

16. Ein wenig über die Struktur von Gruppen

Satz 121: Es sei p eine Primzahl und G eine Gruppe der Ordnung $|G| = p$. Dann ist G zyklisch und daher $G \cong \mathbb{Z}_p$.

Beweis: Ist $a \in G \setminus \{e\}$, so gilt $\text{ord}(a) \mid |G|$, d.h. $\text{ord}(a) \mid p$ und daher $\text{ord}(a) \in \{1, p\}$. Da $\text{ord}(a) = 1$ nicht möglich ist, gilt $\text{ord}(a) = p$. Daher ist $G = \{e, a, a^2, \dots, a^{p-1}\} = \langle a \rangle$ zyklisch und $G \cong \mathbb{Z}_p$ wegen Satz 36 (ii).

Bemerkung: Satz 121 wurde bereits in Übungsbeispiel 46 bewiesen und wird hier der Vollständigkeit halber noch einmal gebracht.

Lemma 122: Ist G eine Gruppe und $G/Z(G)$ zyklisch, so ist G abelsch.

Beweis: Da $G/Z(G)$ zyklisch ist, gibt es ein $a \in G$, sodass

$$G/Z(G) = \langle aZ(G) \rangle = \{a^k Z(G) \mid k \in \mathbb{Z}\}.$$

Sind nun $x, y \in G$, so gibt es $k, \ell \in \mathbb{Z}$, derart dass $xZ(G) = a^k Z(G)$ und $yZ(G) = a^\ell Z(G)$. Also gibt es $u, v \in Z(G)$, sodass $x = a^k u$ und $y = a^\ell v$. Daraus folgt

$$xy = a^k u a^\ell v = a^k a^\ell u v = a^{k+\ell} v u = a^\ell a^k v u = a^\ell v a^k u = yx.$$

Satz 123: Es sei p eine Primzahl und G eine Gruppe der Ordnung $|G| = p^2$. Dann ist G abelsch und daher $G \cong \mathbb{Z}_{p^2}$ oder $G \cong \mathbb{Z}_p \times \mathbb{Z}_p$.

Beweis: Aus $Z(G) \leq G$ folgt $|Z(G)| \mid |G|$ bzw. $|Z(G)| \mid p^2$. Daher muss $|Z(G)| \in \{1, p, p^2\}$ gelten. Aus Korollar 114 folgt $p \mid |Z(G)|$ und daher $|Z(G)| \in \{p, p^2\}$. Wäre $|Z(G)| = p$, so würde

$$|G/Z(G)| = \frac{|G|}{|Z(G)|} = \frac{p^2}{p} = p$$

gelten. Dann wäre nach Satz 121 $G/Z(G) \cong \mathbb{Z}_p$ zyklisch und G daher wegen Lemma 122 abelsch. Dann würde aber $Z(G) = G$ und $|Z(G)| = p^2$ gelten, ein Widerspruch. Also muss $|Z(G)| = p^2$ sein. Daraus folgt $Z(G) = G$ und G ist somit abelsch. Wegen Satz 103 muss $G \cong \mathbb{Z}_{p^2}$ oder $G \cong \mathbb{Z}_p \times \mathbb{Z}_p$ gelten.

Satz 124: Es seien p und q zwei Primzahlen mit den Eigenschaften $p < q$ und $p \nmid (q-1)$. Ist G eine Gruppe der Ordnung $|G| = pq$, so ist G zyklisch und daher $G \cong \mathbb{Z}_{pq}$.

Beweis: Es seien P und Q eine p -Sylowgruppe und eine q -Sylowgruppe von G . Dann gilt $P \cap Q = \{e\}$. (Ist $a \in P \cap Q$, so $\exists m, n \in \{0, 1\} : \text{ord}(a) = p^m = q^n$. Daraus folgt $m = n = 0$ und daher $a = e$.) Bezeichnen s_p und s_q die Anzahl der p - bzw. q -Sylowgruppen von G , so gelten nach Satz 120 $s_p \mid q$, $s_p \equiv 1 \pmod{p}$, $s_q \mid p$ und $s_q \equiv 1 \pmod{q}$. Nach der dritten Bedingung muss $s_q \in \{1, p\}$ gelten. Wäre $s_q = p$, so würde wegen der vierten Bedingung

