Musterlösung zum dritten Übungsblatt von Algebra und Zahlentheorie (Aufgabe 1d), 2, 3 und 4)

14. Januar 2019

Aufgabe 1 (d)**.** *Nehmen Sie an, dass G nicht abelsch ist. Finden Sie dann einen Gruppenisomorphismus $\varphi : G \to S_3$.*

Lösung:

Behauptung 1. *$\varphi : G \to S_3$ mit*

$$\sigma^i\tau^j \mapsto \begin{pmatrix}1 & 2 & 3\\ 3 & 2 & 1\end{pmatrix}^i \begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix}^j,\ i,j \in \mathbb{N}$$

ist ein Gruppenisomorphismus.

Beweis. Da $ord(\begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix}) = 3$ und $ord(\begin{pmatrix}1 & 2 & 3\\ 3 & 2 & 1\end{pmatrix}) = 2$ können wir S_3 nach Aufgabenteil ii) folgendermaßen konstruieren:

$$S_3 = \{ \begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix}^3, \begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix}^2, \begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix}, \begin{pmatrix}1 & 2 & 3\\ 3 & 2 & 1\end{pmatrix},$$
$$\begin{pmatrix}1 & 2 & 3\\ 3 & 2 & 1\end{pmatrix} * \begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix}, \begin{pmatrix}1 & 2 & 3\\ 3 & 2 & 1\end{pmatrix} * \begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix}^2 \}$$

Außerdem ist dann φ surjektiv, da $i, j \in \mathbb{N}$. Somit ist φ auch injektiv, da $|G| = |S_3| = 6$ endlich ist. Es bleibt also zu zeigen: $\varphi(g * g') = \varphi(g) * \varphi(g'),\ g, g' \in G$. Bemerke zunächst, dass für $i \in \{0, 1\}, j \in \{0, 1, 2\}$

$$\sigma^i\tau^j = \begin{cases} \tau^{2j}\sigma^i, i \text{ ungerade und } j > 0 \\ \tau^j\sigma^i\ , \text{ sonst} \end{cases}$$

Nach Konstruktion gilt dies auch für S_3.
Es gilt für $x, y \in G$ mit $x = \sigma^i\tau^j$ und $y = \sigma^k\tau^l$, wobei $i, k \in \{0, 1\}, j, l \in \{0, 1, 2\}$, folgende Fallunterscheidung:

Fall 1: k ungerade und $j > 0$

$$\begin{aligned} x * y &= \sigma^i \tau^j * \sigma^k \tau^l \\ &= \sigma^i \sigma^k \tau^{2j} \tau^l \\ &= \sigma^{i+k} * \tau^{2j+l} \end{aligned}$$

Somit

$$\varphi(x * y) = \varphi(\sigma^{i+k} * \tau^{2j+l}) = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}^{i+k} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}^{2j+l}$$

Gleichzeitig gilt

$$\begin{aligned} \varphi(x) * \varphi(y) &= \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}^{i} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}^{j} * \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}^{k} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}^{l} \\ &= \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}^{i+k} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}^{2j+l}, \end{aligned}$$

da S_3 nicht ablesch ist.
Fall 2: analog mit $x * y = \sigma^{i+k} \tau^{j+l}$.

Somit gilt also $\varphi(g * g') = \varphi(g) * \varphi(g'),\ g, g' \in G$ □

Aufgabe 2. *Beschreiben Sie den ersten Isomorphiesatz für die folgenden Mengen explizit:* $G = GL(2, \mathbb{C})$, $H = SL(2, \mathbb{C})$ *and* $N = \{c * I_2 \mid c \in \mathbb{C}^*\} = \mathbb{C}^* I_2$.

Lösung: Aus der linearen Algebra wissen wir, dass $SL(2, \mathbb{C}) < GL(2, \mathbb{C})$ gilt. Prüfen müssen wir, ob $\mathbb{C}^* I_2$ einen normale Untergruppe von $GL(2, \mathbb{C})$ ist. Dazu gehen wir die Untergruppenaxiome durch:

- (UG1) gilt, da $I_2 \in \mathbb{C}^* I_2$.
- (UG2) gilt, da $xI_2, yI_2 \in \mathbb{C}^* I_2 \Rightarrow x * y * I_2 \in \mathbb{C}^* I_2$ gilt.
- (UG3) gilt, da $xI_2 \in \mathbb{C}^* I_2 \Rightarrow \exists x^{-1} I_2 \in \mathbb{C}^* I_2 : x^{-1} * xI_2 = I_2$ gilt.

