Algebra, Prüfung am 26.6.2014, Goldstern

1. Sei C_2 die Gruppe mit 2 Elementen; mit S_∞ bezeichnen wir die Gruppe aller Permutationen der Mengen $\mathbb{Z}$ aller ganzen Zahlen, mit S_3 die Gruppe aller Permutationen einer festen 3-elementigen Menge.

   (a) Definieren Sie den Begriff „Koprodukt von G_1 und G_2 in der Klasse *aller* Gruppen“, sowie den Begriff „Koprodukt von G_1 und G_2 in der Klasse aller *kommutativen* Gruppen“.
   Definieren Sie (für jede Gruppe G und jedes $g \in G$) den Begriff „Ordnung von g in G.“

   (G, i_1, i_2) is Koprodukt von G_1 und G_2 in der Klasse X, wenn $i_1 : G_1 \to G$ und $i_2 : G_2 \to G$ Homomorphismen sind, $G \in X$, und es für alle Algebren $H \in X$ und alle Homomorphismen $f_1 : G_1 \to H$, $f_2 : G_2 \to H$ genau einen Homomorphismus $h : G \to H$ gibt, der $h \circ i_1 = f_1$ und $h \circ i_2 = f_2$ erfüllt. (Für $X =$ Klasse aller Gruppen ergibt sich der Begriff „Koprodukt in der Klasse aller Gruppen“, für $X =$Klasse alle kommutativen Gruppen ergibt sich da Koprodukt in den kommutativen Gruppen.)
   Die Ordnung von g in G ist die Kardinalität der von g erzeugten Untergruppe $\langle g \rangle = \{g^n : n \in \mathbb{Z}\}$. Äquivalent: Die kleinste natürliche Zahl $n > 0$ mit $g^n = 1_G$; wenn es kein solches n gibt (äquivalent: wenn $\langle g \rangle$ unendlich ist), ist die Ordnung (je nach Lehrbuch) ∞, oder 0, oder undefiniert.

   (b) Im Folgenden sei G das Koprodukt von C_2 und C_2 in der Klasse aller Gruppen, K das Koprodukt von C_2 und C_2 in der Klasse aller kommutativen Gruppen. *Beschreiben* Sie die Gruppe K.

   $K = C_2 \times C_2 = \{0,1\}^2$, mit den Einbettungen $i_1 : C_2 \to K$, $i_1(x) = (x, 0)$, analog $i_2(y) = (0, y)$. ($C_2 \times C_2$ ist die Produktgruppe; die Operationen werden koordinatenweise ausgeführt.)

   (c) Finden Sie zwei verschiedene nichtkonstante Homomorphismen $f_1, f_2 : C_2 \to S_3$. Verwenden Sie diese beiden Homomorphismen, um zu zeigen, dass G nicht kommutativ sein kann.

   Sei (12) die Permutation von $\{1, 2, 3\}$, die 1 und 2 vertauscht. Dann können wir $0 \in C_2$ auf die Identität abbilden, $1 \in C_2$ auf (12) und erhalten so einen Homomorphismus f_1. (Weil (12) Ordnung 2 hat.) Analog könnten wir 1 auf (13) abbilden und erhalten einen weiteren Homomorphismus f_2.
   Sei $h : G \to S_3$ nun wie in der Definition des Koprodukts. Dann ist $h(i_1(1)) = (12)$, und $h(i_2(1)) = (13)$. Wenn $i_1(1)$ und $i_2(1)$ in G vertauschbar wären, dann wären auch deren Bilder in S_3 vertauschbar; das sind sie aber nicht, denn $(12) \circ (13) \neq (13) \circ (12)$, wie man leicht nachrechnet. Daher ist G nicht kommutativ.

