F25T2A5 (Rest)

p Primzahl, $G = \left\{ \begin{pmatrix} a & 0 \\ b & a \end{pmatrix} \mid a \in \mathbb{F}_p^*, b \in \mathbb{F}_p \right\}$

bereits erledigt: (a) $G \leq GL_2(\mathbb{F}_p)$

(b) gezeigt: $H_p = \left\{ \begin{pmatrix} 1 & 0 \\ b & 1 \end{pmatrix} \mid b \in \mathbb{F}_p \right\}$

und $H_{p-1} = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \mid a \in \mathbb{F}_p^* \right\}$ sind zykl. Untergruppen von G, von Ordnung p bzw. $p-1$

zu (c) z.zg.: G ist zyklisch

Beh.: G ist inneres direktes Produkt von

H_{p-1} und H_p

dafür zu überprüfen: i) $H_p, H_{p-1} \trianglelefteq G$

ii) $H_{p-1} \cap H_p = \{E\}$ (iii) $G = H_p H_{p-1}$

zu i) Sei $\begin{pmatrix} \bar{1} & \bar{0} \\ b & \bar{1} \end{pmatrix} \in H_p$, mit $b \in \mathbb{F}_p$ und

$\begin{pmatrix} a & \bar{0} \\ c & a \end{pmatrix} \in G$, mit $a \in \mathbb{F}_p^*$, $c \in \mathbb{F}_p$.

z.zg.: $\begin{pmatrix} a & \bar{0} \\ c & a \end{pmatrix}\begin{pmatrix} \bar{1} & \bar{0} \\ b & \bar{1} \end{pmatrix}\begin{pmatrix} a & \bar{0} \\ c & a \end{pmatrix}^{-1} \in H_p$

$\begin{pmatrix} a & \bar{0} \\ c & a \end{pmatrix}\begin{pmatrix} \bar{1} & \bar{0} \\ b & \bar{1} \end{pmatrix}\begin{pmatrix} a & \bar{0} \\ c & a \end{pmatrix}^{-1} = \begin{pmatrix} a & \bar{0} \\ c+ab & a \end{pmatrix}\begin{pmatrix} a & \bar{0} \\ c & a \end{pmatrix}^{-1} =$

Da

$$\begin{pmatrix} a & \bar{0} \\ c+ab & a \end{pmatrix}\begin{pmatrix} a^{-1} & \bar{0} \\ -ac & a^{-1} \end{pmatrix} = \begin{pmatrix} \bar{1} & \bar{0} \\ b & \bar{1} \end{pmatrix} \in H_p$$

Sei $\begin{pmatrix} a & \bar{0} \\ \bar{0} & a \end{pmatrix} \in H_{p-1}$ und $\begin{pmatrix} d & \bar{0} \\ c & d \end{pmatrix} \in G$, mit $a, d \in \mathbb{F}_p^*$, $c \in \mathbb{F}_p$.

$$\begin{pmatrix} d & \bar{0} \\ c & d \end{pmatrix}\begin{pmatrix} a & \bar{0} \\ \bar{0} & a \end{pmatrix}\begin{pmatrix} d & \bar{0} \\ c & d \end{pmatrix}^{-1} = \begin{pmatrix} ad & \bar{0} \\ ac & ad \end{pmatrix}\begin{pmatrix} d^{-1} & \bar{0} \\ -d^{-2}c & d^{-1} \end{pmatrix} = \begin{pmatrix} a & \bar{0} \\ \bar{0} & a \end{pmatrix} \in H_{p-1}$$

zu (ii) $\Leftarrow$ gilt $\operatorname{ggT}(p-1, p) = 1$. Aus der Teilerfremdheit von $|H_{p-1}|$ und $|H_p|$ folgt $H_{p-1} \cap H_p = \{E\}$.

zu (iii) Wegen $H_p, H_{p-1} \trianglelefteq G$ ist $H_p H_{p-1}$ eine Untergr. von G, sogar Normalteiler. $H_p \subseteq H_p H_{p-1} \overset{\text{Lagrange}}{\Longrightarrow}$ p teilt $|H_p H_{p-1}|$

$H_{p-1} \subseteq H_p H_{p-1} \overset{\text{Lagrange}}{\Longrightarrow}$ $(p-1)$ teilt $|H_p H_{p-1}|$