Nun prüfen wir die Normalität: Seien $g \in GL(2, \mathbb{C})$ und $xI_2 \in \mathbb{C}^* I_2$. Zu zeigen ist, dass $g * xI_2 * g^{-1} \in \mathbb{C}^* I_2$. Da aber $g * xI_2 = xI_2 * g$ gilt, folgt $xI_2 * g * g^{-1} = xI_2$ und $xI_2 \in \mathbb{C}^* I_2$.
Somit können wir uns nun der Aussage des Satzes zuwenden. Dieser besagt:

- $SL(2, \mathbb{C}) * \mathbb{C}^* I_2 < GL(2, \mathbb{C})$ ist eine Untergruppe
- $\mathbb{C}^* I_2 \trianglelefteq SL(2, \mathbb{C}) * \mathbb{C}^* I_2$ ist eine normale Untergruppe
- $SL(2, \mathbb{C}) \cap \mathbb{C}^* I_2 \trianglelefteq SL(2, \mathbb{C})$ ist eine normale Untergruppe
- Die Hauptaussage: $SL(2, \mathbb{C}) / (SL(2, \mathbb{C}) \cap \mathbb{C}^* I_2) \cong (SL(2, \mathbb{C}) * \mathbb{C}^* I_2) / \mathbb{C}^* I_2$

Für die ersten drei Punkte kann der Beweis aus der Vorlesung übernommen werden. Interessant ist vor allem, genau zu untersuchen, zwischen welchen Mengen sich die Isomorphie ergibt. Dazu wollen wir $(SL(2,\mathbb{C}) * \mathbb{C}^* I_2)/\mathbb{C}^* I_2$ und $SL(2,\mathbb{C}) \cap \mathbb{C}^* I_2$ genauer betrachten.

Behauptung 2. $(SL(2,\mathbb{C}) * \mathbb{C}^* I_2)/\mathbb{C}^* I_2 = SL(2,\mathbb{C})/\mathbb{C}^* I_2$

Beweis. Um diese Gleichheit zu sehen, betrachten wir ein Element $M \in (SL(2,\mathbb{C}) * \mathbb{C}^* I_2)/\mathbb{C}^* I_2$. Für dieses M gilt

$$M = (m * cI_2) * \mathbb{C}^* I_2 = m * \mathbb{C}^* I_2$$

Dies gilt, da cI_2 auf jeden Fall ein Element von $\mathbb{C}^* I_2$ ist. Die Gleichung gibt uns beide Richtungen der Teilmengenbeziehungen.

□

Behauptung 3. $SL(2,\mathbb{C}) \cap \mathbb{C}^* I_2 = \{I_2, -I_2\}$

Beweis. Sei $m \in SL(2,\mathbb{C}) \cap \mathbb{C}^* I_2$. Dann ist $m = c * I_2$ für ein $c \in \mathbb{C}^*$ und für die Determinante von m gilt

$$det(c * I_2) = c^2 * det(I_2) = c^2 * 1 = c^2 = 1$$

Die letzte Gleichheit ergibt sich aus dem Schnitt mit $SL(2,\mathbb{C})$. Nun hat $c^2 = 1$ genau zwei Lösungen und diese sind 1 und -1. Damit folgt die Behauptung, da auch $I_2 \in SL(2,\mathbb{C}) \cap \mathbb{C}^* I_2$ (ebenso $-I_2$) ist. □