   (d) Seien π_1 und π_2 die durch $\forall n : \Big(\pi_1(2n) = 2n{+}1,\ \pi_2(2n) = 2n{-}1\Big), \qquad \pi_1 \circ \pi_1 = id_{\mathbb{Z}} = \pi_2 \circ \pi_2$ definierten Permutationen von $\mathbb{Z}$. Geben Sie eine Wertetabelle für π_1, π_2, $\pi_1 \circ \pi_2$ an. (Natürlich nur einen endlichen Ausschnitt, aus dem man aber auch die übrigen Werte leicht erschließen kann.) Geben Sie die Ordnungen von π_1, π_2, $\pi_1 \circ \pi_2$ an. *Schließen* Sie daraus, dass die von π_1 und π_2 erzeugte Untergruppe von S_∞ unendliche viele Elemente haben muss.

x	-2	-1	0	1	2	3	4
$\pi_1(x)$	-1	-2	1	0	3	2	5
$\pi_2(x)$	-3	0	-1	2	1	4	3
$\pi_1 \circ \pi_2(x)$	-4	1	-2	3	0	5	2

   $o(\pi_1) = 2 = o(\pi_2)$, aber $o(\pi_1 \circ \pi_2) = \infty$. Die Untergruppe $\langle \pi_1, \pi_2 \rangle$ enthält alle Potenzen $(\pi_1 \circ \pi_2)^n$, und diese sind alle verschieden. Daher ist diese Untergruppe unendlich groß.

   (e) Zeigen Sie, dass G unendliche viele Elemente haben muss.

   Sei $f_1 : C_2 \to S_\infty$ durch $f_1(1) = \pi_1$ definiert. (und $f_1(0) = id$) Das ist ein Homomorphismus, weil π_1 Ordnung 2 hat. Analog definieren wir f_2 durch $f_2(1) := \pi_2$.
   Wir finden h wie in der Definition des Koprodukts. Dann ist die unendliche Gruppe $\langle \pi_1, \pi_2 \rangle \leq S_\infty$ das Bild (unter h) der Untergruppe $\langle f_1(1), f_2(1) \rangle \leq G$; letztere muss also auch unendlich viele Elemente haben.

2. Sei $R = \mathbb{Q}[x, y]$ der Ring aller Polynome in zwei Variablen mit Koeffizienten in $\mathbb{Q}$.
(R kann auch als Polynomring über dem Ring $\mathbb{Q}[x]$ aufgefasst werden, und ist daher ein Integritätsbereich.) Mit (x), (y), (x, y), $(x-y)$ bezeichnen wir die Ideale, die von den jeweiligen Polynomen erzeugt werden; zum Beispiel ist (x, y) das kleinste Ideal, das sowohl das Polynom x als auch das Polynom y enthält.

(a) *Beschreiben* Sie die Ringe $R/\{0\}$, $R/(x)$, $R/(y)$, $R/(x, y)$, $R/(x-y)$. (Etwa indem Sie wohlbekannte Ringe finden, zu denen die angegebenen Ringe isomorph sind.)
Ihre Beschreibung sollte insbesondere die folgenden Fragen beantworten:

(b) Welche dieser Ringe sind Integritätsbereiche, welche sind Körper?

(c) Geben Sie an, welche dieser 5 Ringe zu welchen anderen isomorph sind. Geben Sie gegebenenfalls Isomorphismen an, bzw. erklären Sie, warum die jeweiligen Ringe nicht isomorph sind.

(d) Geben Sie für jedes der genannte Ideale I beispielhaft an, wie man zwei Elemente von R/I multipliziert.

Für jeden Integritätsbereich S gilt folgendes Lemma:

($*1$) Wenn $p(x) \in S[x]$, $\alpha \in S$ und $p(\alpha) = 0$, dann ist $p(x)$ durch $(x - \alpha)$ teilbar. [Beweis: Da $x - \alpha$ monisch ist, funktioniert der übliche Divisionsalgorithmus und liefert eine Darstellung $p(x) = (x - \alpha) * q(x) + s$, $s \in S$. Wegen $p(\alpha) = 0$ erhält man $s = 0$.

($*2$) Mit anderen Worten: Der Kern des Einsetzungshomomorphismus
$\varphi_\alpha : S[x] \to S$, $p(x) \mapsto p(\alpha)$, ist das vom Polynom $(x - \alpha)$ erzeugte Ideal.

