F15T2A4 Sei Ω eine Menge mit $|\Omega| > 1$ und G eine Gruppe, die auf Ω transitiv operiert.

(a) Zeigen Sie: Besitzt jedes Element $g \in G$ einen Fixpunkt bzgl. der Operation (d.h. gibt es jeweils ein $x \in \Omega$ mit $g \cdot x = x$), dann existiert eine echte Untergruppe U von G mit $G = \bigcup_{g \in G} gUg^{-1}$, d.h. G ist Vereinigung der Konjugierten der Untergruppe U.

(Normalerweise bezeichnet man als Fixpunktmenge

(

=

Au

g

Ve

(b)

das

G =

(Hin

(Normalerweise bezeichnet man als Fixpunktmenge einer Gruppenoperation $\circ$ die Menge $F=\{x\in X \mid g\circ x = x \ \forall g\in G\}$.)

Sei $x\in\Omega$ beliebig gewählt und $U=G_x$.

Beh: (1) $U \subsetneq G_x$ (2) $G = \bigcup_{h\in G} hUh^{-1}$

<u>zu (1)</u> Ang es gilt $G_x = G \Rightarrow \forall g\in G: g\circ x = x$

$\Rightarrow G(x) = \{g\circ x \mid g\in G\} = \{x\} \overset{|\Omega|>1}{\Longrightarrow}$

$\Rightarrow G(x) \subsetneq \Omega$ Aber weil G auf Ω transitiv operiert, muss $G(x)=\Omega$ gelten. $\lightning$

zu (2) „$\supseteq$" ist offensichtlich, weil hUh^{-1} für jedes $h \in G$ eine Teilmenge von G ist

„$\subseteq$" Sei $g \in G$. Nach Voraussetzung besitzt g einen Fixpunkt, d.h. es gibt ein $y \in \Omega$ mit $g \circ y = y$.
Da die Operation transitiv ist, gilt $G(x) = \Omega$ und $y \in G(x)$, d.h. es gibt ein $h \in G$ mit $h \circ x = y$.
Beh.: $g \in hUh^{-1}$ überprüfe zunächst:
$h^{-1}gh \in U$, äquivalent: $h^{-1}gh \in G_x$. Um dies zu überprüfen, muss $(h^{-1}gh) \circ x = x$ gezeigt werden

$$(h^{-1}gh)\circ x = h^{-1}\circ(g\circ(h\circ x)) = h^{-1}\circ(g\circ y)$$
$$= h^{-1}\circ y = h^{-1}\circ(h\circ x) = (h^{-1}h)\circ x = e\circ x = x$$

Aus der Tatsache, dass $u = h^{-1}gh$ in U liegt, folgt $g = huh^{-1} \in hUh^{-1}$. Insbesondere liegt g in der Vereinigung $\bigcup_{h\in G} hUh^{-1}$.

(b) Sei $n \in \mathbb{N}$ mit $n > 1$ und $G = GL_n(\mathbb{C})$. Zeigen Sie, dass G eine echte Untergruppe U mit der Eigenschaft $G = \bigcup_{A\in G} AUA^{-1}$ besitzt.

(Hinweis: Operation von G auf der Menge der 1-dim Untervektorräume von $\mathbb{C}^n$.)

… hUh^{-1} für jedes

Sei $\mathcal{U}$ die Menge der 1-dimensionalen Untervektorräume von $\mathbb{C}^n$. Für jedes $A \in G$ und $U \in \mathcal{U}$ sei $A(U) = \{Au \mid u \in U\}$. Als Bild von U unter der linearen Abb. $\mathbb{C}^n \to \mathbb{C}^n$, $u \mapsto Au$ ist U ein Untervektorraum des $\mathbb{C}^n$. Da A invertierbar ist, ist diese lineare Abb., die wir mit ϕ_A bezeichnen, bijektiv, und $\phi_A|U$ ist injektiv, d.h. $\ker(\phi_A|U) = \{0_{\mathbb{C}^n}\}$. Die Anwendung des Dimensionssatzes für lineare Abb. auf $\phi_A|U$ liefert

E

A

{A

Um

wir

(4)

(5)

Ist die

Unterg

schaft

zu (3)

$\dim \ker(\phi_A|_U) + \dim \operatorname{im}(\phi_A|_U) = \dim U$
$= 1 \Rightarrow \dim A(U) = \dim \operatorname{im}(\phi_A|_U) =$
$1 - \ker(\phi_A|_U) = 1 - \dim\{0_{\mathbb{C}^n}\} = 1 - 0 = 1$

Also ist $A(U)$ wiederum ein Element von $\mathcal{U}$.