Nach der Aussage vom ersten Isomorphissatz können wir also einen Isomorphismus $\phi : SL(2,\mathbb{C})/\{I_2, -I_2\} \to SL(2,\mathbb{C})/\mathbb{C}^* I_2$ finden. Die Abbildungsvorschrift hat folgende Form:

$$m * \{I_2, -I_2\} \mapsto m * \mathbb{C}^* I_2$$

Hier können wir sehen, dass die Anzahl der Äquivalenzklassen gleich groß ist und sich strukturell unter der Multiplikation gleich verhalten (der Gruppenhomomorphismus bezieht sich auf die Multiplikation). Die Anzahl an möglichen Representanten für eine Äquivalenzklasse ist in $SL(2,\mathbb{C})/\{I_2, -I_2\}$ genau zwei (nämlich $m * I_2$ und $m * (-I_2)$ für ein $m \in SL(2,\mathbb{C})$). In $SL(2,\mathbb{C})/\mathbb{C}^* I_2$ finden wir dagegen unendlich viele Representanten für ein einzelnes Element (nämlich $m * c * I_2$ für ein $m \in SL(2,\mathbb{C})$ und ein beliebiges $c \in \mathbb{C}^*$).

Aufgabe 3. *Sei K ein Körper. Sind die folgenden Abbildungen Ringhomomorphismen? Falls ja, was sind Bild und Kern des Homomorphismus?*

Lösung: Im folgenden sei 1 zu verstehen als neutrales Element der Multiplikation im Körper K.
Teil a)
Man gebe ein Gegenbeispiel. Zum Beispiel seinen $t, 1 \in K[t]$. Dann gilt

$$\varphi_1(1 * t) = 1 \neq \varphi_1(1) * \varphi_1(t) = 0 * 1 = 0$$

Und somit kann ϕ_1 kein Ringhomomorphismus sein.

Teil b)

Man gebe wieder ein Gegenbeispiel. Sei $M = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ und sei $N = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$. Dann gilt

$$\varphi_2(M) * \varphi_2(N) = 1 * 1 = 1 \neq \varphi_2(M * N) = 1 + 1$$

und somit kann auch ϕ_2 kein Ringhomomorphismus sein.

Teil c)

Zunächst werden wir checken, ob $\varphi_a(f+g) = \varphi_a(f) + \varphi_a(g)$ ist für $f, g \in K[t]$, wobei $f = \sum_{i=0}^{n} f_i t^i$ und $g = \sum_{j=0}^{m} g_j t^j$.

$$\varphi_a(f+g) = \varphi_a(\sum_{i=0}^{n} f_i * t^i + \sum_{j=0}^{m} g_j * t^j) = \varphi_a(\sum_{k=0}^{max\{n,m\}} (f_k + g_k) * t^k)$$

wobei $f_k = 0$, wenn $k > n$ und $g_k = 0$, wenn $k > m$. Die letzte Gleichheit folgt nach der Definition der Addition im Polynomring $K[t]$. Nun gilt weiter

$$\varphi_a(\sum_{k=0}^{max\{n,m\}} (f_k + g_k) * t^k) = \sum_{k=0}^{max\{n,m\}} (f_k + g_k) * a^k = \sum_{i=0}^{n} f_i * a^i + \sum_{j=0}^{m} g_j * a^j$$

wobei die letzte Gleichheit nun nach den Rechenregeln im Körper K folgt und nicht nach der Definition der Addition im Polynomring! Wir sehen nun

$$\sum_{i=0}^{n} c f_i * a^i + \sum_{j=0}^{n} c g_j * a^j = \varphi_a(f) + \varphi_a(g)$$

wie gewollt.

Als nächstes prüfen wir, ob $\varphi_a(f * g) = \varphi_a(f) * \varphi_a(g)$.

$$\varphi_a(f*g) = \varphi_a(\sum_{i=0}^{n} f_i t^i * \sum_{j=0}^{m} g_j t^j) \overset{*}{=} \varphi_a(\sum_{k=0}^{n+m} (\sum_{i+j=k} f_i * g_j) * t^k) = \sum_{k=0}^{n+m} (\sum_{i+j=k} f_i * g_j) * a^k$$

Man bemerke, dass wir bei der gekennzeichneten Gleichheit die Definition der Multiplikation im Polynomring $K[t]$ verwenden.

$$\sum_{k=0}^{n+m} (\sum_{i+j=k} f_i * g_j) * a^k = \sum_{i=0}^{n} f_i a^i * \sum_{j=0}^{m} g_j a^j$$

Dass diese Gleichheit stimmt, muss man im Körper K nachrechnen zum Beispiel mit Induktion! Es ist keine triviale Gleichheit! Damit haben wir dann

$$\sum_{i=0}^{n} f_i a^i * \sum_{j=0}^{m} g_j a^j = \varphi_a(f) * \varphi_a(g)$$

wie gewollt.

