixner

Fakultät für Informatik
TU München

http://www14.in.tum.de/lehre/2011WS/ds/uebung/

7. Dezember 2011

ZÜ VIII

Übersicht:

1. Übungsbetrieb
2. Tipps: Hin.Ti's für HA Blatt 8
3. Thema: Restklassenringe:
   Homomorphismen, Sätze der Vorlesung
4. Vorbereitung: auf TA Blatt 8:
   Reste bei Polynomdivision (VA1)
   Rechnen in Restklassenringen (VA2)
   Irreduzibilität (VA3)

1. Übungsbetrieb

Fragen?

Am Donnerstag, den 8. Dezember finden keine Übungen statt wegen des dies academicus.

Die betroffenen Teilnehmer gehen bitte als Gast in eine Gruppe ihrer Wahl.
Dies gilt bekanntlich im ganzen Semester immer dann, wenn Übungsgruppentermine ausfallen.

2. Tipps zu HA Blatt 8

weiterer Hinweis ad HA 3.2:

Beachten Sie, dass n eine Primzahl sein muss.

Allgemeiner Hinweis:

Ein Nullteilerfreier Ring ist nicht notwendigerweise ein Körper

Erst die allgemeine Existenz von multiplikativen Inversen macht einen Ring zum Körper!!

3. Thema: Restklassenringe

3.1 Isomorphismus

Ein Isomorphismus vergleicht Bereiche.

Beachten Sie die Isomorphie zwischen $\langle \mathbb{Z}_3[x]/(g), +, \cdot \rangle$ und $\langle \mathbb{Z}_3[x]_{\text{grad}(g)}, +_g, \cdot_g \rangle$, die für alle $g \in R$ durch die Abbildung $[f]_g \rightarrow Rem_g(f)$ gegeben ist.

Wir schreiben gelegentlich $p \in \mathbb{Z}_3[x]/(g)$ für $p \in \mathbb{Z}_3[x]_{\text{grad}(g)}$.

4. Vorbereitung auf TA Blatt 8

4.1 VA 1, Reste bei Polynomdivision in $\mathbb{Z}_5[x]$

Gegeben seien die Polynome
$a(x) = x^4 + x^3 + 3$ und $b(x) = 3x^2 + 4$
aus dem Polynomring $\mathbb{Z}_5[x]$ über dem Körper $\mathbb{Z}_5$.

1. Wie viele Elemente enthält die Menge $R_{\text{grad}(b)}$ aller Polynome $r(x) \in \mathbb{Z}_5[x]$
   mit $\text{grad}(r) < \text{grad}(b)$?
2. Bestimmen Sie Polynome $q(x), r(x) \in \mathbb{Z}_5[x]$, so dass gilt
   $a(x) = q(x) \cdot b(x) + r(x)$ mit $\text{grad}(r) < 2$.

1. Wie viele Elemente enthält die Menge $R_{\mathrm{grad}(b)}$ aller Polynome $r(x) \in \mathbb{Z}_5[x]$ mit $\mathrm{grad}(r) < \mathrm{grad}(b)$?

Lösung:

$|R_{\mathrm{grad}(b)}| = 25$.

Polynome höchstens vom Grad 1 sind durch 2 Koeffizienten bestimmt.

Für jeden Koeffizienten gibt es 5 Belegungsmöglichkeiten.

2. Bestimmen Sie Polynome $q(x), r(x) \in \mathbb{Z}_5[x]$, so dass gilt $a(x) = q(x) \cdot b(x) + r(x)$ mit $\text{grad}(r) < 2$.

Lösung:

Division:

$$
\begin{array}{rrcll}
 & \overbrace{x^4 + x^3 + 3}^{a(x)} & (\text{div}) & \overbrace{3x^2 + 4}^{b(x)} & = 2x^2 \\
- & (x^4 + 3x^2) & & & \\
\hline
 & x^3 + 2x^2 + 3 & & & +2x \\
- & (x^3 + 3x) & & & \\
\hline
 & 2x^2 + 2x + 3 & & & +4 \\
- & (2x^2 + 1) & & q(x) = & 2x^2 + 2x + 4 \\
\hline
 & 2x + 2 = r(x) & & &
\end{array}
$$

4.2 VA 2, Restklassenringe

Wir betrachten den Ring $R = \mathbb{Z}_3[x]$.

Beachten und nutzen Sie im Folgenden die Isomorphie zwischen $\langle \mathbb{Z}_3[x]/(g), +, \cdot \rangle$ und $\langle \mathbb{Z}_3[x]_{\mathrm{grad}(g)}, +_g, \cdot_g \rangle$, die für alle $g \in R$ durch die Abbildung $[f]_g \rightarrow Rem_g(f)$ gegeben ist.