Betrachte nun die Abbildung

$$\circ : G \times \mathcal{U} \to \mathcal{U}, \quad (A, U) \mapsto A(U)$$

Um zu zeigen, dass $\circ$ die Gruppenoperation ist, müssen wir überprüfen

(1) $E \circ U \;\forall U \in \mathcal{U}$ (2) $A \circ B \circ U = (AB) \circ U \;\forall A, B \in G, U \in \mathcal{U}$

Seien also $A, B \in G$ und $U \in \mathcal{U}$ vorgeg.

sc
$e_1,$
vek
zu (
„$\subseteq$"
„$\supseteq$"
$A \circ ($
gewäh
Wegen
$u_2, \dots,$
Sei A d
Auf Gru
$G = GL_n$

...an
...des
$\{Au\,|$
linearen
ein Un-
inver-
...b., die
...ktiv,
$\ker(\varphi_A|U)$
Dimensions-
$\ldots A|U$ liefert

$$E \circ U = \{Eu \mid u \in U\} = \{u \mid u \in U\} = U$$

$$A \circ (B \circ U) = \{Av \mid v \in B \circ U\} =$$

$$\{A(Bu) \mid u \in U\} = \{(AB)u \mid u \in U\} = (AB)(U)$$

Um Teil (a) anwenden zu können, überprüfen wir (3) $|\mathcal{U}| > 1$

(4) Die Operation $\circ$ ist transitiv.

(5) Jedes $A \in G$ besitzt einen Fixpunkt bezüglich der Operation.

Ist dies gezeigt, dann liefert Teil (a) eine Untergruppe von G mit der gewünschten Eigenschaft.

<u>zu (3)</u> klar, da $\mathbb{C}e_1$, $\mathbb{C}e_2$ z.B. zwei ver-

schiedene Elemente von $\mathcal{U}$ sind (wobei $e_1, e_2 \in \mathbb{C}$ den ersten bzw. zweiten Einheitsvektor bezeichnet)

<u>zu (4)</u> zeige: $G(\mathbb{C}e_1) = \mathcal{U}$

„$\subseteq$" ist nach Def. der Bahn offensichtlich

„$\supseteq$" Sei $U \in \mathcal{U}$ z.zg.: $\exists A \in G$ mit $A \cdot (\mathbb{C}e_1) = U$. Sei $u \in U \setminus \{0_{\mathbb{C}^n}\}$ beliebig gewählt. Wegen $\dim U = 1$ gilt $U = \mathbb{C}u$. Wegen $u \neq 0_{\mathbb{C}^n}$ können wir u durch Vektoren $u_2, \dots, u_n$ zu einer Basis des $\mathbb{C}^n$ ergänzen. Sei A die Matrix mit $u, u_2, \dots, u_n$ als Spalten. Auf Grund der Basiseigenschaft liegt A in $G = GL_n(\mathbb{C})$, und es gilt $A e_1 = u$.

Daraus folgt $A \cdot (\mathbb{C}e_1) = \{Au \mid u \in \mathbb{C}e_1\} =$
$\{A(\lambda e_1) \mid \lambda \in \mathbb{C}\} = \{\lambda(Ae_1) \mid \lambda \in \mathbb{C}\} = \{\lambda u \mid \lambda \in \mathbb{C}\}$
$= \mathbb{C}u = U$.

<u>zu (5)</u> Sei $A \in G$. Da $\mathbb{C}$ algebraisch abg. ist, besitzt das char. Pol. $\chi_A \in \mathbb{C}[x]$ eine Nullstelle $\alpha \in \mathbb{C}$. Da A invertierbar ist, gilt $\alpha \neq 0$. Sei u ein Eigenvektor von A zum Eigenwert α und $U = \mathbb{C}u$. <u>Beh.</u>: U ist Fixpunkt von A

$$A \cdot U = \{Av \mid v \in U\} = \{A\lambda u \mid \lambda \in \mathbb{C}\} =$$
$$\{\lambda(Au) \mid \lambda \in \mathbb{C}\} = \{\lambda(\alpha u) \mid \lambda \in \mathbb{C}\} \overset{\alpha \neq 0}{=} \{\lambda u \mid \lambda \in \mathbb{C}\}$$
$$= \mathbb{C}u = U. \qquad \square$$

ch
G
ine
Sylow-

ist, gilt $\alpha \neq 0$. Sei u ein Eigenvektor von A zum Eigenwert α und $U = \mathbb{C}u$. Beh.: U ist Fixpunkt von A

<u>Aufgabe</u> Sei K ein Körper, $n \in \mathbb{N}$ und $\mathcal{U}$ die Menge der Untervektorräume des K^n

(a) Zeigen Sie, dass eine Abb. $\circ : G \times \mathcal{U} \to \mathcal{U}$ existiert mit $A \circ U = \phi_A(U)$ $\forall A \in G, U \in \mathcal{U}$, wobei $G = GL_n(K)$ ist und $\phi_A : K^n \to K^n$ die lineare Abbildung $v \mapsto Av$ bezeichnet.

(b) Weisen Sie nach, dass $\circ$ eine Gruppenoperation von G auf $\mathcal{U}$ definiert.