Außerdem gilt, dass $\varphi_a(1) = 1$ ist. Somit ist φ_a ein Ringhomomorphismus.

Wie sieht es nun mit Bild und Kern von φ_a aus?

Behauptung 4. $Im(\varphi_a) = K$

Um dies zu sehen, sei $x \in K$. Dann gilt aber auch $x \in K[t]$. Außerdem ist $x(a) = x$ für alle $a \in K$, wobei x in $K[t]$ betrachtet wird. Somit folgt die Behauptung.

Behauptung 5. $ker(\varphi_a) = (t - a)$

Beweis. Rückrichtung: Sei $x \in (t - a)$. Dann gilt $x(t) = (t - a) * g(t)$ mit $g(t) \in K[t]$. Somit ist

$$x(a) = (a - a) * g(t) = 0$$

und damit $x \in ker(\varphi_a)$.
Hinrichtung: Sei $x \in ker(\varphi_a)$. Wir wissen, dass $K[t]$ ein kommutativer Ring mit Eins ist und, dass der höchste Koeffizient von $(t - a) \in K[t]$ eine Einheit ist. Somit existiert eine Polynomdivision mit Rest folgender Form:

$$x = (t - a) * g(t) + r(t), \text{ wobei } g(t), r(t) \in K[t] \text{ und } grad(r) < grad(g) = 1.$$

Wir wissen, dass $x(a) = 0$ also $(a - a) * g(a) + r(a) = r(a) = 0$. Da aber $grad(r) = 0$ gilt, ist $r = 0$. Die sich ergebende Darstellung $(t - a) * g(t)$ für $x(t)$ impliziert, dass $x(t) \in (t - a)$, dem Ideal von $t - a$, gilt. □

Aufgabe 4. *Sei $d \in \mathbb{Z}$, sodass $n^2 \nmid d$ für die ganzen Zahlen $n > 1$. Sei*

$$\mathbb{Z}[\sqrt{d}] := \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\} \subset \mathbb{C}.$$

a) Beweisen Sie, dass $\mathbb{Z}[\sqrt{d}]$ ein Unterring von $\mathbb{C}$ ist.
b) Sei $\varphi : \mathbb{Z}[t] \mapsto \mathbb{C}$ die Abbildung mit $\varphi(P(t)) := P(\sqrt{d})$. Beweisen Sie, dass φ ein Ringhomomorphismus ist und finden Sie den Kern und das Bild von φ.

Lösung: Teil a) Um zu zeigen, dass $\mathbb{Z}[\sqrt{d}]$ ein Unterring von $\mathbb{C}$ ist, müssen wir folgende Punkte beweisen:

- 1) Abgeschlossenheit bezüglich der Subtraktion: $\forall a, b \in \mathbb{Z}[\sqrt{d}] : a - b \in \mathbb{Z}[\sqrt{d}]$
- 2) Abgeschlossenheit bezüglich der Multiplikation: $\forall a, b \in \mathbb{Z}[\sqrt{d}] : a * b \in \mathbb{Z}[\sqrt{d}]$
- 3) $1 \in \mathbb{Z}[\sqrt{d}]$

Zu 1): Seien $x + y\sqrt{d}$ und $v + w\sqrt{d}$ zwei Elemente von $\mathbb{Z}[\sqrt{d}]$. Dann ist

$$x + y\sqrt{d} - (v + w\sqrt{d}) = x - v + (y - w)\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$$

da $(\mathbb{Z}, +)$ eine Gruppe ist.