$q \mid (p-1)$ gelten, was wegen $p < q$ unmöglich ist. Also ist $s_q = 1$ und $Q \trianglelefteq G$ wegen Korollar 119 (ii). Ebenso folgt aus der ersten Bedingung $s_p \in \{1, q\}$. Wäre $s_p = q$, so würde aus der zweiten Bedingung $p \mid (q-1)$ folgen, was der Voraussetzung widerspricht. Also ist auch $s_p = 1$ und $P \trianglelefteq G$. Aus Satz 29 (iii) folgt $PQ \leq G$. Nun gilt aber $|PQ| = |G|$ und daher $G = PQ$. (Es ist $PQ = \{xy \mid x \in P, y \in Q\}$. Ist $x_1y_1 = x_2y_2$ für $x_1, x_2 \in P$ und $y_1, y_2 \in Q$, so folgt $x_2^{-1}x_1 = y_2y_1^{-1} \in P \cap Q = \{e\}$. Also ist $x_2^{-1}x_1 = y_2y_1^{-1} = e$ und daher $x_1 = x_2$ und $y_1 = y_2$.) Daher ist G inneres direktes Produkt von P und Q (nach Korollar 98). Aus $|P| = p$ und $|Q| = q$ folgt wegen Satz 121 $P \cong \mathbb{Z}_p$ und $Q \cong \mathbb{Z}_q$. Mit Hilfe von Korollar 99 und Satz 101 erhält man

$$G \cong P \times Q \cong \mathbb{Z}_p \times \mathbb{Z}_q \cong \mathbb{Z}_{pq}.$$

Bemerkung: Aus Satz 124 folgt, dass eine endliche Gruppe G zyklisch ist, wenn

$$|G| \in \{15, 33, 35, 51, 65, 69, 77, 85, 87, 91, 95, \dots\}.$$

Satz 125: Es sei $p \neq 2$ eine Primzahl und G eine Gruppe der Ordnung $|G| = 2p$. Dann ist G entweder isomorph zur zyklischen Gruppe \mathbb{Z}_{2p} oder zur Diedergruppe D_p .

Beweis: Nach Satz 111 gibt es $a, b \in G$, derart dass $\text{ord}(a) = p$ und $\text{ord}(b) = 2$. Wegen

$$[G : \langle a \rangle] = \frac{|G|}{|\langle a \rangle|} = \frac{2p}{p} = 2$$

ist $\langle a \rangle \trianglelefteq G$.

Wir behaupten nun $\langle a \rangle \cap \langle b \rangle = \{e\}$. Ist $x \in \langle a \rangle \cap \langle b \rangle$, so ist $x = a^k$ für ein $k \in \{0, 1, \dots, p-1\}$ und $x \in \langle b \rangle = \{e, b\}$. Aus der zweiten Bedingung folgt aber $x^2 \in \{e^2, b^2\} = \{e\}$. Also ist $x^2 = e$ und daher $a^{2k} = (a^k)^2 = x^2 = e$. Wegen Satz 15 (iii) gilt $p \mid (2k)$ und daher $p \mid k$. Das ist aber nur für $k = 0$ möglich und somit $x = e$.

Wir zeigen nun $G = \langle a \rangle \cdot \langle b \rangle = \{a^k b^\ell \mid 0 \leq k \leq p-1, \ell \in \{0, 1\}\}$. Wegen Satz 29 (iii) ist $\langle a \rangle \cdot \langle b \rangle \leq G$. Um Gleichheit zu zeigen, reicht es zu überprüfen, dass die in $\langle a \rangle \cdot \langle b \rangle$ enthaltenen Elemente paarweise verschieden sind. Es seien also $k_1, k_2 \in \{0, 1, \dots, p-1\}$, $\ell_1, \ell_2 \in \{0, 1\}$ und $a^{k_1} b^{\ell_1} = a^{k_2} b^{\ell_2}$. Dann ist $a^{k_1 - k_2} = b^{\ell_2 - \ell_1} \in \langle a \rangle \cap \langle b \rangle = \{e\}$. Dabei gelten $-p < k_1 - k_2 < p$, $\ell_2 - \ell_1 \in \{-1, 0, 1\}$ und wegen Satz 15 (iii) $p \mid (k_1 - k_2)$ und $2 \mid (\ell_2 - \ell_1)$. Das ist nur für $k_1 - k_2 = \ell_2 - \ell_1 = 0$ möglich. Also ist $k_1 = k_2$ und $\ell_1 = \ell_2$.

