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

9. Übungsblatt – Lösungsskizze

Aufgabe P26

Es gilt
$$|X| = |X^G| + \sum_{i\in I}[G : G_{x_i}],$$
also
$$|X^G| = |X| - \sum_{i\in I}[G : G_{x_i}].$$
Da n jeden Summanden auf der rechten Seite nach Annahme teilt, mus n auch die linke Seite teilen.

Aufgabe P27

1. Es gilt $\mathrm{id} \in \mathrm{Gal}(k \subseteq E)$, da $\mathrm{id} \in \mathrm{Aut}(E)$ und $\mathrm{id}|_k = \mathrm{id}_k$. Falls $\lambda \in k$ und $\varphi, \psi \in \mathrm{Gal}(k \subseteq E)$, so gilt $\varphi(\psi(\lambda)) = \varphi(\lambda) = \lambda$, also ist auch $\varphi \circ \psi \in \mathrm{Gal}(k \subseteq E)$. Ebenso gilt für $\varphi \in \mathrm{Gal}(k \subseteq E)$ dass $\varphi^{-1}(\lambda) = \lambda$. Damit ist $\mathrm{Gal}(k \subseteq E)$ eine Untergruppen von $\mathrm{Aut}(E)$.

   Falls $x, y \in E$, $\lambda \in k$ und $\varphi \in \mathrm{Gal}(k \subseteq E)$ gilt, so haben wir
   $$\varphi(\lambda \cdot x + y) = \varphi(\lambda) \cdot \varphi(x) + \varphi(y) = \lambda \cdot \varphi(x) + \varphi(y).$$
   Also gilt $\varphi \in \mathrm{GL}(E)$ und $\mathrm{Gal}(k \subseteq E)$ ist eine Untergruppe von $\mathrm{GL}(E)$.

2. Es sei $p = \sum_{i=0}^n \lambda_i X^i$. Dann gilt
   $$p(\varphi(\alpha)) = \sum_{i=0}^n \lambda_i \varphi(\alpha)^i = \sum_{i=0}^n \varphi(\lambda_i)\varphi(\alpha^i) = \varphi\left(\sum_{i=0}^n \lambda_i \alpha^i\right) = 0,$$
   Da $\varphi(\lambda) = \lambda$ für alle $\lambda \in k$ gilt. Bezeichnet $\mathrm{NS}(p)$ die Menge der Nullstellen von p in E, so definiert folglich
   $$\mathrm{Gal}(k \subseteq E) \times \mathrm{NS}(p) \to \mathrm{NS}(p), (\varphi, \alpha) \mapsto \varphi.\alpha := \varphi(\alpha)$$
   eine Wirkung von $\mathrm{Gal}(k \subseteq E)$ auf $\mathrm{NS}(p)$.

Aufgabe P28

Es ist $\mathrm{Gal}(\mathbb{R} \subseteq \mathbb{C})$ eine Untergruppe von $\mathrm{GL}_2(\mathbb{R})$. Da alle Elemente von $\mathrm{Gal}(\mathbb{R} \subseteq \mathbb{C})$ die x-Achse (welche gerade $\mathbb{R}$ als Teilmenge von $\mathbb{C}$ entspricht) fixieren müssen, gilt
$$\mathrm{Gal}(\mathbb{R} \subseteq \mathbb{C}) \leq \left\{ \begin{pmatrix} 1 & a \\ 0 & b \end{pmatrix} \mid a \in \mathbb{R}, b \in \mathbb{R} \setminus \{0\} \right\}.$$
Da wir für $\varphi \in \mathrm{Gal}(\mathbb{R} \subseteq \mathbb{C})$
$$\varphi(i)^2 = \varphi(i^2) = \varphi(-1) = -1$$

haben muss i von jedem Element $\varphi \in \mathrm{Gal}(\mathbb{R} \subseteq \mathbb{C})$ entweder auf i oder auf $-i$ abgebildet werden. Also kann φ nur aus der Menge

$$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \right\} \tag{1}$$

sein. Andererseits definiert jedes Element aus (1) ein Element aus $\mathrm{Gal}(\mathbb{R} \subseteq \mathbb{C})$, wir haben also

$$\mathrm{Gal}(\mathbb{R} \subseteq \mathbb{C}) = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \right\} \cong \mathbb{Z}_2$$

Dass $\mathrm{Gal}(\mathbb{R} \subseteq \mathbb{C})$ gerade aus der Identität und der komplexen Konjugation besteht heißt für ein Polynom mit reellen Koeffizienten gerade, dass die komplexen und nicht-reellen Nullstellen gerade in Paaren aus konjugierten komplexen Zahlen auftreten müssen.