$ggT(p, p-1) = 1 \Rightarrow p(p-1)$ teilt $|H_p H_{p-1}| \Rightarrow$

$|H_p H_{p-1}| \geq p(p-1) = |G|$ $\overset{H_p H_{p-1} \leq G}{\Longrightarrow}$ $G = H_p H_{p-1}$ ($\Rightarrow$ Beh)

Aus der Beh. folgt $G \cong H_p \times H_{p-1} \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/(p-1)\mathbb{Z}$
$\uparrow$ H_p, H_{p-1} zyklisch

$\cong \mathbb{Z}/p(p-1)\mathbb{Z}$
$\uparrow$ $ggT(p, p-1) = 1$
Chin. Restsatz

Also ist G zyklisch. $\square$

Gruppenoperationen

Def. Sei G eine Gruppe und X eine Menge.
Operation von G auf X = Abbildung $\circ : G \times X \to X$ mit
(i) $e \circ x = x \quad \forall x \in X$ (ii) $g \circ (h \circ x) = (gh) \circ x \quad \forall g, h \in G \; \forall x \in X$

wichtige Beispiele für Gruppenoperationen:

(1) $n \in \mathbb{N}$, $G = S_n$, $X = M_n = \{1, \dots, n\}$

$\cdot : S_n \times M_n \to M_n$ definiert durch

$\sigma \cdot k = \sigma(k) \quad \forall \sigma \in S_n, k \in M_n$

(2) $G = GL_n(K)$, $X = K^n$ (K Körper, $n \in \mathbb{N}$)

$\cdot : GL_n(K) \times K^n \to K^n$ ist definiert durch

$A \cdot v = Av \quad \forall A \in GL_n(K), v \in K^n$

(3) Jede Gruppe G operiert auf der Menge ihrer Elemente durch

$\cdot : G \times G \to G, (g, h) \to gh$

(Operation durch Linkstranslation,

(Op

Syl

Def

i) Für

die

ii) Die

des S

wichtige

(1) Die

(Gibt es

dann wird

Anwendung: Satz von Cayley

(4) Jede Gruppe G operiert auf G auch durch $\circ : G \times G \to G, (g,h) \mapsto ghg^{-1}$
(Operation durch Konjugation: Klassengleichung, Gruppen von Primzahlquadratordnung sind abelsch, Gruppen von Primzahlpotenzordnung sind auflösbar, Satz von Sylowsatz, Lemma von Cauchy)

(5) Ist G eine Gruppe und p eine Primzahl, dann operiert G auf der Menge P ihrer p-Sylowgruppen durch
$\circ : G \times P \to P, (g,P) \mapsto gPg^{-1}$.

(2)

(3)

wob
bezei
Bahn
(nicht

F25T

Primt
der El

(a) Ze
(La

(Operation durch Konjugation, Anwendung: Sylowsätze)

Def: G Gruppe, X Menge, $\circ : G \times X \to X$ Gruppenoperation

i) Für jedes $x \in X$ heißt $G(x) = \{g \circ x \mid g \in G\}$ die Bahn von x unter der Operation

iii) Die Untergr. $G_x = \{g \in G \mid g \circ x = x\}$ wird der Stabilisator von x genannt.

wichtige Regeln:

(1) Die Bahnen bilden eine Zerlegung von X.
(Gibt es nur eine Bahn, d.h. $G(x) = X \ \forall x \in X$, dann wird die Operation transitiv genannt.)

(2) Ist G endlich oder X endlich, dann gilt

$$|G(x)| = (G : G_x) \quad \forall x \in X.$$

(3) Bahngleichung: $|X| = |F| + \sum_{x \in R} (G : G_x)$

wobei F die Fixpunktmenge der Operation bezeichnet und R ein Repräsentantensystem der Bahnen mit mehr als einem Element.

(wichtiger Spezialfall: Klassengleichung)

F25T1A4 Sei G eine endl. Gruppe, p ein Primteiler der Gruppenordnung und M die Menge der Elemente der Ordnung p in G.

(a) Zeigen Sie, dass $\mathbb{F}_p^\times \times M \to M$, $([a], g) \mapsto g^a$ eine Gruppenoperation definiert.

Zeige zunächst: Es existiert eine Abb. $\phi : \mathbb{F}_p \times M \to G$
mit (*) $\phi([a], g) = g^a \quad \forall a \in \mathbb{Z}, g \in M$.