Wir zeigen als nächstes $bab \in \{a, a^{-1}\}$. Da $\langle a \rangle \trianglelefteq G$ ist $bab = bab^{-1} \in \langle a \rangle$ und folglich gibt es ein $k \in \{0, 1, \dots, p-1\}$ mit der Eigenschaft $bab = a^k$. Daher ist

$$a = b^2 ab^2 = b(bab)b = ba^k b = (bab)^k = (a^k)^k = a^{k^2}$$

und $a^{k^2-1} = e$. Aus Satz 15 (iii) folgt $p \mid (k^2 - 1)$. Das besagt aber gerade $p \mid (k-1)(k+1)$, woraus $p \mid (k-1)$ oder $p \mid (k+1)$ folgt. Das kann man umformulieren zu $k \equiv 1 \pmod{p}$ oder $k \equiv -1 \pmod{p}$. Mittels Satz 15 (iv) erhält man $bab = a$ oder $bab = a^{-1}$.

Ist $bab = a$, so folgt $ab = ba$ und G ist abelsch, da

$$a^{k_1} b^{\ell_1} a^{k_2} b^{\ell_2} = a^{k_1+k_2} b^{\ell_1+\ell_2} = a^{k_2+k_1} b^{\ell_2+\ell_1} = a^{k_2} b^{\ell_2} a^{k_1} b^{\ell_1}$$

für $k_1, k_2 \in \{0, 1, \dots, p-1\}$ und $\ell_1, \ell_2 \in \{0, 1\}$. In diesem Fall ist auch $\langle b \rangle \trianglelefteq G$ und G ist nach allem bisher gezeigten inneres direktes Produkt von $\langle a \rangle$ und $\langle b \rangle$ (nach Korollar 98). Also ist

$$G \cong \langle a \rangle \times \langle b \rangle \cong \mathbb{Z}_p \times \mathbb{Z}_2 \cong \mathbb{Z}_{2p}.$$

Ist $bab = a^{-1}$, so folgt $ba = a^{-1}b$ und $G \cong D_p$, da G genau die in Satz 47 beschriebenen Relationen erfüllt, d.h.

$$G = \langle a, b \rangle = \langle a \rangle \cdot \langle b \rangle, \text{ ord}(a) = p, \text{ ord}(b) = 2 \text{ und } ba = a^{-1}b = a^{p-1}b$$

und daher die selbe Struktur wie D_p hat.

Bemerkung: Aus Satz 125 folgt, dass eine nichtabelsche Gruppe G der Ordnung $|G| = 6$ zu D_3 isomorph ist. Insbesondere gelten $S_3 \cong D_3$ und $\text{GL}_2(\mathbb{Z}_2) \cong D_3$, da

$$\text{GL}_2(\mathbb{Z}_2) = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \right\}.$$

Lemma 126: Ist p eine Primzahl und G eine abelsche Gruppe der Ordnung $|G| = p^3$, so ist G zu einer der Gruppen \mathbb{Z}_{p^3} , $\mathbb{Z}_p \times \mathbb{Z}_{p^2}$ und $\mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p$ isomorph.

Beweis: Folgt sofort aus Satz 103.

Satz 127: Ist G eine nichtabelsche Gruppe der Ordnung $|G| = 8$, so ist $G \cong D_4$ oder $G \cong Q_8$ (wobei Q_8 die Quaternionengruppe aus Übungsbeispiel 25 bezeichnet).