Aufgabe H23

1. Da $G^{(n+1)}$ die Kommutatorgruppe von $G^{(n)}$ ist reicht es aus, für eine abstrakte Gruppe H zu zeigen, dann H' eine normale Untergruppe von H ist. Dazu sei ein Produkt von Kommutatoren

$$[a_1, b_1] \cdot ... \cdot [a_k, b_k],$$

also eine Element aus H' gegeben und $h \in H$. Da $h \cdot [a, b] \cdot h^{-1} = [h \cdot a \cdot h^{-1}, h \cdot b \cdot h^{-1}]$ gilt somit

$$h \cdot [a_1, b_1] \cdot ... \cdot [a_k, b_k] \cdot h^{-1} = h \cdot [a_1, b_1] \cdot h^{-1} \cdot ... \cdot h \cdot [a_k, b_k] \cdot h^{-1} = \\ [h \cdot a_1 \cdot h^{-1}, h \cdot b \cdot h^{-1}] \cdot ... \cdot [h \cdot a_k \cdot h^{-1}, h \cdot b_k \cdot h^{-1}].$$

Damit ist $h \cdot [a_1, b_1] \cdot ... \cdot [a_k, b_k] \cdot h^{-1}$ wieder ein Produkt von Kommutatoren, also in H'.

2. Ist $H \leq G$ eine Untergruppe, so gilt $H' \leq G'$ und induktiv $H^{(n)} \leq G^{(n)}$. Gilt also $G^{(n)} = \{e\}$ für ein $n \in \mathbb{N}_{>0}$, so auch $H^{(n)} = \{e\}$ und H ist auflösbar.

3. Es gilt $[gN, hN] = [g, h]N$, also $(G/N)' \subseteq (G')N := \{gN \mid g \in G'\}$. Induktiv erhalten wir also $(G/N)^{(n)} \subseteq G^{(n)}N$. Also folgt $(G/N)^n = N$ aus $G^{(n)} = \{e\}$. Somit ist G/N auflösbar falls G auflösbar ist.

Aufgabe H24

1. Anhand der Matrix-Multiplikation sieht man sofort, dass die Strikten oberen Dreiecksmatrizen abgeschlossen sind unter Multiplikation. Bestimmt man das Inverse einer Matrix mit der Cramerschen Regel, so sieht man, dass das Inverse einer strikten unteren Dreiecksmatrix wieder eine strikte untere Dreiecksmatrix ist. Also ist H_3 auch abgeschlossen unter Inversenbildung, also eine Untergruppe.

2. H_3 nicht nist normal, da die Konjugation von

$$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

mit der Transpositionsmatrix

$$\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

keine obere Dreiecksmatrix mehr ist.

3. Es gilt

$$\begin{pmatrix} 1 & a & x \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & c & y \\ 0 & 1 & d \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a+c & x+y+ad+cb \\ 0 & 1 & b+d \\ 0 & 0 & 1. \end{pmatrix} \tag{2}$$

Daran sieht man, dass

$$\begin{pmatrix} 1 & a & x \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & y \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a & x+y \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & y \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & a & x \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix},$$

also

$$\begin{pmatrix} 1 & 0 & y \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \in Z(H_3)$$

für alle $x \in k$. Für

$$A = \begin{pmatrix} 1 & a & x \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix}$$

mit $a \neq 0$ oder $b \neq 0$ konstruiert man mit (2) leicht eine Matrix, die nicht mit A kommutiert, also ist A nicht in $Z(H_3)$. Damit gilt

$$Z(H_3) = \left\{ \begin{pmatrix} 1 & 0 & x \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \mid x \in k \right\}.$$

Da $Z(H_3) \neq H_3$ ist H_3 nicht abelsch.

4. Multipliziert man eine Matrix aus H_3 mit e_2, so ist der zweite Eintrag in dem Ergebnis immer gleich 1 und der letzte Eintrag immer gleich Null. Für ein beliebiges $\lambda \in k$ gilt außerdem, dass

$$\begin{pmatrix} 1 & \lambda & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \lambda \\ 1 \\ 0 \end{pmatrix},$$

also liegt jeder Vektor $\begin{pmatrix} \lambda \\ 1 \\ 0 \end{pmatrix}$ ind er Bahn von e_2. Damit gilt

$$H_3.e_2 = \left\{ \begin{pmatrix} \lambda \\ 1 \\ 0 \end{pmatrix} \mid \lambda \in k \right\}.$$

Da eine Bahn existiert, die ungleich k^3 ist kann die Wirkung nicht transitiv sein (im Fall einer transitiven Wirkung würde nur genau eine Bahn existieren). Soll $A.e_2 = e_2$ für ein A aus H_3 gelten, so muss A die form

$$A = \begin{pmatrix} 1 & 0 & x \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix}$$

haben. Also gilt

$$(H_3)_{e_2} = \left\{ \begin{pmatrix} 1 & 0 & x \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \mid b, x \in k \right\}.$$

5. Aus (2) folgt, dass

$$\begin{pmatrix} 1 & a & x \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & -a & -x + 2ab \\ 0 & 1 & -b \\ 0 & 0 & 1 \end{pmatrix},$$

und somit $[A, B] \in Z(H_3)$ für $A, B \in H_3$, da sich alle Einträge auf der ersten Nebendiagonalen gerade wegheben. Ferner sieht man direkt, dass man ein beliebiges Element aus $Z(H_3)$ als Kommutator darstellen kann. Also Gilt $H_3' = Z(H_3)$. Da $Z(H_3)$ abelsch ist gilt $(Z(H_3))' = \{e\}$, mit e der Einheitsmatrix. Also ist $(H_3)^n = \{e\}$ für alle $n > 1$. Insbesondere ist H_3 auflösbar.