Wir schreiben gelegentlich $p \in \mathbb{Z}_3[x]/(g)$ für $p \in \mathbb{Z}_3[x]_{\mathrm{grad}(g)}$.

Sei $g(x) = x^2 + 2x + 1$.

1. Bestimmen Sie alle Elemente des Rings $\mathbb{Z}_3[x]/(g)$.
2. Bestimmen Sie die Spalten der Additions- und Multiplikations-Verknüpfungstafeln zum Element $[x+2]_g \in \mathbb{Z}_3[x]/(g)$.
3. Berechnen Sie Polynome $p(x) \in \mathbb{Z}_3[x]$ und $r(x) \in \mathbb{Z}_3[x]_2$ mit der Eigenschaft

$$x^4 + x + 1 = p(x) \cdot (x^2 + 2x + 1) + r(x)\,.$$

4. Ist der Restklassenring $\mathbb{Z}_3[x]/(g)$ ein Körper? Begründung!

1. Bestimmen Sie alle Elemente des Rings $\mathbb{Z}_3[x]/(g)$.

Lösung:

Wir stellen die Elemente des Rings $\mathbb{Z}_3[x]/(x^2+2x+1)$ durch die Reste in $\mathbb{Z}_3[x]_2$ dar.
Es gilt

$$\mathbb{Z}_3[x]_2 = \{0, 1, 2, x, x+1, x+2, 2x, 2x+1, 2x+2\}\,.$$

2. Bestimmen Sie die Spalten der
Additions- und Multiplikations-Verknüpfungstafeln
zum Element $[x+2]_g \in \mathbb{Z}_3[x]/(g)$.

Lösung:

$+$	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
$x+2$	$x+2$	x	$x+1$	$2x+2$	$2x$	$2x+1$	2	0	1

$\cdot$	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
$x+2$	0	$x+2$	$2x+1$	2	$x+1$	$2x$	1	x	$2x+2$

3. Berechnen Sie Polynome $p(x) \in \mathbb{Z}_3[x]$ und $r(x) \in \mathbb{Z}_3[x]_2$ mit der Eigenschaft

$$x^4 + x + 1 = p(x) \cdot (x^2 + 2x + 1) + r(x)\,.$$

Lösung:

Es gilt $p(x) = x^2 + x$ und $r(x) = 1$.

4. Ist der Restklassenring $\mathbb{Z}_3[x]/(g)$ ein Körper? Begründung!

Lösung:

Der Restklassenring $\mathbb{Z}_3[x]/(x^2+2x+1)$ ist kein Körper, weil er nicht nullteilerfrei ist. Es gilt

$$(x+1)\cdot(x+1) = x^2+2x+1 \equiv_g 0\,.$$

4.3 VA 3, Irreduzibilität

Ist $x^4 + x^3 + 1$ irreduzibel in GF(2)[x]? Begründung!

Lösung:

Antwort: $p(x) = x^4 + x^3 + 1$ ist irreduzibel in $GF(2)$.

Bemerkung: $GF(2)$ ist isomorph zu $\langle \mathbb{Z}_2, +_2, \cdot_2 \rangle$.

Widerspruchsbeweis:

Wir nehmen an, dass p reduzibel ist.

Dann gibt es Polynome $p_1, p_2 \in \mathbb{Z}_2[x]$ mit $\text{grad}(p_i) \geq 1$, $(i = 1, 2)$ und $p = p_1 \cdot p_2$.

p besitzt keine Nullstelle, denn $p(0) = p(1) = 1$.

Daraus folgt, dass weder p_1 noch p_2 linear, d.h., vom Grad 1 sein kann.

Also gilt $\text{grad}(p_1) = \text{grad}(p_2) = 2$.

Wir machen dan Ansatz $p_1 = x^2 + ax + b$ und $p_2 = x^2 + cx + d$.

Dann gilt

$$\begin{aligned} x^4 + x^3 + 1 &= (x^2 + ax + b)(x^2 + cx + d) \\ &= x^4 + (a + c)x^3 + (b + d + ac)x^2 + (ad + bc)x + bd\,. \end{aligned}$$

Koeffizientenvergleich ergibt die 4 Gleichungen

$$(1)\ a+c=1, \quad (2)\ b+d+ac=0, \quad (3)\ ad+bc=0, \quad (4)\ bd=1\,.$$

Aus (4) folgt $b=d=1$.

Eingesetzt in (3) folgt $a+c=0$ im Widerspruch zu (1).