Beweis: Für $a \in G$ ist $\text{ord}(a) \in \{1, 2, 4, 8\}$. Dabei gilt $\text{ord}(a) = 1$ nur für $a = e$ und $\text{ord}(a) = 8$ ist unmöglich, da G dann zyklisch und daher abelsch wäre. Das zeigt, dass $\text{ord}(a) \in \{2, 4\} \forall a \in G \setminus \{e\}$. Wegen Übungsbeispiel 12 ist $\text{ord}(a) = 2 \forall a \in G \setminus \{e\}$ unmöglich, da sonst G abelsch wäre. Also $\exists a \in G : \text{ord}(a) = 4$ und $\langle a \rangle = \{e, a, a^2, a^3\} \trianglelefteq G$, da $[G : \langle a \rangle] = |G|/|\langle a \rangle| = 8/4 = 2$. Ist $b \in G \setminus \langle a \rangle$, so ist

$$G = \langle a \rangle \cup b\langle a \rangle = \{e, a, a^2, a^3\} \cup \{b, ba, ba^2, ba^3\} \quad (*)$$

die Partition von G in Linksnebenklassen.

Wir behaupten $bab^{-1} = a^3 = a^{-1}$. Da $\langle a \rangle \trianglelefteq G$, ist $bab^{-1} \in \langle a \rangle = \{e, a, a^2, a^3\}$. Wäre $bab^{-1} = e$, so wäre $a = e$, Widerspruch. Wäre $bab^{-1} = a$, so wäre $ab = ba$ und wegen (*) würde leicht folgen, dass G abelsch ist, Widerspruch. Wäre $bab^{-1} = a^2$, so wäre $ba^2b^{-1} = (bab^{-1})^2 = (a^2)^2 = a^4 = e$ und daher $a^2 = e$, Widerspruch. Also ist $bab^{-1} = a^3$.

Wir zeigen als nächstes $b^2 \in \{e, a^2\}$. Da $|G/\langle a \rangle| = 2$, ist $G/\langle a \rangle \cong \mathbb{Z}_2$. Daraus ergibt sich $b^2\langle a \rangle = (b\langle a \rangle)^2 = \langle a \rangle$, woraus $b^2 \in \langle a \rangle = \{e, a, a^2, a^3\}$ folgt. Wäre $b^2 \in \{a, a^3\}$ (oder kurz

$b^2 = a^{\pm 1}$), so wäre $\text{ord}(b) \in \{1, 2, 4, 8\}$ aber unmöglich. Zunächst ist $\text{ord}(b) \neq 1$, da $b \neq e$. Auch ist $\text{ord}(b) \neq 2$, da $b^2 = a^{\pm 1} \neq e$. Weiters ist $\text{ord}(b) \neq 4$, da

$$b^4 = (b^2)^2 = (a^{\pm 1})^2 = a^{\pm 2} = a^2 \neq e.$$

Schließlich ist $\text{ord}(b) \neq 8$, da G dann zyklisch und daher abelsch wäre.

Ist $b^2 = e$, so folgt $G \cong D_4$, da G genau die in Satz 47 beschriebenen Relationen erfüllt, d.h.

$$G = \langle a, b \rangle, \text{ord}(a) = 4, \text{ord}(b) = 2 \text{ und } ba = a^{-1}b = a^3b$$

und daher die selbe Struktur wie D_4 hat.

Ist $b^2 = a^2$, so folgt $G \cong Q_8$, da G genau die in Übungsbeispiel 25 beschriebenen Relationen erfüllt, d.h.

$$G = \langle a, b \rangle, \text{ord}(a) = \text{ord}(b) = 4, a^2 = b^2 \text{ und } ba = a^3b$$

und daher die selbe Struktur wie Q_8 hat.

Bemerkung: Mit Hilfe der bisherigen Resultate kann man alle Gruppen G mit Ordnung $|G| \leq 15$ klassifizieren (mit Ausnahme einer Lücke für Gruppen der Ordnung 12):

Ordnung	abelsch	nichtabelsch	Begründung
2	\mathbb{Z}_2		Satz 121
3	\mathbb{Z}_3		Satz 121
4	$\mathbb{Z}_4, \mathbb{Z}_2 \times \mathbb{Z}_2$		Satz 123
5	\mathbb{Z}_5		Satz 121
6	\mathbb{Z}_6	D_3	Satz 125
7	\mathbb{Z}_7		Satz 121
8	$\mathbb{Z}_8, \mathbb{Z}_4 \times \mathbb{Z}_2, \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$	D_4, Q_8	Lemma 126, Satz 127
9	$\mathbb{Z}_9, \mathbb{Z}_3 \times \mathbb{Z}_3$		Satz 123
10	\mathbb{Z}_{10}	D_5	Satz 125
11	\mathbb{Z}_{11}		Satz 121
12	$\mathbb{Z}_{12}, \mathbb{Z}_6 \times \mathbb{Z}_2$	D_6, A_4, T	
13	\mathbb{Z}_{13}		Satz 121
14	\mathbb{Z}_{14}	D_7	Satz 125
15	\mathbb{Z}_{15}		Satz 124

