Übung zu Algebraische und Geometrische Strukturen in der Mathematik, SoSe 2014

6. Übungsblatt

Aufgabe P17

Bestimmen Sie die Menge $\mathrm{Sym}(\{A, B, C\}) = \{f : \{A, B, C\} \to \{A, B, C\} \mid f \text{ bijektiv}\}$. Wenn Sie A, B, C als Ecken eines gleichseitigen Dreiecks im $\mathbb{R}^2$ auffassen, welche geometrische Interpretation haben die Elemente von $\mathrm{Sym}(\{A, B, C\})$?

Aufgabe P18

Zeigen Sie, dass es genau einen Ring-Automorphismus von $\mathbb{Q}$ gibt.

Hinweis: Zeigen Sie zunächst, dass es nur einen Automorphismus von $\mathbb{Z}$ gibt und benutzen Sie dann, dass $\mathbb{Q}$ der Quotientenkörper von $\mathbb{Z}$ ist.

Aufgabe P19

Sei $(G, \cdot)$ eine Gruppe und $x, g, h \in G$. Beweisen Sie die folgenden Identitäten:

1. Wenn $x \cdot g = h$, so gilt $x = h \cdot g^{-1}$. Wenn $g \cdot x = h$, so gilt $x = g^{-1} \cdot h$.
2. Es gilt $(g \cdot h)^{-1} = h^{-1} \cdot g^{-1}$ und $(g^{-1})^{-1} = g$.
3. Für beliebige $n, m \in \mathbb{N}$ gilt, dass $g^n \cdot g^m = g^{n+m} = g^m \cdot g^n$ und $(g^m)^n = g^{n \cdot m} = (g^n)^m$.
4. Für beliebiges $n \in \mathbb{N}$ gilt: Wenn $h \cdot g = g \cdot h$, so gilt $(h \cdot g)^n = h^n \cdot g^n$.

Hausübungen

Aufgabe H14 (4P)

Für $m \in \mathbb{N}_{>0}$ setzen wir $G_m := \{0, 1, ..., m-1\}$ und definieren

$$a * b := \text{ Rest von } a + b \text{ bei Division durch } m.$$

Zeigen Sie, dass G_m eine abelsche Gruppe ist, die isomorph zu $\mathbb{Z}_m$ ist.

Beachten Sie: Diese Aufgabe soll besonders das formal korrekte Aufschreiben üben. Dementsprechend können Sie nur die vollen Punkte für diese Aufgabe erhalten, wenn Ihre Lösung auch formal korrekt ist (das kann zum Beispiel auch heißen, die Assoziativität oder Kommutativität der Verknüpfung $*$ auf die entsprechende Eigenschaft einer bekannten Verknüpfung zurückzuführen; vergleichen Sie hierzu insbesondere die Lösungsskizze).

Bitte wenden!

Aufgabe H15 (4P)

Wenn R ein Ring ist, so bezeichne $\mathrm{Aut}(R)$ die Menge aller Ring-Automorphismen von R.

1. Zeigen Sie, dass für einen beliebigen Ring R die Menge $\mathrm{Aut}(R)$ zusammen mit der Verknüpfung

$$\circ : \mathrm{Aut}(R) \times \mathrm{Aut}(R) \to \mathrm{Aut}(R),\ (\varphi, \psi) \mapsto \varphi \circ \psi$$

   eine Gruppe bildet.

2. Sei k ein Körper. Zeigen Sie, dass es zu $a \in k \setminus \{0\}$ und $b \in k$ genau einen Automorphismus $\varphi_{a,b}$ von $k[X]$ gibt, sodass gilt:

$$\forall \lambda \in k: \quad \varphi_{a,b}(\lambda) = \lambda, \tag{1}$$

$$\varphi_{a,b}(X) = aX + b. \tag{2}$$

3. Sei k ein Körper und sei $\varphi \in \mathrm{Aut}(k[X])$ derartig, dass (1) gilt. Dann gibt es $a \in k \setminus \{0\}$ und $b \in k$, sodass (2) gilt.

4. Zeigen Sie, dass $(\mathrm{Aut}(\mathbb{Q}[X]), \circ)$ als Gruppe isomorph ist zu der Untergruppe

$$M := \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \mid a \in \mathbb{Q} \setminus \{0\}, b \in \mathbb{Q} \right\}$$

   von $\mathbb{Q}^{2\times 2}$.

   Hinweis: Verifizieren Sie, dass für jedes $\varphi \in \mathrm{Aut}(\mathbb{Q}[X])$ schon gilt, dass $\varphi|_{\mathbb{Q}} \in \mathrm{Aut}(\mathbb{Q})$. Verwenden Sie dann Aufgabe **P18**.

Bemerkung: Wie immer dürfen Sie frühere Aufgabenteile verwenden, um spätere Aufgabenteile zu lösen, selbst wenn sie erstere nicht gelöst haben.

Aufgabe H16 (4P)

Es sei k ein Körper. Für $s \in k$ setzen wir $k_s := \left\{ \begin{pmatrix} a & sb \\ b & a \end{pmatrix} \mid a, b \in k \right\}$.

1. Zeigen Sie, dass k_s für beliebiges $s \in k$ ein kommutativer Ring bezüglich der Addition und Multiplikation von 2×2-Matrizen ist. Zeigen Sie, dass k_s genau dann ein Körper ist, wenn für alle $x \in k$ gilt, dass $x^2 \neq s$.

   Hinweis: Erinnern Sie sich an den Zusammenhang zwischen der Invertierbarkeit einer Matrix und dem Wert ihrer Determinante.

2. Zeigen Sie, dass $\mathbb{R}_{-1}$ als Ring isomorph zu $\mathbb{C}$ ist.

3. Zeigen Sie, dass es für jede Primzahl $p > 2$ einen Körper mit genau p^2 Elementen gibt.

   Hinweis: Finden Sie eine Zahl $n < p$, sodass $(\mathbb{Z}/p\mathbb{Z})_{\overline{n}}$ ein Körper ist. Benutzen Sie hierfür Aufgabenteil 1 zusammen mit der Tatsache, dass $p - 1 \equiv -1 \pmod{p}$ und somit $(p-1)^2 \equiv 1 \pmod{p}$.