Algebra (Wintersemester 2014/15) — Blatt: 9

Stefan Wewers, Michel Börner

Punkte: 20 +5*

Abgabe **zu zweit oder zu dritt** vor der Vorlesung am Di., **16.12.14** oder am gleichen Tag in He18, Zimmer E07 (ggf. unter der Tür durchschieben). **Bitte auch das Moodle-Forum nutzen!**

Aufgabe 1 (Chinesischer Restsatz) (3+3+2+2*+3* = **8+5* P**)

Lösen Sie mit dem chinesischem Restsatz die folgenden Kongruenzen. Geben Sie insbesondere ein möglichst großes Ideal I an so dass x eine Lösung der Kongruenz modulo I ist.

a) Es sei $R = \mathbb{Z}$. Zeigen Sie zunächst, dass sich das linke System von Kongruenzen auf das rechte reduzieren lässt. Sie dürfen auch nur das rechte System lösen (1 Punkt Abzug).

$$\begin{aligned} x &\equiv 1 \mod 2 \\ x &\equiv 2 \mod 3 \\ x &\equiv 0 \mod 5 \\ x &\equiv 5 \mod 6 \\ x &\equiv 3 \mod 7 \\ x &\equiv 3 \mod 8 \\ x &\equiv 17 \mod 21 \\ x &\equiv 38 \mod 63 \end{aligned} \qquad\qquad \begin{aligned} x &\equiv 3 \mod 8 \\ x &\equiv 2 \mod 9 \\ x &\equiv 0 \mod 5 \\ x &\equiv 3 \mod 7 \end{aligned}$$

b) Verfahren Sie wie oben mit $R = \mathbb{F}_2[x]$,

$$\begin{aligned} g &\equiv x \mod (x^2+x+1) \\ g &\equiv 1 \mod (x^3+x+1) \end{aligned}$$

Zusatz: Zeigen Sie, dass das Problem über $R = \mathbb{F}_{64}[x]$ ein Interpolationsproblem ist und ein Polynom g vom Grad 1 liefert. (2* P)

c) Verfahren Sie wie oben mit $R = \mathbb{Z}[i]$,

$$\begin{aligned} x &\equiv 2 \mod (2+i) \\ x &\equiv 1 \mod (3-2i) \end{aligned}$$

Stellen Sie die Lösung als $x \mod I$ dar mit einem Repräsentanten $x \in \mathbb{Z}$ und $I \lhd \mathbb{Z}[i]$.

d) (Weihnachtsaufgabe*) Der Weihnachtsmann will sicherstellen, dass 3 seiner Elfen im Falle seines Ablebens den Schlitten mit den Geschenken fliegen können – er möchte jedoch verhindern, dass bis zu 2 seiner Elfen den Schlitten zweckentfremden. Dazu versieht er seinen Schlitten mit einem Code und definiert ein (geheimes) Polynom $f(x)$ vom (öffentlich bekannten) Grad 2 in dem (öffentlich bekannten) Ring $\mathbb{F}_p[x]$, $p > 10^{10}$, p prim. Nun nennt er dem ersten Elfen den Wert $f(1) \in \mathbb{F}_p$, dem zweiten Elfen den Wert $f(2) \in \mathbb{F}_p$, usw. . Der Code am Schlitten ist $f(0) \in \mathbb{F}_p$.

Zeigen Sie, dass der Schlitten genau dann fliegt, wenn sich mindestens 3 Elfen einig sind.

Hinweis: Es darf angenommen werden, dass es mehr als 2 und weniger als p Elfen gibt.

Aufgabe 2 (Ideale) **(3 P)**

Zeigen Sie, dass der Ring

$$\mathbb{Z}[i] / (3+2i)$$

ein Körper mit 13 Elementen ist.

Aufgabe 3 (Affine Geometrie) (1+1+1+1+1 = **5 P**)

Sei K ein nichtendlicher Körper, $R = K[x_1, \ldots, x_n]$ und Z, W Teilmengen des affinen Raumes $\mathbb{A}^n_K$. Zeigen Sie:

a) $Z \subseteq W \implies \mathcal{I}(Z) \supseteq \mathcal{I}(W)$

b) $\mathcal{I}(Z \cup W) = \mathcal{I}(Z) \cap \mathcal{I}(W)$

c) $\mathcal{I}(Z \cap W) \supseteq \mathcal{I}(Z) + \mathcal{I}(W)$

d) $Z \subseteq \mathcal{Z}(\mathcal{I}(Z))$

e) Gleichheit in Teilaufgabe d) gilt genau dann, wenn Z algebraisch ist.

Aufgabe 4 (Einheitskreis) (1+1+2 = **4 P**)

Sei $R := \mathbb{R}[x, y \mid x^2 + y^2 = 1]$ der Koordinatenring des Einheitskreises.

a) Zeigen Sie: Jedes Element $f \in R$ besitzt eine eindeutige Darstellung

$$f = f_0 + f_1 y,$$

mit $f_0, f_1 \in \mathbb{R}[x]$.

b) Zeigen Sie: $y \mid f \in R$ genau dann wenn $1 - x^2 \mid f_0 \in \mathbb{R}[x]$.

c) Schließen Sie aus Teilaufgabe b): R ist nicht faktoriell.
Hinweis 1: Rechnen Sie zunächst nach, dass $N: R \to \mathbb{R}[x], f_0 + f_1 y \mapsto f_0^2 + (x^2-1) f_1^2$ multiplikativ ist und insbesondere folgt $N(\alpha) \in \mathbb{R}[x]^\times$ für $\alpha \in R^\times$.
Hinweis 2: $y^2 = 1 - x^2$.