Dass jede abelsche Gruppe der Ordnung 12 entweder zu \mathbb{Z}_{12} oder zu $\mathbb{Z}_6 \times \mathbb{Z}_2$ isomorph ist, folgt sofort aus Satz 103. Sowohl D_6 als auch A_4 sind nichtabelsche Gruppen der Ordnung 12, die nicht zu einander isomorph sind (z.B. weil D_6 ein Element der Ordnung 6 enthält, A_4 aber nicht). Nicht angegeben habe wir aus Zeitgründen eine Konstruktion der Gruppe T und einen Beweis, dass jede nichtabelsche Gruppe der Ordnung 12 zu einer der Gruppen D_6 , A_4 und T isomorph ist. Es existieren genau 14 paarweise nicht zueinander isomorphe Gruppen der Ordnung 16.

Lemma 128: Die alternierende Gruppe A_5 ist einfach.

Beweis: Die Gruppe A_5 enthält folgende Elemente:

20 verschiedene 3-Zyklen $(a b c)$, d.h. Elemente der Ordnung 3, die in 10 verschiedenen 3-Sylowgruppen der Gestalt $\{\varepsilon, \sigma, \sigma^2\}$ bzw. $\{\varepsilon, (a b c), (a c b)\}$ enthalten sind.

24 verschiedene 5-Zyklen $(a b c d e)$, d.h. Elemente der Ordnung 5, die in 6 verschiedenen 5-Sylowgruppen der Gestalt $\{\varepsilon, \sigma, \sigma^2, \sigma^3, \sigma^4\}$ bzw.

$$\{\varepsilon, (a b c d e), (a c e b d), (a d b e c), (a e d c b)\}$$

enthalten sind.

15 verschiedene Produkte zweier elementfremder Transpositionen $(a b)(c d)$ der Ordnung 2, die in 5 verschiedenen 2-Sylowgruppen der Gestalt $\{\varepsilon, (a b)(c d), (a c)(b d), (a d)(b c)\}$ enthalten sind

Schließlich enthält A_5 noch das neutrale Element ε .

Es sei nun $N \trianglelefteq A_5$, $N \neq \{\varepsilon\}$. Wegen $|A_5| = 60 = 2^2 \cdot 3 \cdot 5$ gilt $|N| \mid 2^2 \cdot 3 \cdot 5$.

1. Fall: $3 \mid |N|$. Wegen Satz 111 $\exists \sigma \in N : \text{ord}(\sigma) = 3$, d.h. N enthält einen 3-Zyklus σ . Daher enthält N auch die 3-Sylowgruppe $P = \{\varepsilon, \sigma, \sigma^2\}$. Wegen

$$\tau \circ P \circ \tau^{-1} \leq \tau \circ N \circ \tau^{-1} = N \quad \forall \tau \in A_5$$

und Korollar 119 (i) enthält N alle 3-Sylowgruppen und damit alle 3-Zyklen. Da A_5 nach Satz 46 (iii) von den 3-Zyklen erzeugt wird, gilt $N = A_5$.

2. Fall: $5 \mid |N|$. Wegen Satz 111 $\exists \sigma \in N : \text{ord}(\sigma) = 5$, d.h. N enthält einen 5-Zyklus σ . Daher enthält N auch die 5-Sylowgruppe $P = \{\varepsilon, \sigma, \sigma^2, \sigma^3, \sigma^4\}$. Wegen

$$\tau \circ P \circ \tau^{-1} \leq \tau \circ N \circ \tau^{-1} = N \quad \forall \tau \in A_5$$

und Korollar 119 (i) enthält N alle 5-Sylowgruppen und damit alle 5-Zyklen. Wegen

$$(a b c) = (a c d b e) \circ (a d c e b)$$

enthält N dann auch alle 3-Zyklen und $N = A_5$.