Jedes Element aus $\mathbb{F}_p$ hat eine eindeutige Darstellung
der Form $[r] = r + p\mathbb{Z}$ mit $0 \leq r \leq p-1$. Definiere
ϕ durch $\phi([r], g) = g^r \quad \forall r \in \{0, \ldots, p-1\}, g \in M$.

z.zg.: (*) ist erfüllt für alle $a \in \mathbb{Z}, g \in M$

Seien also $a \in \mathbb{Z}, g \in M$ beliebig. Division mit Rest $\Rightarrow$
$\exists q, r \in \mathbb{Z}$ mit $a = qp + r$, $0 \leq r \leq p-1$. und $|g| = p$

$\Rightarrow g^p = e \Rightarrow g^a = g^{qp+r} = (g^p)^q \cdot g^r = e^q \cdot g^r = g^r$

$\Rightarrow \phi([a], g) = \phi([r], g) = g^r = g^a$

Definiere nun $\circ : \mathbb{F}_p^* \times M \to G$ durch $([a], g) \mapsto \phi([a], g)$

$\forall\, [a] \in \mathbb{F}_p^*$ (mit $a \in \mathbb{Z}$, $p \nmid a$) und $g \in M$ (**)

noch zu überprüfen: (1) $[1] \circ g = g \;\forall g \in M$

(2) $[a] \circ ([b] \circ g) = ([a] \cdot [b]) \circ g$

$\forall\, [a], [b] \in \mathbb{F}_p^*$ und $g \in M$

Seien also $[a], [b] \in \mathbb{F}_p^*$ (mit $a, b \in \mathbb{Z}$, $p \nmid a$, $p \nmid b$)

und $g \in M$. zu (1) $[1] \circ g = g^1 = g$

zu (2) $[a] \circ ([b] \circ g) = [a] \circ (g^b) = (g^b)^a = g^{ab}$

$= [ab] \circ g \overset{(\Delta)}{=} ([a] \cdot [b]) \circ g \overset{(\Delta)}{(ab + p\mathbb{Z} = (a + p\mathbb{Z})(b + p\mathbb{Z}))}$

(**) Dies ist eine Abbildung nach M, denn: Aus $p \nmid a$ folgt $ggT(a,p) = 1$, und daraus folgt, dass mit g auch g^a ein Element der Ordnung p ist, also in M liegt.

(b) Zeigen Sie, dass für jedes $g \in M$ die Stabilisatorgruppe $(\mathbb{F}_p^\times)_g$ trivial ist.

Sei $g \in M$. z.Zg.: $(\mathbb{F}_p^\times)_g = \{[1]\}$

„$\supseteq$" Es ist $(\mathbb{F}_p^\times)_g$ eine Untergruppe von $\mathbb{F}_p^\times$, und diese enthält das Neutralele-

ment $[1]$ von $\mathbb{F}_p^\times$.

„$\subseteq$" Sei $[a] \in (\mathbb{F}_p^\times)_g$, mit $a \in \mathbb{Z}$, $p \nmid a$.

$[a] \in (\mathbb{F}_p^\times)_g \Rightarrow [a] \cdot g = g \Rightarrow g^a = g$

$\Rightarrow g^{a-1} = e \overset{\text{ord}(g)=p}{\Rightarrow} p \mid (a-1) \Rightarrow$

$a \equiv 1 \bmod p \Rightarrow [a] = [1] \Rightarrow [a] \in \{[1]\}$

zu (c) zeige: $|M|$ ist Vielfaches von $p-1$

Laut Vl. ist für jedes $g \in G$ die Bahnlänge der Index des Stabilisators $\Rightarrow |\mathbb{F}_p^\times(g)| =$

$(\mathbb{F}_p^\times : (\mathbb{F}_p^\times)_g) = \dfrac{|\mathbb{F}_p^\times|}{|(\mathbb{F}_p^\times)_g|} \overset{(6)}{=} |\mathbb{F}_p^\times| = p-1$

Da die Bahnen eine Zerlegung von M bilden,

- folgt $|M| = d \cdot (p-1)$, wobei $d \in \mathbb{N}$ die Anzahl der Bahnen der Operation angibt.

(Bem.: Die Zahl d gibt die Anzahl der (zyklischen) Untergruppen der Ordnung p von G an.)