- $\boxed{\mathbb{Q}[x, y] \simeq R/\{0\}}$ durch den trivialen Isomorphismus $p \mapsto p + \{0\} = \{p\}$. Dieser Ring ist ein Integritätsbereich, sogar faktoriell, aber kein Hauptidealring. (Zum Beispiel ist (x, y) kein Hauptideal, siehe UE.)
- Der Einsetzungshomomorphismus $\varphi_0 : \mathbb{Q}[x][y] \to \mathbb{Q}[x]$ (der für y den Wert 0 einsetzt), hat laut ($*2$) den Kern (y).
Außerdem ist φ surjektiv. Daher (laut Homomorphiesatz): $\boxed{R/(y) \simeq \mathbb{Q}[x].}$
- Analog zeigt man $\boxed{R/(x) \simeq \mathbb{Q}[y]}$. (Isomorphismus $p(x, y) + (x) \mapsto p(0, y) \in \mathbb{Q}[y]$.)
- $\mathbb{Q}[x] \simeq \mathbb{Q}[y]$, durch den Isomorphismus $x \mapsto y$ (auf $\mathbb{Q}$ ist der Isomorphismus die Identität), also allgemeiner $p(x) \mapsto p(y)$. Dies ist ein Hauptidealring, aber kein Körper.
- Sei $I := (x, y)$. Wenn ein Polynom $p(x, y)$ den konstanten Term $r \in \mathbb{Q}$ hat (es muss $r = p(0, 0)$ sein) dann ist $p(x, y) - r \in I$, also $p(x, y) + I = r + I$; verschiedene Konstante sind aber nie äquivalent. Daher ist $p(x, y) + I \mapsto p(0, 0)$ wohldefiniert und ein $\boxed{\text{Isomorphismus zwischen } R/(x, y) \text{ und } \mathbb{Q}}$. (Anders gesagt: Der Kern des Einsetzunghomomorphismus $\varphi_{0,0} : \mathbb{Q}[x, y] \to \mathbb{Q}$, $p(x, y) \mapsto p(0, 0)$, ist genau das Ideal (x, y).
- Laut ($*2$) (mit $S := \mathbb{Q}[y]$, $\alpha := y$) hat der Einsetzungshomomorphismus $\varphi_y : \mathbb{Q}[y][x] \to \mathbb{Q}[y]$ den Kern $(x - y)$. Außerdem ist φ_y surjektiv, also laut Homomorphiesatz: $\boxed{\mathbb{Q}[x, y]/(x - y) \simeq \mathbb{Q}[y]}$, mit Isomorphismus $p(x, y) + ((x - y)) \mapsto p(y, y)$.
- Die Ringe $\mathbb{Q}[x, y]$, $\mathbb{Q}[x]$, $\mathbb{Q}$ sind nicht isomorph: $\mathbb{Q}$ ist der einzige Körper, $\mathbb{Q}[x, y]$ der einzige nicht-Hauptidealring. Alle drei sind abzählbar unendliche Integritätsvereiche.
- Wir betrachten das Polynom $p = 4 + 3x - 2y$ und quadrieren es (bzw seine Nebenklasse):
Modulo $\{0\}$ rechnet man wie mit Polynomen: $p^2 = 16 + 9x^2 + 4y^2 + 24x - 16y - 12xy$.
Modulo (x) gilt $p + (x) = 4 - 2y + (x)$, mit Quadrat $16 - 8y + 4y^2 + (x)$.
Modulo (y): $(p + (y))^2 = (4 + 3x + (y))^2 = 16 + 24x + 9x^2 + (y)$.
Modulo $I := (x - y)$ gilt $x + I = y + I$, also $4 + 3x - 2y + I = 4 + x + I$, mit Quadrat $16 + 8x + x^2 + I$.
Modulo $J := (x, y)$ gilt $x + J = y + J = 0 + J$, wir rechnen also mit rationalen Zahlen: $4 + 3x - 2y + J = 4 + J$, quadriert: $16 + J$.