3. Fall: $|N| = 4$. Dann wäre N eine 2-Sylowgruppe. Da es 5 verschiedene 2-Sylowgruppen gibt, kann N wegen Korollar 119 (ii) aber kein Normalteiler sein, Widerspruch.

4. Fall: $|N| = 2$: Dann hätte N die Gestalt $N = \{\varepsilon, (a b)(c d)\}$. Wegen

$$(a b e) \circ (a b)(c d) \circ (a b e)^{-1} = (a b e) \circ (a b)(c d) \circ (a e b) = (b e)(c d) \notin N$$

(für $\{a, b, c, d, e\} = \{1, 2, 3, 4, 5\}$) wäre N dann aber kein Normalteiler, Widerspruch.

Satz 129: Die alternierende Gruppe A_n ist einfach für $n \geq 5$.

Beweis: Wir verwenden Induktion nach n . Der Fall $n = 5$ wurde in Lemma 128 bewiesen. Es sei nun $n > 5$. Für $1 \leq i \leq n$ sei $U_i = \{\sigma \in A_n \mid \sigma(i) = i\}$. Dann ist $U_i \leq A_n$ und $U_i \cong A_{n-1}$. Daher ist U_i nach IV einfach für $1 \leq i \leq n$. Für $i, j, k \in \{1, \dots, n\}$ paarweise verschieden gilt

$$(i j k) \circ U_i \circ (i j k)^{-1} = (i j k) \circ U_i \circ (i k j) = U_j.$$

Ist nämlich $\sigma \in U_i$, so ist $\sigma(i) = i$ und daher $((i j k) \circ \sigma \circ (i k j))(j) = j$. Das besagt, dass $(i j k) \circ \sigma \circ (i k j) \in U_j$ und somit $(i j k) \circ U_i \circ (i k j) \subseteq U_j$. Aus Symmetriegründen gilt $(j i k) \circ U_j \circ (j i k)^{-1} \subseteq U_i$ und daher

$$U_j \subseteq (j i k)^{-1} \circ U_i \circ (j i k) = (i j k) \circ U_i \circ (i j k)^{-1}.$$

Es sei nun $N \trianglelefteq A_n$ und $N \neq \{\varepsilon\}$. Nach Satz 29 (i) ist $N \cap U_i \trianglelefteq U_i$ und daher $N \cap U_i = \{\varepsilon\}$ oder $N \cap U_i = U_i$.

1. Fall: $\exists i \in \{1, \dots, n\} : N \cap U_i = U_i$. Dann ist $U_i \leq N$. Aus

$$U_j = (i j k) \circ U_i \circ (i j k)^{-1} \leq (i j k) \circ N \circ (i j k)^{-1} = N$$

(für $i, j, k \in \{1, \dots, n\}$ paarweise verschieden) folgt $U_1 \cup \dots \cup U_n \subseteq N$ und daher auch $\langle U_1 \cup \dots \cup U_n \rangle \leq N$. Da $U_1 \cup \dots \cup U_n$ alle 3-Zyklen enthält, ist $A_n = \langle U_1 \cup \dots \cup U_n \rangle \leq N$, also $N = A_n$.

2. Fall: $N \cap U_i = \{\varepsilon\}$ für $1 \leq i \leq n$. Es sei $\sigma \in N \setminus \{\varepsilon\}$. Dann muss $\sigma(i) \neq i$ für $1 \leq i \leq n$ gelten. Da $n \geq 6$, gibt es 6 paarweise verschiedene $a, b, c, d, e, f \in \{1, \dots, n\}$ mit den Eigenschaften $\sigma(a) = b$ und $\sigma(c) = d$. Wir betrachten die Permutation

$$\tau := \sigma^{-1} \circ (c f e) \circ \sigma \circ (c e f).$$

Dann ist $\tau \in N$ (da $(c f e) \circ \sigma \circ (c e f) = (c f e) \circ \sigma \circ (c f e)^{-1} \in N$ und $\sigma^{-1} \in N$) sowie $\tau \in U_a$ und $\tau \neq \varepsilon$ (da $\tau(f) = c$), Widerspruch.