(c) Zeigen Sie, dass es bzgl. der Operation genau $n+1$ Bahnen gibt.

Sylowsätze

Def. Sei G eine endliche Gruppe, p eine Primzahl, und seien $r \in \mathbb{N}_0$ und $m \in \mathbb{N}$ definiert durch $|G| = p^r m$ und $p \nmid m$. Eine Untergruppe U von G heißt

(i) p-Untergruppe, falls $|U| = p^s$ für ein $s \in \{0, 1, \dots, r\}$

(ii) p-Sylowgruppe, wenn $|U| = p^r$ gilt.

Erinnerung:

- Durch $\circ : G \times \mathcal{P} \to \mathcal{P}$, $g \mapsto gPg^{-1}$ ist eine Operation von G auf der Menge $\mathcal{P}$ der p-Sylow-

Da

$\{A$

$= ($

zu (5)

char.

ist,

und (

$A \cdot U$

$\{\lambda(A$

$= C$

ein $s \in \{0, 1, \dots, r\}$

(ii) <u>p-Sylowgruppe</u>, wenn $|U| = p^r$ gilt.

ist

und

gruppen von G definiert.

- Diese Operation ist transitiv, d.h. $G(P) = \mathcal{P}$ $\forall P \in \mathcal{P}$ (Zweiter Sylowsatz).
- Für jedes $P \in \mathcal{P}$ ist der <u>Normalisator</u> $N_G(P) = \{g \in G \mid gPg^{-1} = P\}$ der Stabilisator von P bzgl. dieser Operation.
- Aus dem Zusammenhang $(G : G_x) = |G(x)|$ für beliebige Gruppenoperationen folgt
$$(G : N_G(P)) = \nu_p \quad \forall P \in \mathcal{P},$$
wobei ν_p die Anzahl der p-Sylowgr. in G bezeichnet.

Au

M

(a)

(b)

(c)

<u>F25T1A1</u> Sei p eine Primzahl und $G = GL_2(\mathbb{F}_p)$. bereits erledigt:

(a) gezeigt: $|G| = p(p-1)^2(p+1)$

(b) Ordnung von $\begin{pmatrix} \bar{1} & \bar{1} \\ \bar{0} & \bar{1} \end{pmatrix}$ in G: p

noch zu bearbeiten:

(c) Es gibt mehr als eine p-Sylowgruppe.

(d) Sei $p = 3$ und $H = \left\langle \begin{pmatrix} \bar{1} & \bar{1} \\ \bar{0} & \bar{1} \end{pmatrix} \right\rangle$.
Zeigen Sie, dass der Normalisator von H genau aus den oberen Dreiecksmatrizen besteht. Zeigen Sie damit, dass die Anzahl ν_3 der 3-Sylowgruppen gleich 4 ist.

<u>zu (c)</u>

$|H|$

teiler

H ein

Sei B

Für $k=$

wzF es

$B^{k+1} =$

für $k+$

k mit $\bar{k}$

$\Rightarrow$ ord (

eine von

...l und
...gt:
...+1)
...p

...Sylowgruppe.
...$\begin{pmatrix} \bar1 & \bar1 \\ \bar0 & \bar1 \end{pmatrix}\Big) \Big\rangle$.
...rator von H
...esmatrizen
...dass die An-
...gleich 4 ist.

<u>zu (c)</u> Sei $H = \left\langle \begin{pmatrix} \bar1 & \bar1 \\ \bar0 & \bar1 \end{pmatrix} \right\rangle$. Dann gilt $|H| = \mathrm{ord}\left(\begin{pmatrix} \bar1 & \bar1 \\ \bar0 & \bar1 \end{pmatrix}\right) \overset{(b)}{=} p$. Weil $m = (p-1)^2(p+1)$ teilerfremd zu p ist, folgt aus Teil (a), dass H eine p-Sylowgruppe von G ist.

Sei $B = \begin{pmatrix} \bar1 & \bar0 \\ \bar1 & \bar1 \end{pmatrix}$. <u>Beh</u>: $B^k = \begin{pmatrix} \bar1 & \bar0 \\ \bar k & \bar1 \end{pmatrix}\ \forall k \in \mathbb{N}_0$

Für $k = 0$ ist das offensichtlich erfüllt, und setzen wir es für ein $k \in \mathbb{N}_0$ voraus, dann ist es wegen

$$B^{k+1} = B^k \cdot B = \begin{pmatrix} 1 & 0 \\ k & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ \overline{k+1} & 1 \end{pmatrix}$$

auch für $k+1$ erfüllt. Weil p die minimale nat. Zahl k mit $\bar k = \bar0$ ist, ist p auch minimal mit $B^k = E$.

$\Rightarrow \mathrm{ord}(B) = p \Rightarrow |\langle B\rangle| = p$. Also ist $\langle B \rangle$ eine von H verschiedene p-Sylowgruppe in G.