Zu 2): Seien wieder $x + y\sqrt{d}$ und $v + w\sqrt{d}$ zwei Elemente von $\mathbb{Z}[\sqrt{d}]$. Dann ist

$$(x+y\sqrt{d})*(v+w\sqrt{d}) = xv+xw\sqrt{d}+y\sqrt{d}v+y\sqrt{d}*w\sqrt{d} = (xv+ywd)+(xw+vy)\sqrt{d} \in \mathbb{Z}[\sqrt{d}].$$

Zu 3): $1+0\sqrt{d}$ ist das Einselement in $\mathbb{C}$, also ist $1+0\sqrt{d} = 1 \in \mathbb{Z}[\sqrt{d}]$ gesuchtes Element.

Teil b) Aufgabe 3 Teil c) können wir an dieser Stelle nicht direkt benutzen, da Domain und Wertebereich von φ nicht der Voraussetzung entsprechen. Da allerdings einige Schritte ähnlich sind, wird darauf verwiesen werden. Wir prüfen die geforderten Eigenschaften eines Ringhomomorphismus nach. Starten wir mit $\varphi(f) + \varphi(g) = \varphi(f + g)$ für $f, g \in \mathbb{Z}[t]$.
Seien also $f, g \in \mathbb{Z}[t]$. Dann

$$\varphi(f + g) = (f + g)(\sqrt{d}) = f(\sqrt{d}) + g(\sqrt{d}) = \varphi(f) + \varphi(g).$$

Die Gleichheiten ergeben sich analog zu Aufgabe 3 Teil c).
Als nächstes prüfen wir, ob $\varphi(f) * \varphi(g) = \varphi(f * g)$ ist. Seien dazu wieder $f, g \in \mathbb{Z}[t]$.

$$\varphi(f * g) = (f * g)(\sqrt{d}) = f(\sqrt{d}) * g(\sqrt{d}) = \varphi(f) * \varphi(g).$$

Die Gleichheiten ergeben sich wieder analog zu Aufgabe 3 Teil c).
Außerdem gilt $\varphi(1) = 1$, wodurch folgt, dass φ ein Ringhomomorphismus ist.
Nun gilt es, das Bild und den Kern von φ zu finden. Beginnen wir mit dem Bild.

Behauptung 6. $Im(\varphi) = \mathbb{Z}[\sqrt{d}]$

Beweis. $\supseteq$: Sei $a + b\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$. Somit ist also $f(t) := a + bt \in \mathbb{Z}[t]$ und $f(\sqrt{d}) = a + b\sqrt{d}$, wodurch also $a + b\sqrt{d} \in Im(\varphi)$.
$\subseteq$: Sei nun $x \in Im(\varphi)$. Dann $\exists f \in \mathbb{Z}[t] : f(\sqrt{d}) = x$. Insbesondere hat $f(\sqrt{d})$ folgende Form:

$$f(\sqrt{d}) = \sum_{i=0}^{n} a_i \sqrt{d}^i = \sum_{i \ gerade} a_i * d^{\frac{i}{2}} + \sum_{i \ ungerade} a_i \sqrt{d} * d^{\frac{i-1}{2}}$$

Da $\mathbb{Z}[\sqrt{d}]$ ein Ring ist, folgt $f(\sqrt{d}) \in \mathbb{Z}[\sqrt{d}]$. □

Behauptung 7. $Ker(\varphi) = (t^2 - d)$

Beweis. $\subseteq$: Sei $f \in Ker(\varphi)$. Dann können wir nach dem Satz über Division mit Rest von Polynomen f in folgender Form schreiben: $f = (t^2 - d) * q + r$ mit $q, r \in \mathbb{Z}[t]$. Außerdem gilt $grad(r) < 2$ und somit ist also $r = at + b$ für $a, b \in \mathbb{Z}$. Da aber $f(\sqrt{d}) = 0$ folgt $r = a * \sqrt{d} + b = 0$. Wegen $\sqrt{d} \notin \mathbb{Z}$ müssen sowohl a als auch b gleich 0 sein. Insgesamt haben wir, dass $f = (t^2 - d) * q$ mit $q \in \mathbb{Z}[t]$, was nach Definition genau $f \in (t^2 - d)$ bedeutet.
$\supseteq$: Sei $f \in (t^2 - d)$, also $f = (t^2 - d) * q$ mit $q \in \mathbb{Z}[t]$. Dann ist $f(\sqrt{d}) = 0 * q = 0$ und somit $f \in Ker(\varphi)$. □